TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

2€

0% DE PUBLICITÉ

LIBERTÉ ET PARTAGE

HACKER news Magazine

LE MAGAZINE 100% SÉCURITÉ L

VIE PRIVÉE

MASQUER LE SYSTÈME OPÉRATIF

HACKING

AU COEUR D'UN MALWARE

HAMACHI

CRÉEZ VOTRE RÉSEAU UNDERGROUND

WINDOWS VISTA

CRÉEZ VOTRE VERSION HACKER

HARDWARE

SURVEILLÉ PAR VOTRE

IMPRIMANTE

CAUCHEMAR OU RÉALITÉ

Les logiciels qui CRAQUENT VOTRE CONNEXION WIFI

Année 6 – n° 25 Bimestriel
mars - avril 2009

Hacker News Magazine
Et son complice italien
Hacker Journal
1ers magazines européens Hacker

Les camarades de la rédaction européenne :
Damien Bancal,
BMS, Majo, Gualty.

Traduction et adaptation :
Laurent et Sylvie Arsena

Couverture:
Daniele Festa

Editeur :
WLF Publishing SRL
Via Donatello 71
00196 Roma

Imprimeur : Roto 2000.
Via Leonardo da Vinci 18/20
Casarile (MI) Italy

Distribution:
NMPP
Directeur de la publication :
Teresa Carsaniga

Dépôt légal : à parution
ISSN : en cours

Lamer ('lae'mr)
Aspirant cracker, aux capacités et connaissances informatiques limitées, souvent maladroit et disposé à mener des actions douteuses et nuisibles.

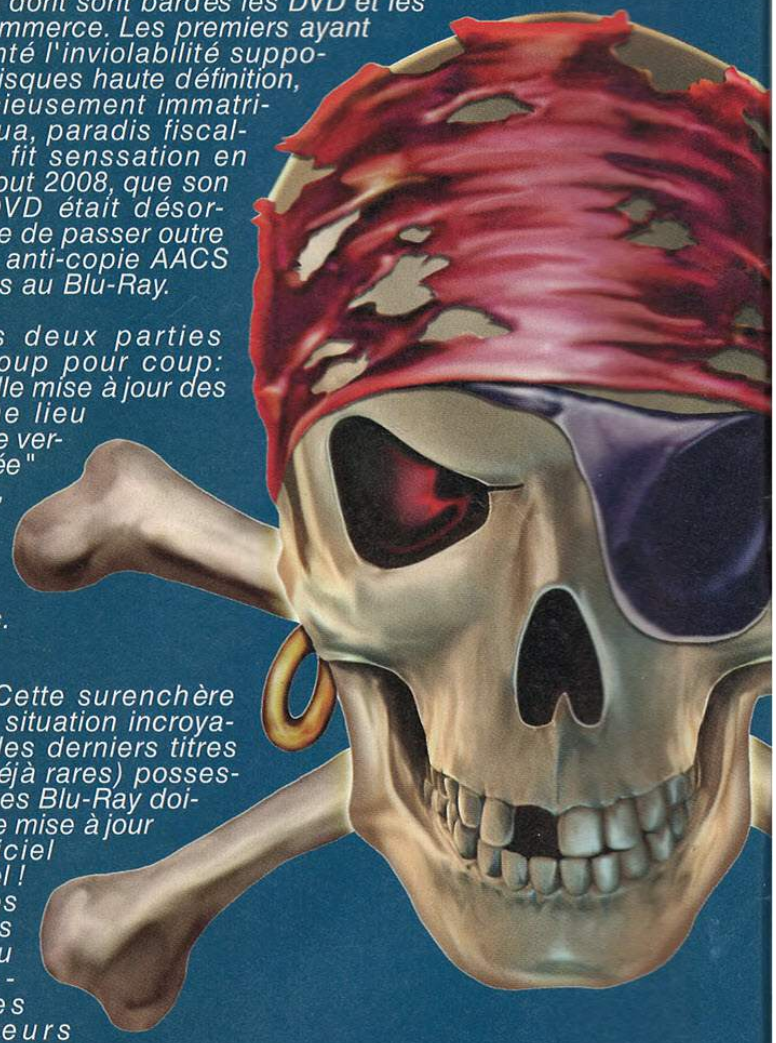
Editorial

HACKER Magazine

Et pendant ce temps là...

"La liberté n'offre qu'une chance d'être meilleur, la servitude n'est que la certitude de devenir pire."
Albert Camus (1913-1960)

Depuis quelques semaines se déroule un petit jeu du chat et de la souris, aussi réjouissant que navrant. Il met aux prises, d'un coté les éditeurs vidéo et les fabricants de lecteurs Blu-Ray, de l'autre Slysoft, concepteur d'un programme capable d'oter les protections dont sont bardés les DVD et les Blu-Ray du commerce. Les premiers ayant longtemps vanté l'inviolabilité supposée de leurs disques haute définition, Slysoft - judicieusement immatriculée à Antigua, paradis fiscal- let législatif - fit senssation en annonçant, début 2008, que son logiciel AnyDVD était désormais en mesure de passer outre les dispositifs anti-copie AACS et BD+ intégrés au Blu-Ray.



Depuis, les deux parties se rendent coup pour coup: Chaque nouvelle mise à jour des verrous donne lieu à la sortie d'une version "améliorée" d'ANYDVD, à laquelle succède une mouture renforcée des protections, etc. Amusant ?

Oui et Non. Cette surenchère conduit à une situation incroyable: pour lire les derniers titres publiés les (déjà rares) possesseurs de platines Blu-Ray doivent opérer une mise à jour du micro-logiciel de leur matériel ! Révalateur des paradoxes que vivent au quotidien- les honnetes consommateurs de biens et services numériques, payant moult redevances et taxes au nom d'un droit à la copie privée qu'ils ne pauvent exercer puisque les supports enregistrés disposent de verrous que la loi interdit de briser !

CARTES de CRÉDIT

Piratage d'hologrammes

Découverte d'un groupe de pirates d'Europe de l'Est qui commercialisent des hologrammes de cartes bancaires.

Un forum russe des plus particulier, que nous ne garderons secret, propose un petit commerce qui semble particulièrement lucratif. Nous connaissions les skimmeurs (pour copier les données de la bande magnétique), les embosseurs (qui reproduisent les données physiques d'une CB), les mules (blanchissent l'argent volé). Voici venir les vendeurs d'hologrammes pour cartes bancaires. Les prix varient selon la carte et surtout l'hologramme. Nous avons pu constater 1 dollar par autocollant à 2 dollars pour les hologrammes destinés à une presse à chaud. Les "commerçants" vendent en gros "100 pièces, 250$; 500 pièces, 800$".

Des pirates de plus en plus équipés

Le FBI a mis la main, début février, sur un homme soupçonné de piéger des distributeurs de billets. Les policiers de l'Oncle Sam parlent d'une vaste escroquerie "sophistiquée" destinée à voler des renseignements bancaires à partir de distributeurs automatiques de billets. Gabriel Cirlan, un citoyen roumain, a été arrêté en possession de dizaines de cartes de crédit et du matériel d'interception, des skimmers. L'équipement en sa possession n'avait encore jamais été vu.

Même inquiétude, en Europe, en fin 2008. Les policiers de plusieurs pays européens enquêtaient sur une fraude à la carte bancaire à très grande échelle. Les pirates piégaient des lecteurs de cartes bancaires de magasins afin d'en intercepter les données (bande magnétique, code secret). Première constatation, nous sommes très loin des yescardeurs des années 90. Trois circuits piratés ont été découverts dans un des T.P.E. (Terminal carte bancaire) saisi dans une boutique. Le premier circuit est conçu pour copier les détails de la carte avant que le lecteur ne puisse chiffrer les renseignements. Le deuxième circuit sauvegarde les données et utilise un chiffrement pour les protéger de toutes lectures extérieures. Le troisième et dernier circuit agit comme un téléphone portable qui communique les données volées à un serveur basé à Lahore, au Pakistan.

TWITT JACKING

Les utilisateurs du réseau social Twitter découvrent que cliquer sur n´importe quel lien peut rapidement devenir dangereux. Le blogueur Korben a expliqué, fin janvier, comment

Korben

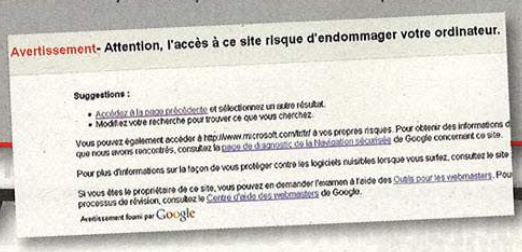
il est simple d'afficher un lien et un message sur le compte des utilisateurs Twitter. Une technique qui a été baptisée le "twitt-jacking". Les blogueurs se retrouvaient, après avoir cliqué sur un bouton, avec des messages diffusés en leur nom sur leur Twitt. http://www.korben.info/twitter/ohoh.html.

BRAQUAGE NUMÉRIQUE

Des pirates informatiques ont tenté de voler 242 millions d'euros aux clients de la Sumitomo Mitsui Banking Corporation en infiltrant, tout simplement, les ordinateurs des salariés de la banque japonaise. L'affaire est en cours de jugement en Angleterre. Le piratage date de 2004, des escrocs, avec la complicité d'un vigile, ont installé des keylogger (des logiciels espion, NDR) dans les machines des banquiers. Finalité de ce braquage peu commun, détourner 229 millions de Livres Sterling, soit la coquette somme de 242 millions d'euros, via 20 transferts. Parmi les sociétés visées par ces transferts pirates, Toshiba. Le vigile, Kevin O'Donoghue, aidé par deux pirates informatiques belges (Jan Van Osselaer et Gilles Poelvoorde), va réussir a installer les espiogiciels dans les machines de l'agence bancaire. Quelques jours plus tard, le vigile récupérait les données tapées au clavier par les salariés, logins et mots de passe en tête. Les 20 transferts d'argent seront orchestrés pour remplir des comptes basés à Dubaï, Hong-Kong et Singapour. Une erreur dans la commande de transfert va faire capoter ce piratage. Les pirates viennent de passer devant le tribunal de Snaresbrook Crown. Ils ont plaidé coupable. Trois autres présumés pirates, des bulgares, ont été entendus par la justice britannique. A la différence du vigile et des deux sujets belges, les trois hommes venus de l'Est nient toute implication dans cette tentative de fraude. Un quatrième homme concerné par cette affaire est décédé quelques jours après les transferts ratés.

UN SIMPLE SLASH FAIT PLANTER GOOGLE

Le dernier jour de janvier aura été plus que particulier pour le géant de l'Internet Google. L'ensemble des sites Internet référencés par le moteur de recherche avaient été considérés, pendant 50 minutes, comme potentiellement dangereux. Une panne de 14H30 et 15H25 qui informait les internautes, à chaque requête, que le site que les surfeurs recherchaient été potentiellement malsains. Google a invoqué une erreur humaine "Malheureusement, indique le service presse de Google, l'erreur humaine, l'URL / a été par mégarde cochée dans le fichier et le slash s'est retrouvé dans toutes les URL". Le groupe a présenté ses excuses. Google a annoncé "mettre en place des vérifications plus rigoureuses pour empêcher que l'erreur ne se reproduise".


Avertissement- Attention, l'accès à ce site risque d'endommager votre ordinateur.

Suggestions :

- Accédez à la page précédente et sélectionnez un autre résultat.
- Modifiez votre recherche pour trouver ce que vous cherchez.

Vous pouvez également accéder à http://www.microsoft.com/fr/fr/ à vos propres risques. Pour obtenir des informations que nous avons rencontrés, consultez la page de diagnostic de la Navigation sécurisée de Google concernant ce site.

Pour plus d'informations sur la façon de vous protéger contre les logiciels nuisibles lorsque vous surfez, consultez le site

Si vous êtes le propriétaire de ce site, vous pouvez en demander l'examen à l'aide des Outils pour les webmasters. Pour processus de révision, consultez le Centre d'aide des webmasters de Google.

Avertissement fourni par Google

STOP WAREZ

La Gendarmerie Nationale de Roubaix, a interpellé six pirates de films, fin janvier. Plus de 900 DVD saisis. Six pirates de films qui commercialisaient, sur leur étale, des DVD contrefaits. La plainte est partie de la Fédération nationale des distributeurs de films (FNDF) et de l'Association de Lutte contre le piratage audiovisuel (ALPA). 941 DVD et 800 euros en liquide ont été saisis. Les officiers de police judi-

HOT NEWS

ÉTRANGE BUG CHEZ SFR

Fin janvier, des clients Internet NeufBox SFR se sont retrouvés à pouvoir regarder dans les ordinateurs des autres clients. Le Media Center, l'outil de visualisation informatique, a été montré du doigt. Tout est parti d'une alerte postée dans le forum dédié à la Neufbox SFR "Utilisant pour la 1ère fois le média center, explique un client, J'ai eu la surprise de constater que le contenu de l'ordinateur d'un abonné SFR et habitant près de chez moi s'affichait sur ma télé". Plusieurs tests plus tard, il s'est avéré qu'effectivement un abonné Neufbox, équipé de son média center, était capable de lire les informations contenues dans un ordinateur d'un autre client. SFR a remplacé les modems capricieux par une nouvelle génération.

PRISON FERME POUR AVOIR PIRATÉ NUMERICABLE

David H., 22 ans, a été condamné à six mois de prison ferme pour escroquerie par le tribunal correctionnel de Meaux. Le substitut du procureur avait requis une peine de deux ans ferme à l'encontre de ce pirate informatique. Un pirate qui dort depuis en prison. L'internaute a été accusé d'avoir escroqué Numericable de 286,000 €. Il utilisait 4 modems, donc 4 numéros différents, pour la mise ne place de son escroquerie. Une arnaque qu'il exploitait depuis mai 2007. Il a été condamné pour vol, usage de faux, dénonciation mensongère et escroquerie. Les enquêteurs de la section financière de la police judiciaire de Meaux ont interpellé le jeune homme en pleine action, devant son clavier. L'internaute passait douze heures par jour sur des sites de jeux.

SON NOM BON, JAMBON

Un Néo-zélandais de 29 ans, en vacances aux USA, a acheté dans une boutique d'occasion un dossier de 60 pages de données militaires. Dans le dossier, les noms et des détails personnels sur des soldats américains. Pour être plus précis, Chris Ogle avait trouvé un sympathique baladeur MP3 dans un magasin d'Oklahoma. Il va donc l'acheter et tenté d'y placer sa musique. Dans le petit disque dur de l'appareil, les précieux et sensibles documents traitant de militaires basés en Irak et en Afghanistan en 2005. Le baladeur lui a coûté 7 euros.

Un comique face aux pirates

Le comique Québécois Anthony Kavanagh proposait, pour les fêtes de fin d'année, son dernier spectacle en DVD, un spectacle (très bon) intitulé Anthony.kavanagh.com. Mi-janvier, ce dernier a déposé plainte pour piratage de sa carte bancaire. Un pirate a utilisé les données bancaires de l'artiste pour faire des achats sur la toile. Bilan de l'escroquerie, 7.000 euros d'achats. Nous ne savons pas encore si le comique a été piégé par un skimmeur ou un "simple" récupération de données bancaires lues sur la carte de ce dernier.

ciaire se sont invités aux domiciles des interpellés. Des graveurs et des centaines de jaquettes ont été saisies. Trois personnes ont été mises en garde à vue. C'est la section financière du parquet de Lille qui se charge de la suite de l'affaire. Le préjudice a été évalué à 26.000 €.

Piratage de Nintendo DS

L'ELSPA, une entité en charge des droits d'entreprises comme Nintendo, vient de communiquer sur l'arrestation d'un couple de Britannique accusé de piratage. L'homme et la femme ont été pris la main dans le sac en commercialisant des Nintendo DS contrefaites. L'ELSPA n'explique pas si les consoles étaient fausses ou tout simplement équipées d'une cartouche de type R4. Une quarantaine de consoles DS - modifiées - ont été saisies ainsi que 150 jeux piratés pour DS et Game Boy Advance. Michael Rawlinson, le directeur de l'ELSPA s'est félicité de cette arrestation. Les deux présumés pirates auraient gagné, rien que pour le mois de décembre, 53.000 euros. Ils trouvaient leurs clients via eBay.

E.T.; APPELER; POLICE

Comme Bastia et Issy-les-Moulineaux, la commune de Béthune, dans le Nord de la France, est en train de tester deux bornes qui ont pour mission de contrôler les stationnements automobiles. En cas de dépassement, les robots policiers avertissent la police municipale. Dès que les 15 minutes de stationnement autorisés sont dépassés, la machine change de couleur, annonce le temps de dépassement, le montant de l'amende et téléphone à la police municipale qui n'a plus qu'à verbaliser. Un système sans fil permettra de rentrer en contact avec des cartes que les personnes handicapées apposeront sur leur pare-brise.

LA RIAA ABANDONNE LES POURSUITES ALÉATOIRES

La RIAA, l'association en charge des droits d'auteurs des majors du disque US, a annoncé qu'elle allait arrêter de poursuivre les internautes américains soupçonnés de téléchargement illégal. Une chasse à l'homme qui ne cesse pas pour autant. La RIAA compte passer des accords avec des FAI pour adopter un mécanisme comparable à celui de la "riposte graduée" à la française. L'idée reste la même : envoi d'un courriel d'avertissement, baisse de la bande passante (retour au bon vieux 28 bauds ?), et coupure de l'accès en cas de récidive. Aux USA, pas de loi pour cette riposte graduée. La RIAA s'en fou !

TRICHERIE POUR CALL OF DUTY WORLD AT WAR

Qu'est ce qu'il y a de plus rageant dans un jeu en réseau qu'un tricheur ? Et bien deux tricheurs ! Depuis quelques semaines, Des joueurs ont trouvé le moyen de ne plus perdre dans la nouvelle version de Call of Duty World at war. Que se soit sur Xbox 360 ou Playstation 3, la rédaction a pu constater que des petits malins pouvaient se cacher sous les maps de certaines parties en ligne. Les cartes RoundHouse et Makin sont bugguées. Dans le premier cas, le tricheur peut passer sous les éléments du décor et flinguer tout ce qui lui passe sous le fusil. Dans le second cas, il peut se cacher dans un rocher. Dernier trouvaille en date... s'envoler. Certains ont trouvé le moyen de survoler le décor et de tirer sur tout ce qui bouge.

UN PLAN EUROPÉEN CONTRE LES PIRATES

Le Conseil de l'Union Européenne a édité un plan, sur 5 ans, qui aura pour mission de traquer les infractions sur les réseaux. Dans le document, l'Europe annonce des cyberpatrouilles et des équipes d'investigation Internet qui auront pour mission de dépister les criminels sur le net. Le terrorisme, la pédophilie, l'usurpation d'identité, faux documents, ventes illicites, détournement et blanchiment d'argent, contrefaçon, ...seront dans la liste des actes à traquer. Autant dire que les policiers vont avoir du boulot dans le siècle à venir !

PIRATES DE DISTRIBUTEURS DE BILLETS VOLATILISES DANS LA NATURE

Le buzz avait fait le tour de la planète en Lucian Popa, 26 ans, Nicolae Manea, 34 ans, Ionel Stoïca, 22 ans et Ionut Parvu, 29 ans, le chef de la bande, avaient piégé le distributeur de billets d'une agence bancaire bretonne. Avec une mini caméra et un lecteur de

HOT NEWS

UN FABRICANT DE CARTES BANCAIRES PIRATÉ

Le fabricant américain de cartes de crédits Heartland Payment Systems a découvert qu'un pirate informatique était passé dans son système informatique a été piraté. Dans son communiqué de presse, l'entreprise Heartland Payment Systems fait savoir que son équipe d'informaticien a découvert que son système informatique avait été visité.

Une intrusion qui date de 2008 et qui aurait permis à des pirates de faire main basse sur des données concernant les systèmes de paiement de la société.

L'alerte a été lancée par Visa et MasterCard. D'après cette entreprise "ni les données commerciales, ni les numéros de Sécurité sociale, ni les chiffres cryptés d'identification personnelle (PIN), pas plus que les adresses et numéros de téléphones" n'ont été volés.

carte collés sur le vrai distributeur, ils avaient réussi à intercepter et cloner les cartes bancaires passées par leur système électronique. Une technique qui va permettre de retirer, ensuite via les CB clonées 17,725 € dans plusieurs pays d'Europe comme la Roumanie, en Italie et en France.

Le tribunal de Rennes en Bretagne a condamner les quatre pirates à six, 12 et 30 mois de prison. Seul petit détail, les quatre pirates n'étaient pas là. Ils ont pris la fuite, avec un mandat d'arrêt international leur colle dorénavant aux baskets.

BACK TO THE FUTUR POUR GEARS OF WAR

Voilà une sécurité comme on les aime. Bien charnue, bien dodue et... bien débile. Le 28 janvier, les utilisateurs du jeu PC Gears Of War se sont retrouvés avec un achat inutilisable. Motif ? L'expiration du dit software qui s'est mis ne marche. La faute à l'expiration inopinée du certificat de validation. Bilan, les joueurs qui avaient acquis légalement leur jeu se sont retrouvés avec un DVD inutilisable. Epic, l'éditeur, cherche une solution. Plusieurs solutions ont été proposées comme celle de retarder l'horloge de son ordinateur. No comment !

DIRECTION LA PRISON POUR MAKSIK

Maksym Yastremsky, connu sur la toile sous le pseudonyme de Maksik, était un pirate informatique très recherché. L'homme, âgé de 25 ans, était même un gros poisson. L'escroc s'était spécialisé dans la capture de données bancaires sur Internet. Maksym avait été arrêté en Turquie, en août 2007, dans une station balnéaire du sud du pays.

3Le pirate, qui était recherché par les autorités américaines, a été arrêté cinq jours après son arrivée en Turquie en compagnie d'un ressortissant israélien dans une boîte de nuit de Kemer.

Il a été accusé d'avoir revendu des centaines de milliers de numéros de cartes de crédit via plusieurs groupes qu'il fréquentait. L'un des groupes en question a été reconnu coupable du piratage des sociétés OfficeMax, T.J.Maxx, Boston market, ...Maksym Yastremsky vient d'écoper de 30 ans de prison ferme dans les geôles Turques.

Fin de la guerre des licences du monde "libre" ?

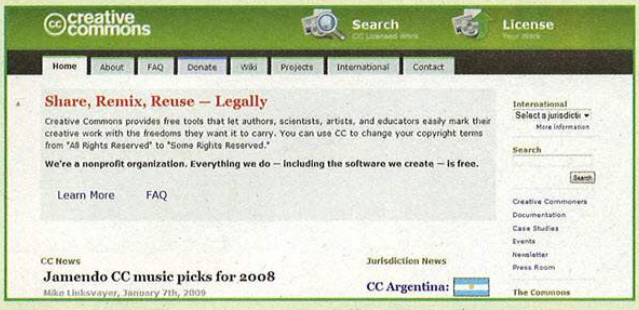
Open oui, mais avec quelle licence ?

En matière de protection des œuvres, maintenant plusieurs années que le monde Open source se divisait en deux courants bien distincts: tandis que la quasi-totalité des programmeurs était réunie autour de la Free Software Foundation, presque tous les auteurs de contenus Open (musique, vidéos et éléments graphiques en tête), utilisaient les licences proposées par l'organisation Creative Commons.

Le problème n'était pas banal: si ces deux groupes scandent haut et fort la libre circulation des idées, les perspectives développées restent propres à chacun. La Free Software Foundation a toujours placé le software et le matériel inhérent, au centre de son système, tandis que les Commoners, fervents défenseurs de la Creative Commons, ont toujours évalué la question sur le plan des contenus, en consacrant leurs efforts à la réglementation de la diffusion de musiques, vidéos et textes.
Les licences Creative Commons se caractérisent depuis toujours par la possibilité d'être personnalisées dans leurs moindres détails, en laissant à leurs auteurs un large choix parmi les options suivantes : utiliser ou non leurs œuvres dans un cadre commercial, accepter certaines modifications et plus généralement en attribuant une partie de l'œuvre finale à son auteur original, bloquer ces modifications ou encore changer la juridiction de la licence en fonction du pays d'appartenance de l'auteur, etc. Les licences FSF se sont, quant à elles, toujours caractérisées par une rigidité plus prononcée, typique de l'utilisation sous licence du software. Deux univers séparés, donc, qui ont malgré tout cohabité pendant plusieurs années.

:: Ensemble... sous la contrainte

Mais nul doute qu'à la fin, ces deux associations étaient vouées à se rencontrer, où plutôt à se heurter. Si, par exemple, la FSF protège le software et les manuels qui vont avec, il est évident que ces mêmes manuels peuvent aussi être considérés comme de simples œuvres pouvant, à ce titre, intégrer les principaux intérêts des



Creative Commons s'est toujours distinguée de par l'attention portée aux licences consacrées à tous types d'œuvres: musique, textes, sans oublier les softwares et le graphisme.

GNU s'est consacrée quant à elle aux licences à destination des softwares, en se heurtant par la force des choses, aux licences Creative Commons destinées aux autres types d'œuvres.

licences CreativeCommons. De la même façon, un jeu vidéo n'est pas uniquement un software: il présente toujours de nombreux points communs avec un film et dispose de sa propre bande-son, d'éléments graphiques, etc. D'autres problèmes surgissent aujourd'hui encore, si l'on considère les possibilités offertes aux utilisateurs de ces matériels. Comme la possibilité de réutiliser en tout ou partie l'œuvre originale pour créer quelque chose de nouveau, en reprenant certains extraits tout en citant leurs sources, pour des résultats différents selon qu'il s'agisse d'œuvres musicales ou littéraires.

La confusion, qui n'a fait que se renforcer au fil des ans, a souvent contraint les créateurs de contenus de tout type, à se transformer en véritables avocats pour identifier laquelle des licences disponibles leur correspondait le mieux. Sans parler ensuite des licences originales, auxquelles certains auteurs ont ajouté des clauses supplémentaires, en augmentant par-là même le niveau de fragmentation générale. Des auteurs qui, sans même s'en rendre compte, violent ainsi des licences à cause de quelques détails. C'est ainsi que le problème des licences a explosé de façon incontrôlable au cours de ces dernières années.
Un auteur qui souhaite écrire un essai publié sous licence Creative Commons, et dans lequel il cite des extraits de Wikipédia, qui, elle, utilise une licence FSF: ces deux licences sont incompatibles et l'auteur risque donc de les enfreindre toutes deux. Idem pour un programmeur qui souhaiterait insérer un dessin publié sous licence Creative Commons dans un programme utilisant des parties développées pour Linux, distribué sous licence FSF. Une cohabitation qui, avant le grand revirement, était difficile voire impossible. Une situation qui, alliée à la confluence naturelle de tous les types de matériels, n'a fait qu'aggraver le niveau de confrontation entre les associations et les licences proposées, en les contraignant au final à une certaine forme de conciliation.

:: L'Open uni

La Free Software Foundation a donc fait le premier pas, en ajoutant dans la version 1.3 de la GNU Free Document License, plus connue sous le nom de licence FDL, une section permettant aux wiki publiés sous cette licence, tels que Wikipédia, d'adopter également la licence Creative Commons Attribution ShareAlike version 3.0. La nouvelle licence FDL permet d'utiliser simultanément la version concurrente de Creative Commons. Seule obligation: utiliser la variante de Creative Commons, qui permet de réutiliser l'œuvre commercialement parlant, en attribuant sa paternité à l'auteur et en autorisant toute modification de cette dernière.
Un événement sans doute médiatisé du fait que l'encyclopédie la plus connue au monde, Wikipédia, a toujours été distribuée sous licence FDL. Un choix délibéré des programmeurs qui l'ont créée, dans la mesure où il s'agissait du type de licence auquel tout programmeur se référait, mais qui rendait incompatibles les termes d'utilisation de Wikipédia avec ceux de nombreux autres contenus se référant aux licences CreativeCommons. Un problème, donc, qui séparait Wikipédia du reste du monde Open, en empêchant la libre circulation des contenus qui ne cadraient pas avec la licence FSF et qui, ne pouvaient intégrer Wikipédia. Parallèlement, les articles qui composent Wikipédia ne pouvaient être réutilisés dans de nombreux autres contextes Open.

Wikipédia avec les licences GNU, est sans doute à l'origine des plus gros problèmes de cohabitation avec les licences Creative Commons. S'en est suivi un processus d'unification inachevé.

En attendant la version 2 de la licence GNU Free Document License, cette mise à jour de la version 1.3 résout les problèmes créés par ces incompatibilités, et marque une ouverture vers un monde Open réellement unifié, même sur un plan juridique.

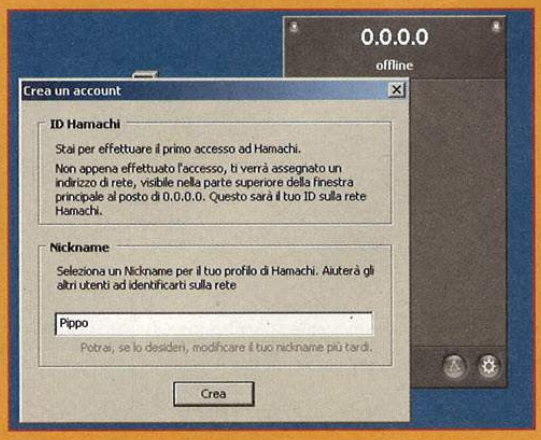
Connectez deux ordinateurs distants à l'aide d'un VPN qui vous permettra également de chatter !

Rencontres du... troisième type

Tout est né de l'exigence d'échanger rapidement des données avec mon ami Zot et ce, sans trop de complication. Dans un premier temps, nous nous sommes contentés d'exploiter les éléments mis à notre disposition par Windows, tant volontairement qu'involontairement (en exploitant les fameux problèmes de sécurité en termes de partage). Mais sur des systèmes constamment mis à jour, cette approche ne convenait pas. En outre, mon ami dispose d'un PC derrière un pare-feu. Quant à moi, j'ai une structure réseau un peu complexe avec pare-feu et proxy. Après mûres réflexions, nous avons opté pour Hamachi, un programme au nom quelque peu étrange mais qui, au final, présente de multiples avantages : valide, robuste, facile à configurer et à gérer. Ce programme crée une carte de réseau virtuel sur votre PC, avec sa propre adresse IP, qui peut être utilisée pour se connecter à des réseaux Hamachi déjà existants (créés par exemple par vos amis) ou pour en créer un bien à vous et permettre à vos amis d'accéder à vos partages.

:: Installation

Son installation est très simple : il suffit de télécharger le fichier à partir de l'adresse www.hamachi.it, de l'exécuter et de suivre les instructions fournies par le système ; seule recommandation : utiliser des noms d'ordinateurs lisibles et des mots de passe complexes. Vous devez surtout être très attentifs à ces derniers. En effet, une fois le mot de passe "deviné" par un individu malintentionné, celui-ci pourra accéder en toute quiétude à votre système.



Choix de votre pseudo sur le réseau Hamachi

Le setup d'Hamachi vous demande s'il doit installer le programme en tant que service de Windows ou s'il doit le lancer normalement. Il est généralement conseillé de toujours garder le contrôle sur toutes les applications, choisissez donc la seconde option. Une fenêtre s'affiche ensuite, où l'installation vous demande si elle doit désactiver ou non les services réseau pour Hamachi, pour des raisons de sécurité. Mais vu que vous l'installez justement pour pouvoir utiliser ces services, gardez-les activés sans cocher la case. Il vous sera enfin demandé si vous souhaitez utiliser la version commerciale d'essai ou celle gratuite. Choisissez celle gratuite, largement suffisante pour notre opération.

:: La configuration

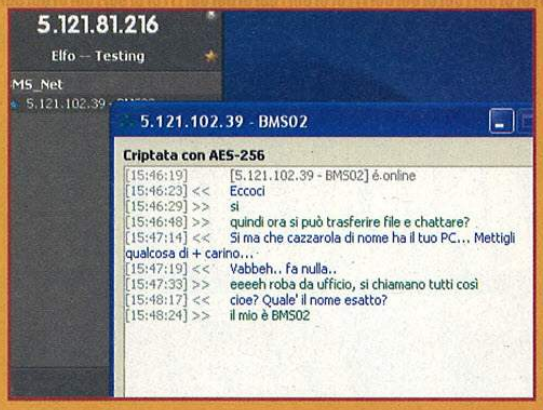
Une fois le tout installé, lors du premier lancement du programme, celui-ci vous demandera certaines informations relatives à la création de votre pseudo grâce auquel les autres utilisateurs vous verront et vous rejoindront via le réseau. Hamachi tentera dès lors une connexion en se basant sur les données utilisées par Internet Explorer. Malheureusement, il ne

parvient pas toujours à les lire correctement. Ne soyez donc pas étonné si vous recevez un message d'erreur. Pour accéder aux menus de configuration, vous devez cliquer sur l'icône en forme de roue dentée en bas à droite. Dès lors, vous pourrez effectuer toutes les modifications nécessaires, y compris le changement de Pseudo, le paramétrage des proxies...

Ici, vous pouvez choisir de rejoindre un réseau existant ou d'en créer un bien à vous

:: Utilisation d'Hamachi

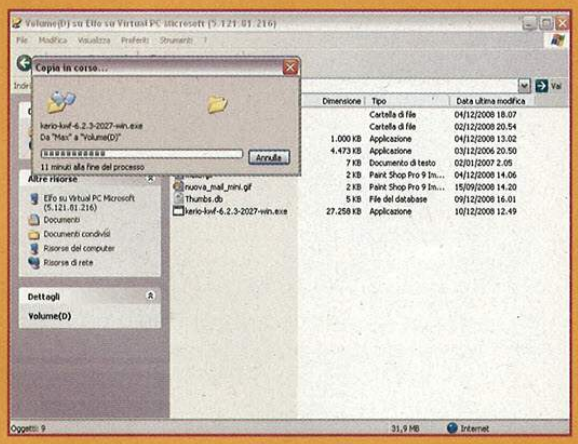
Après avoir personnalisé toutes les différentes fonctions, vous pourrez accéder au réseau en cliquant sur le bouton en bas à gauche. Dès que vous serez connecté, le système affichera en haut l'adresse IP de la carte du réseau virtuel d'Hamachi. Cette adresse sera utilisée pour accéder à des réseaux Hamachi déjà existants ou pour créer votre réseau privé. Nous vous conseillons de configurer dès à présent un master password. Créez ensuite votre réseau ou connectez-vous à un réseau existant, en cliquant sur l'icône avec le triangle en bas à droite. Une fois la connexion établie avec le serveur, vous pourrez également contrôler le trafic généré par le réseau, en ouvrant Ressources réseau et en double-cliquant sur la carte réseau Hamachi.
Si vous créez vous-même votre réseau, après avoir communiqué à vos amis son nom et le mot de passe que vous avez choisi, vous pourrez utiliser les véritables services du programme. Le plus direct ? Le chat bien sûr, certes spartiate mais très utile si vous partagez des fichiers ou dossiers et que vous souhaitez contacter directement l'utilisateur sans devoir utiliser d'autres messageries. Vous pourrez lancer de façon tout aussi simple une session de ping permanente, en double-cliquant sur le nom de l'utilisateur destinataire. Un service très utile si vous souhaitez détecter d'éventuels problèmes de performances sur le réseau. Pour trouver en revanche vos "copains de réseau", vous pouvez utiliser les Ressources réseau en cliquant sur Rechercher ordinateur... ou encore sélectionner Rechercher à partir du menu contextuel d'Hamachi. Une fois que serez directement connecté au PC de votre ami, vous pourrez envoyer et recevoir des fichiers en utilisant tout simplement les systèmes de partage de Windows, comme si vous étiez en train de travailler sur un réseau local. Bref, une méthode infiniment plus rapide que n'importe quel programme P2P.



Le chat d'Hamachi, spartiate certes, rapide et utile

:: Le véritable objectif d'Hamachi

En réalité, Hamachi a été créé en tant que protocole de communication pour pouvoir jouer en multijoueur et ce, même si vous n'êtes pas connectés au même réseau local. Avec un peu de patience, vous pouvez configurer le réseau pour l'utiliser avec la plupart des jeux. Dans ce cas, vous pourriez rencontrer certaines difficultés liées au fait que certains serveurs de jeux exigent que les joueurs soient sur le même réseau. Je m'explique. Prenons par exemple les IP 5.1.12.123 et 5.1.34.111. Dans ce cas, il ne devrait pas y avoir de problèmes. Mais le réseau d'Hamachi attribuera difficilement des IP proches aux différents utilisateurs. Il y aura donc de fortes chances pour que la seconde IP soit 5.4.21.145 et, dans ce cas, le serveur pourrait signaler une erreur de type "IP Class C error". Surtout, pas de panique ! Vous pourrez facilement résoudre le problème en cliquant à l'aide du bouton droit sur votre ami présent dans la liste et en lui assignant un "Peer VPN alias" qui réponde à vos exigences.



Le transfert de fichier s'effectue directement via le système de partage de Windows

:: Conclusions

Le système de connexion proposé par Hamachi est très utile pour créer de petits réseaux VPN et présente l'avantage d'être très léger et fiable, à travers l'utilisation du protocole SSL. Vous devez toutefois rester vigilant lorsque vous configurez des options de connexion avec bridging car vous pourriez modifier involontairement les paramètres réseau en cours et rendre inutilisable le réseau local ou même Internet pour certaines applications. Sentiment général : un réseau rapide et simple qui permet d'agir sur les ordinateurs de vos amis un peu comme s'ils étaient chez vous...

GPU: DES ARMES INQUIETANTES ET REDOUTABLES...

WLAN en danger ! Le système de défense le plus efficace, a été percé ! La nouvelle inquiète les entreprises de sécurité IT

Il n'y a pas encore si longtemps, seuls les jeux vidéo et le 3D nous venaient à l'esprit lorsqu'on évoquait les accélérateurs graphiques. Pourtant, le 9 octobre dernier, Elcomsoft (www.elcomsoft.com), une entreprise russe spécialisée dans la récupération de mots de passe, a présenté un software capable de "cracker" les protections WPA et WPA2 utilisées sur les réseaux Wi-Fi et ce, en exploitant la capacité de calcul des cartes nVidia. Son nom ? Elcomsoft Distributed Password Recovery (EDPR). L'interception de quelques paquets de données lui suffirait semble-t-il à contourner les défenses de l'algorithme, pour lancer ensuite une attaque. Avec 20 postes de travail en parallèle, chacun équipé de deux GeForce GTX 280 et une licence à 599 €, on parviendrait ainsi à centupler la vitesse de crackage par rapport à ce que l'on obtiendrait avec un seul PC. Autrement dit, avec ce nouveau logiciel, une clé WPA peut être forcée en quelques semaines, voire quelques jours.

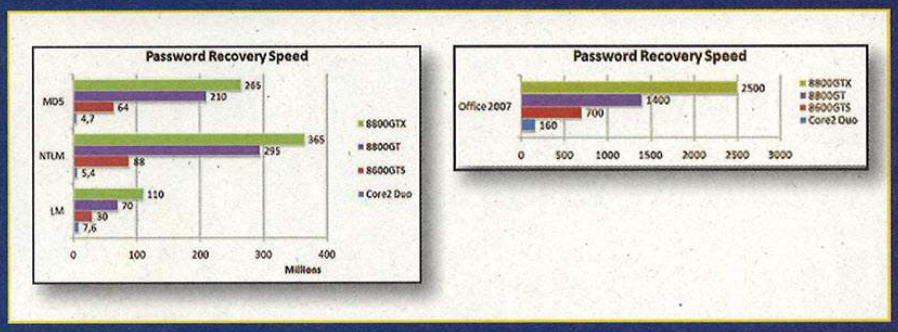
La nouvelle a immédiatement fait bondir le secteur de l'IT Security. Dès le 10 octobre, la société GSS, leader mondial dans le domaine de la sécurité informatique, a commencé à alerter ses clients en leur suggérant de renforcer leurs défenses. Comment ? En ajoutant un niveau de sécurité supplémentaire à leurs réseaux Wi-Fi: un système de chiffrement basé sur le VPN (Virtual Private Network), puisqu'il agit au niveau de l'application, à savoir entre PC et PC (vous trouverez le communiqué officiel à l'adresse suivante): **www.gss.co.uk/news/article/5503/Wi-Fi_is_no_longer_a_viable_secure_connection/).**

:: COMMENT LE WPA PEUT-IL ETRE VIOLE ?

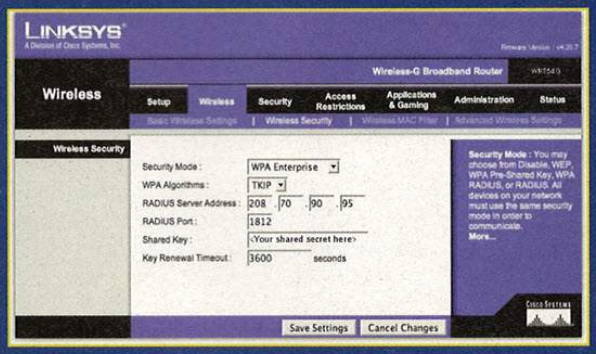
Il existe deux méthodes pour protéger les réseaux Wi-Fi : l'une basée sur le WEP et l'autre sur les clés WPA/WPA2. Contrairement à l'univers de l'entreprise, où les réseaux utilisent habituellement une protection RADIUS les réseaux Wi-Fi domestiques utilisent les

méthodes de sécurité WPA et WPA2, basées sur l'utilisation du chiffrement et d'un mot de passe pour protéger le trafic de données entre utilisateurs et point d'accès. La force de ces algorithmes (l'ancien protocole WEP a été désormais abandonné car jugé peu fiable du fait de certaines failles de sécurité découvertes dans son algorithme) réside dans le fait qu'il faut nécessairement recourir à une attaque par "brute force" pour les percer. Autrement dit, tous les mots de passe possibles et inimaginables doivent être testés jusqu'à ce que le bon soit trouvé.

Avec des milliards de combinaisons possibles, il faudrait ainsi des années avant de réussir à pénétrer un réseau protégé par WPA/WPA2. Et c'est là qu'intervient la nouveauté d'Elcomsoft: grâce à la puissance de calcul des accélérateurs graphiques et l'utilisation d'algorithmes développés à cet effet, les délais peuvent être radicalement écourtés, en renforçant ainsi les performances de ce type d'attaque.



Avec l'exploitation du GPU, la récupération du mot de passe est jusqu'à 50 fois plus rapide, comparé aux méthodes traditionnelles qui utilisent uniquement le processeur du PC.

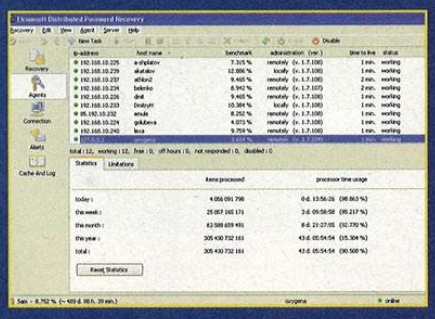


RADIUS est l'acronyme de Remote Authentication Dial-In User Service. Il s'agit du protocole utilisé par les applications qui permettent d'accéder à distance aux réseaux IP.

:: COMMENT CE SOFTWARE FONCTIONNE-T-IL ?

EPDR est vendu comme un outil de "récupération de mots de passe", conçu donc pour retrouver des données qui vous appartiennent. En théorie, il ne fonctionne qu'avec certains des formats de fichiers les plus courants (par exemple .doc, .pdf...). Mais dans la pratique, la liste de ces fichiers est si longue, qu'il fonctionne en réalité avec tous les formats de fichier. Cette liste semble être là pour éviter de dire que le programme récupère en fait le mot de passe de n'importe quel fichier (ce qui serait illégal). Ce software peut piloter jusqu'à 64 postes de travail dont chacun peut supporter jusqu'à 4 cartes avec GPU. Une carte NVIDIA GeForce GTX280 peut traiter à elle seule des centaines de milliards de calculs entiers par seconde. Il est possible d'atteindre 1,5 Go de mémoire vidéo onboard et d'augmenter jusqu'à 128 le nombre de processeurs pouvant fonctionner en parallèle, en entrant ainsi dans l'univers du calcul parallèle pour un coût bien inférieur à celui des supercalculateurs.

EDPR peut coordonner le travail de 10 000 postes de travail connectés entre eux en réseau. L'administrateur réseau dispose d'une console de gestion qui affiche tous les nœuds connectés ainsi qu'un résumé de la quantité de calculs effectués. Mais ce software peut exploiter l'accélération de calcul à partir d'une seule carte montée sur votre PC. Prenons un exemple: pour récupérer le mot de passe d'accès à Windows Vista, avec un dual-core récent, il faudrait deux mois, tandis qu'avec EDPR et une seule carte GeForce, la même opération prendrait 3 à 5 jours, selon la puissance du processeur et de la carte.



Voici l'interface graphique d'EDPR, très simple mais efficace...

:: COMMENT SE DEFENDRE ?

Concernant les clés actuellement utilisées, il faut dire que le software délivré peut forcer les mots de passe les plus simples, ceux basés sur des caractères ASCII et ceux de type statique. Mais, souvent, lorsqu'on installe un réseau Wi-Fi dans une petite entreprise, on ne s'attarde pas à activer ce type de protection ou on se contente de survoler la personnalisation de la configuration, en paramétrant des niveaux de sécurité trop bas ou en gardant les valeurs par défaut. Nous vous conseillons de renforcer le plus possible vos seuils de sécurité et de considérer comme un minimum ce qui, jusqu'à hier, était considéré comme un niveau avancé.

La question de la sécurité des WLAN concerne l'aspect "Application": combien de temps faudra-t-il en effet avant que la prochaine génération de GPU ou de puces dédiés, puisse casser la protection des VPN ? Les algorithmes 3DES et DES peuvent être violés déjà assez facilement par des machines dédiées à cet effet, et tandis que le cryptage AES semble être le meilleur, rien ne garantit que tôt ou tard, quelqu'un découvrira un beau ver caché dans son algorithme.

Vista... façon hacker

Après Windows 98, 2000 et XP, testons dès à présent une version allégée de Vista. Un défi pur et dur !

Windows Vista symbolise à lui seul un réel pas en arrière par rapport aux dernières versions de Windows XP, sans doute le produit le plus apprécié de chez Microsoft. Sans doute disparaîtra-t-il aussi rapidement de notre mémoire dès que de nouvelles versions sortiront. Les raisons de cet échec sont nombreuses et chacun d'entre nous a son avis sur la question et sur son (faible) attrait. C'est pourtant le système d'exploitation dont vous devrez vous contenter puisque, la plupart du temps, il est déjà pré-installé lorsque vous achetez un nouveau PC. A vous, donc, de vous adapter... Mais s'adapter ne signifie pas pour autant baisser les bras. D'ailleurs, comme nous l'avons déjà expérimenté avec Windows XP, voici quelques conseils pour "retoucher" Vista et créer sa version strip down !

:: Manque de polyvalence

Principal difficulté de cette opération: le manque de polyvalence de Vista. De nombreux hackers du monde entier essaient de mettre au point une installation allégée de Vista, mais tôt ou tard, des incidents surgissent et le rendent inutilisable. Nous ne disposons donc pas des mêmes conditions que pour une installation d'XP, où XPLite permettait de réduire à 40 Mo l'espace occupé, qui plus est, avec le système d'exploitation déjà installé, ou encore à seulement 9 Mo l'espace nécessaire pour Windows 9x embedded !

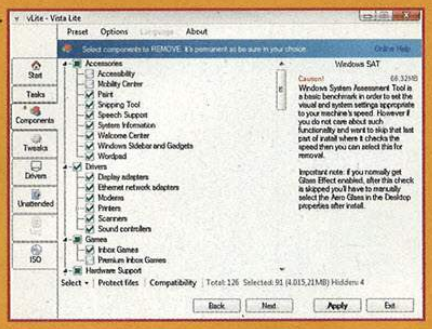
Dans le cas présent, vous pouvez retirer certaines fonctionnalités non critiques, mais pas assez pour pouvoir affirmer que l'OS a été réduit à sa plus simple expression. Cette opération doit surtout être réalisée avant d'avoir installé le système, c'est-à-dire en agissant sur les fichiers setup et en recréant une image ISO de l'installation, prête à être utilisée sur un nouveau PC. Pour accomplir cette opération, vous devrez utiliser vLite, un programme disponible à l'adresse suivante : http://www.vlite.net/.

La première fenêtre de vLite vous demande où trouver les files originaux de Vista et où enregistrer les files de la nouvelle ISO.

:: Outils nécessaires

Vous avez tout d'abord besoin du support d'origine contenant l'installation de Vista. Dès lors, le programme récupérera les fichiers nécessaires en fonction des options choisies et les gravera à nouveau sur DVD (impossible ici de parler de CD comme pour XP) avec le fichier contenant le script d'installation modifié. Il s'agit en réalité de l'héritier de nLite, le programme avec lequel vous pouviez créer des versions "strip down" (réduites en fonctionnalités) des précédents OS.

A noter toutefois que vous n'êtes pas obligé de vous en servir sur Vista:

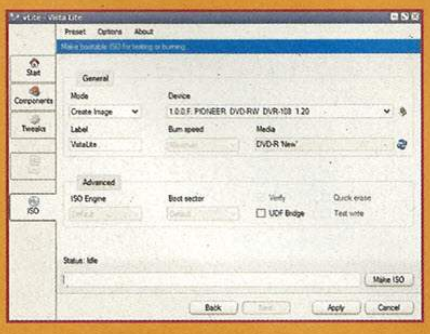


La liste des options que vous pouvez retirer. Pour celles indispensables, un message tel que celui-ci s'affiche.

si vous disposez du DVD original, vous pouvez préparer l'image en utilisant Windows XP. Pour créer l'image finale, vous avez également besoin d'au moins 4 Go d'espace disque.

:: Comment procéder ?

Installez vLite sur votre PC et insérez le DVD original de Vista dans le lecteur de votre PC. Après avoir lancé le programme et accepté les conditions d'utilisation, vous devez sélectionner la source des fichiers de Vista, c'est-à-dire indiquer à vLite le lecteur où réside le DVD original et, en quelques minutes (une fois que le programme aura accompli la lecture et la préparation des fichiers initiaux), vous pourrez commencer à faire le tri parmi les différentes options pour gagner un peu d'espace. Ce programme permet de retirer toute une variété d'options. En passant le pointeur sur chacune d'elles, vous pourrez lire leur description sur le panneau de droite, et un message vous avertira si le composant en question est vital ou non pour le fonctionnement



La phase de gravure du nouveau DVD de Vista avec sa configuration minimale.

d'autres composants. Dans ce cas, vous devrez bien réfléchir avant de le retirer, sous peine de créer des dysfonctionnements au sein de votre système d'exploitation, une fois celui-ci installé. Voici les éléments qui peuvent être retirés selon la communauté online, sans engendrer de problèmes spécifiques:

GAMES
- Inbox Games
- Premium Inbox Games

HARDWARE SUPPORT
- SmartCards

LANGUAGES
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

MULTIMEDIA
- Speech Support
- Tablet PC
- Wallpapers

NETWORK
- Connect to a Network Projector
- Internet Information Services
- Remote Desktop and Assistance

SERVICES
- Error Reporting
- Remote registry
- Windows Remote Management

SYSTEM
- Accessibility
- Natural Language
- Windows Easy Transfer

Après avoir sélectionné ceux que vous souhaitez retirer, en cliquant sur Next, vous accéderez à la phase de création de l'ISO finale. Vous pourrez choisir de retirer totalement les fichiers inutiles de la nouvelle version allégée, ou de les garder et de modifier uniquement ceux avec les scripts d'installation pour qu'ils ne soient pas pris en compte, ni copiés sur le disque en phase de setup. Il ne vous reste donc plus qu'à graver votre version personnelle de Vista et à essayer de l'installer sur un PC ou sur une machine virtuelle pour voir si elle fonctionne.

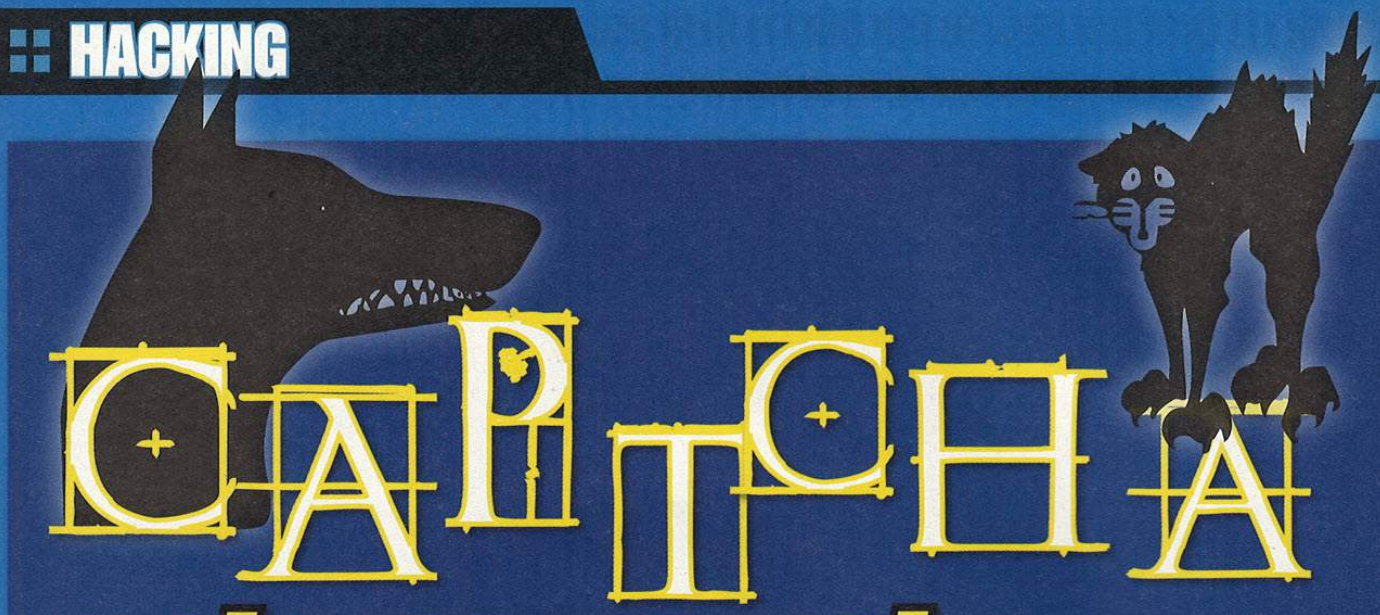
Les principaux avantages d'une version allégée avec vLite de Windows Vista tiennent davantage du gain d'espace disque que du gain en termes de performances. En retirant presque tous les composants mentionnés (et fiables), vous pourrez économiser quelques centaines de Mo. Sur les forums online, certains affirment avoir allégé l'installation jusqu'à 1,5 Go, mais on ignore avec quelle fiabilité et facilité d'utilisation. Vous aurez également quelques programmes en moins tournant en background, mais pour obtenir une réelle augmentation de performances, les hackers sont unanimes: désactiver Aero, l'interface graphique de Vista, à partir du menu Personnaliser pour passer à celles plus spartiates, jusqu'à ce que vous atteignez celle ultra légère tirée de Windows 2000.

:: Autres options

En réalité, vLite vous permet de réaliser d'autres opérations, mais, pour l'heure, elles ne sont pas fiables à 100 %. Vous pouvez intégrer dans l'installation d'éventuels drivers pour périphériques en votre possession, ou inclure des Services Packs et autres mises à jour publiés par Microsoft au fil du temps. Vous pouvez également inclure d'autres softwares dont vous souhaitez profiter, une fois l'installation terminée. Mais dans ce cas, vous ne serez plus face à une version allégée de Windows Vista, puisque, au contraire, vous augmenterez considérablement sa taille. Les autres options disponibles permettent de paramétrer les scripts d'installation de sorte que celle-ci s'effectue automatiquement.

:: Des alternatives ?

Eh non, inutile de passer à Linux, le but de l'opération étant de continuer à utiliser Vista mais seulement avec les composants essentiels à son fonctionnement. Il existe sur le Net une version super allégée de Vista, appelée TinyVista, téléchargeable via Torrent et qui promet d'occuper moins de 3 Go d'espace, de ne fonctionner qu'avec 256 Mo de RAM et de conserver tant Aero que les principaux programmes comme Internet Explorer 7 et Windows Media Player. Il s'agit d'un produit non officiel, il autorise l'installation sans demander aucun code produit: attention donc à ce que vous téléchargez...



CAPTCHA

mais pourquoi sont-ils si méchants ?

A quoi servent les Captcha et pourquoi tombons-nous aussi souvent dessus ?

Agaçants au possible, on aimerait bien les voir disparaître ! Et pourtant, ils poussent comme des champignons tandis que nous surfons. Eux, ce sont les champs où vous devez taper, avec une extrême précision, ces lettres et chiffres presque illisibles qui apparaissent là, à proximité, sur la page. Mais pourquoi les sites nous demandent-ils d'accomplir cette action ? Rares sont ceux qui se sont posés la question... L'existence des Captcha est liée à la nécessité de se défendre contre ces personnes qui n'utilisent Internet que pour leur profit personnel. A l'exemple du spamming. Le "spammeur" a en effet besoin d'un grand nombre d'adresses e-mail pour faire partir ses messages. Pour remplir cette mission, il utilise donc des robots qui, à partir des différents fournisseurs de services de messagerie online, tels qu'Hotmail, Orange, Free, etc., "dérobent" automatiquement des adresses utiles au spamming. Autre application utile des Captcha: le contrôle des demandes adressées aux sites. Des demandes fréquentes, telles que l'envoi anormal et répété de messages à un forum, pourraient mettre en péril la capacité de traitement du serveur, en provoquant des conséquences semblables à celles d'une attaque DoS.Les Captcha sont chargés de s'assurer qu'il y a bien un être pensant et non un robot malveillant derrière chaque demande adressée à un serveur, d'où leur nom qui, en anglais, signifie : "completely automated public turing test to tell computers and humans apart" (test public de Turing complètement automatique ayant pour but de différencier les humains des ordinateurs).

Malgré la présence des Captcha, des services comme Hotmail ou Gmail continuent d'être attaqués. D'après une récente enquête, il semblerait même que le taux de réussite des attaques contre Hotmail soit compris entre 10 et 15 %. Pour contourner cet obstacle, l'astuce est simple, du moins en théorie: créer des programmes qui, à l'instar d'OCR hyper-intelligents, soient capables d'interpréter les Captcha, en permettant de contourner leur filtre sans l'intervention humaine.

:: Comment fonctionnent-ils ?

Etapes de ce type de programme pour décoder un Captcha textuel (des Captcha vocaux existent également):

- **Réduction des brouillages de fond**
  Elle consiste à retirer tous les fragments d'informations inutiles et à réduire les couleurs de fond. Des images cassées ou n'ayant

aucune correspondance possible avec des intersections de lettres ou de chiffres existants, sont généralement écartées et effacées du fond.

- **Segmentation logique**
  Une fois l'image nettoyée, on assiste alors à la segmentation logique des éléments.
- **Identification**
  La dernière phase se base sur les comparaisons entre formes et sur la compatibilité correspondante des différentes lettres et chiffres avec ces formes.

Des résultats de ce genre ont déjà été atteints par différents programmes. Parmi les plus célèbres: Xrumer Conjecture qui outre le fait de simuler le comportement d'un utilisateur standard, en créant par exemple des messages sur les forums, peut justement interpréter les Captcha défensifs de Gmail, et PWNtcha, très simple à utiliser en termes d'implémentation et de programmation, capable de décoder des Captcha spécifiques.

:: La bataille continue

C'est du fait de la simplicité avec laquelle on parvient à cracker un Captcha textuel que l'on recherche des solutions autres que des chiffres et caractères déformés. Certains développeurs travaillent en direction de l'interprétation des images, en proposant des photos montrant un hippopotame, un serin et un chat et en demandant à l'utilisateur de répondre à une question inhérente à ces animaux. Mais dans ce secteur, l'incroyable puissance de l'Intelligence Artificielle entre en scène. Philippe Golle, chercheur au célèbre Palo Alto Research Center, a expliqué comment une IA, parfaitement entraînée, pouvait parvenir à des résultats impensables. Ce chercheur a ainsi montré que l'on pouvait violer la nouvelle technologie graphique de Microsoft (Asirra) en entraînant l'IA à distinguer le contenu des images proposées par le système.

L'interface d'Asirra : si vous décidez d'adopter un petit chat, en cliquant sur le lien, la procédure s'annule. Vous devrez renouvelez la sélection.

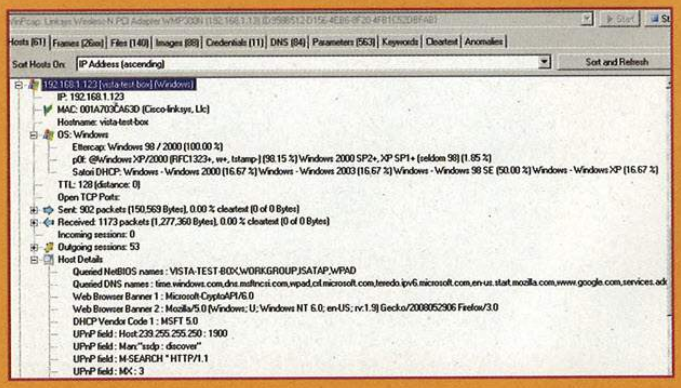
Dans un test effectué avec un software utilisant des principes semblables à ceux de Microsoft, on propose au visiteur certaines images d'animaux, issues d'une base de données constituée de millions de photos, et on lui demande de faire la distinction entre des races et variétés de félins ou canidés. Golle a prouvé que la barrière n'était pas insurmontable pour un ordinateur. Son logiciel est parvenu à différencier les photos de chiens des photos de chats. Pour obtenir ce résultat, des techniques avancées ont été utilisées, capables de reconnaître les formes en tenant en compte de la position de ces dernières, de leurs proportions et de leurs couleurs. La proportion de rose sur la langue d'un chien pourrait être un facteur discriminant pour écarter la possibilité qu'il s'agisse d'un chat. Ou, au contraire, la présence de la couleur jaune des yeux, associée au noir du pelage, pourrait identifier un chat au détriment d'un chien. En attendant, les études et les tests de Golle se poursuivent et son système continue d'apprendre... Jusqu'où ira-t-il ? Ainsi nous le saurons rapidement...

OSfuScate

Changez l'empreinte de votre système d'exploitation et éviter ainsi qu'il ne soit identifié sur le Web

Comme nous le savons tous, quiconque est confronté au choix de lancer une attaque sur une machine Windows ou une machine Linux, n'a pas l'ombre d'un doute : de par sa nature, Windows est (hélas) un véritable parc d'attraction pour les individus malintentionnés du Net, qui changent d'exploit comme de chaussures, certains que tôt ou tard ils trouveront la faille.

Dès le premier sondage de la machine victime, il leur est en effet très facile d'identifier votre système d'exploitation. Une donnée qui peut être facilement déduite des caractéristiques TCP/IP détectées. Si vous souhaitez donc passer la nuit tranquille tandis que vous laissez votre PC télécharger sur la Mule, mieux vaut alors brouiller les pistes et laisser croire aux éventuels intrus insomniaques que votre PC tourne sur un système d'exploitation différent du système réel.



Pour découvrir votre système d'exploitation, rien de plus facile avec des programmes comme Nmap, NetworkMiner ou Ettercap

:: Le principe

Des programmes comme Nmap, Ettercap ou NetworkMiner peuvent reconnaître un système d'exploitation grâce à ses paramètres TCP/IP spécifiques. Autrement dit, lorsque ce type de programme trouve une séquence spécifique de paramètres, il est sûr d'être en présence d'une machine Windows, ou Linux ou BSD et ainsi de suite.

Le principe du subterfuge est simple : si vous changez la façon dont le stack TCP/IP de votre machine est lu depuis l'extérieur, il est alors fort probable que le programme utilisé pour vous espionner

le confonde avec celui d'un autre système ou encore ne soit pas du tout en mesure de l'identifier. L'opération doit toutefois être réalisée très attentivement, pour ne pas provoquer de dysfonctionnements. Nous savons que Windows conserve toutes les données de configuration dans la base de registre. C'est donc sur cette base de registre que vous devrez intervenir, avec toutes les précautions qui s'imposent. Faites tout d'abord une copie de sauvegarde du registre pour pouvoir le restaurer en cas de problèmes. A cet égard, vous pouvez utiliser un programme spécifique très utile, tel qu'ERUNT (vous pouvez le télécharger à l'adresse http://www.larshederer.homepage.t-online.de/erunt/). Si vous disposez ensuite d'un autre ordinateur en réseau, vous pouvez l'utiliser comme machine de tests en y installant les programmes nécessaires (Nmap par exemple). C'est à partir de là que vous lancerez les scans vers votre PC, avant et après avoir brouillé l'empreinte du système d'exploitation.

:: Procédures de changement

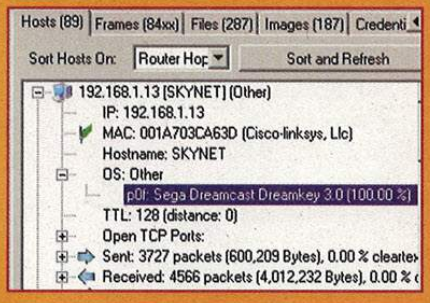
Deux solutions s'offrent à vous : la première consiste à agir manuellement ; dans ce cas, ouvrez la base de registre avec Regedit (si vous n'avez pas créé de raccourci pour le lancer, passez par Démarrer/Exécuter/regedit.exe). Les rubriques que vous devez modifier sont toutes enregistrées dans **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**. Les voici :

DefaultTTL
Tcp1323Opts
EnablePMTUDiscovery
TcpUseRFC1122UrgentPointer
TcpWindowSize
SackOpts
Interfaces*\MTU

Bien sûr, vous ne pouvez pas entrer de valeurs au hasard, non seulement parce que vous saboteriez ainsi, selon toute probabilité, le fonctionnement de votre système, mais aussi parce que votre objectif consiste à laisser croire aux attaquants qu'ils se trouvent face à un autre système d'exploitation. Vous devrez donc récupérer des informations sur la façon dont ces paramètres sont réglés dans le système d'exploitation que vous souhaitez simuler. Une bonne source d'informations à cet égard : le guide de Nmap, que vous trouverez à l'adresse http://nmap.org/book/toc.html. Le chapitre 8 est notamment entièrement consacré à l'identification du système d'exploitation. La seconde solution consiste à se fier à un programme capable d'effectuer directement toutes ces opérations.

Grâce à l'interface d'insertion d'OSfuscate, choisissez votre profil...

OSfuscate est un software spécialement conçu à cet effet. Vous devez juste le lancer, choisir quel système d'exploitation vous souhaitez imiter et lui permettre de changer le registre de Windows en toute autonomie. Vous pouvez le télécharger à l'adresse suivante : http://irongeek.com/downloads/OSfuscate.3.zip. Il ne nécessite pas d'installation. Qui plus est, il est totalement personnalisable grâce à des fichiers de configuration portant l'extension .os et contenant toutes les informations nécessaires pour imiter un système spécifique.



Après le "traitement" OSfuscate, votre PC surfe sur le Web à l'instar d'une Nintendo Dreamcast

:: Mais ce n'est pas tout !

Cette opération de brouillage de pistes vous protège des scans occasionnels et non approfondis, sans doute lancés par des programmes qui se contentent d'une analyse partielle sans entrer dans les détails. NetworkMiner et Satori sont en revanche plus agressifs, car ils peuvent également identifier votre OS à partir de l'empreinte DHCP émise sur le réseau. Impossible de modifier celle ci en altérant simplement le registre, la chaîne étant codée dans une dll de Windows (dhcpcsvc.dll). Seule alternative : vous équiper d'un éditeur hexadécimal qui fonctionne à partir d'un CD ou d'une disquette de boot (vous ne pouvez pas modifier la librairie tandis que Windows fonctionne) et modifier manuellement les bytes qui contiennent la chaîne d'identification "MSFT 5.0", représentés par les valeurs hexadécimales 4d53465420352e30.

En exploitant le protocole DHCP, les personnes mal intentionnées parviennent tout de même à vous identifier...

Là encore, OSfuscate vous vient en aide : vous trouverez en effet le programme "dhcpcsvc patcher.exe" spécialement conçu à cet effet.
Néanmoins désactivez la fonction de restauration du système de Windows. Sinon, vous retrouverez la dll non modifiée au redémarrage. Le programme copie le fichier original dans un nouveau fichier appelé patched-dhcpcsvc.dll, que vous pourrez renommer et substituer à la dll originale en démarrant le PC à partir d'un CD bootable, tel que BartPE contenant des outils pour lire et écrire sur le système de fichiers NTFS.
Dernier point : toute modification apportée à votre système est à vos risques et périls. Si quelque chose tournait mal, inutile de vous en prendre au journaliste (ou encore au programmeur d'OSfuscate) !

ANATOMIE D'UN MALWARE

Un malware décortiqué en profondeur, dans le cadre du Malware Challenge 2008

Nous savons tous ce qu'est un malware: nous avons rarement l'occasion de découvrir en détail son mode de fonctionnement. Idem pour les procédures qui permettent de l'analyser. Nous avons rencontré Anthony Lineberry qui, en participant au Malware Challenge 2008, a documenté son analyse dans les moindres détails, tout en préparant un PDF du résultat, que vous pourrez récupérer à cette adresse: http://blog.flexilis.com/wp-content/uploads/2008/12/malwarechallenge2008.pdf. Quant à son blog, tapez http://blog.flexilis.com/2008/12/the-2008-malware-challenge/ pour y accéder.

:: Outils utiles

Noubliez pas que vous avez affaire à un malware. Vous devez donc absolument le cadrer pour éviter qu'il ne fasse une incursion sur votre PC. Pour ce faire, préparez une machine virtuelle en utilisant VMWare, l'infection sera ainsi limitée au seul PC virtuel. Sur cette machine, vous pouvez par exemple installer Windows XP SP2, assez simple à gérer et relativement léger. Vous aurez également besoin de divers outils, dont certains payants et d'autres libres. Tout d'abord, IDA Pro 5.0, célèbre désassembleur et debugger. Viennent ensuite Windbg, Ollydbg avec son plugin Ollydump, PEiD, ImpRec, ProcessMon et Wireshark. Découvrons ensemble la façon dont ils ont été utilisés.

:: Comportement du malware

Wireshark a détecté que le malware tentait de se connecter à une adresse IRC: il est donc fort probable que le cracker qui l'a créé, le contrôle justement via un canal IRC et que le dit malware contient un bot. Anthony a constaté qu'en installant un serveur IRC local et en paramétrant sa rubrique correspondante dans le fichier hosts, le malware accédait en effet au serveur et se connectait au canal #chalenge à travers le mot de passe happy12. Quant à l'analyse avec ProcessMon, elle a permis de remarquer de nombreux changements au niveau des clés de registre ainsi que la création de deux fichiers: a.bat, un fichier batch qui se charge de créer le second fichier, et 1.reg, qui contient les modifications effectives apportées au registre.
Ces modifications sont généralement dédiées au fonctionnement des connexions TCP de l'ordinateur infecté. Deux clés ont toutefois retenu notre attention, puisqu'elles créent deux rubriques dans \\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\

CurrentVersion\Run et dans \\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices, qui serviront à lancer automatiquement le malware au démarrage du PC domestique.

:: Jeu de cache-cache

Pour ne pas être détecté par les programmes antivirus, l'exécutable du malware est compressé puis décompressé dynamiquement lors de son exécution. Pour pouvoir analyser le programme, il est donc nécessaire d'identifier précisément le packer utilisé (compresseur/encrypteur). D'après PEiD, il s'agirait d'UPX, un packer très répandu: dès lors, en utilisant Ollydbg avec le plugin Ollydump, et après avoir paramétré un breakpoint à la fin de la procédure de décompression, vous pouvez enregistrer le désassemblage effectif de l'exécutable, pour pouvoir l'étudier calmement. ImpRec16 vous aidera à reconstituer les tables des procédures importées des DLL système avec des noms plus faciles à lire, dans la mesure où le programme les charge en mémoire et exécute leur programme en les appelant par leur adresse et non par leur nom.

:: Analyse du désassemblage

Première opération accomplie par le malware, une fois lancé: installer son propre gestionnaire d'exceptions, qui se charge essentiellement des actions de nettoyage et de fermer les connexions. Le fichier a.bat est ensuite créé et lancé; un fichier qui, comme nous l'avons vu, se charge de créer et de lancer à son tour le fichier 1.reg. Après avoir paramétré les clés de registre pour le lancement automatique, place à la création de la connexion sur IRC. Tandis que le mot de passe est toujours le même, le nickname utilisé sur IRC change selon la position géographique, le système d'exploitation utilisé et un nombre aléatoire (par exemple USA[XP]803984): un programme spécifique se charge de cette opération. Après s'être logué, le malware se trouve dans le loop principal: il attend dès lors les instructions du cracker qui se trouve vraisemblablement sur le même canal IRC, prêt à les transmettre.

(Code 1)
La section chargée de la connexion à IRC.

```
ABC0:00403B5B push 7Fh ; size_t
ABC0:00403B5D push offset aTestirc1_sh1xy ; "testirc1.sh1xy2bg.NET"
ABC0:00403B62 push offset byte_47554C ; char *
ABC0:00403B67 call _strncpy
ABC0:00403B6C mov eax, dword_41C7B8
ABC0:00403B71 push 3Fh ; size_t
ABC0:00403B73 push offset aChalenge ; "#chalenge"
ABC0:00403B78 push offset byte_4755CC ; char *
ABC0:00403B7D mov ds:dword_47569C, eax
ABC0:00403B82 call _strncpy
ABC0:00403B87 add esp, 40h
ABC0:00403B8A push 3Fh ; size_t
ABC0:00403B8C push offset aHappy12 ; "happy12"
ABC0:00403B91 push offset byte_47560C ; char *
ABC0:00403B96 call _strncpy
```

:: Contrôle du malware

Pour contrôler le malware, vous devez vous connecter au même canal IRC et transmettre une commande de login avec un mot de passe par défaut. Le mot de passe est entré dans le code du malware, mais ne suffit pas à lui seul pour obtenir l'accès: il faut également provenir d'un nom de domaine spécifique, lui aussi codé dans le programme. Si vous souhaitez essayer de commander le bot, vous devez donc paramétrer le serveur IRC virtuel de sorte qu'il apparaisse comme installé sur ce nom de domaine. Une fois l'accès obtenu, un large éventail de possibilités s'offre à vous. A travers la machine infectée, vous pourrez ainsi lancer un serveur Web, un serveur FTP, des attaques de différents types (DDOS, ping flood, syn flood et autres) vers des noms de domaine ou autres machines en réseau, démarrer un shell distant donnant un accès total à la machine victime, et bien d'autres choses encore. Vu les délais restreints imposés par le Challenge, Anthony n'a pas pu analyser dans le détail toutes les commandes disponibles dans le malware, mais celles listées sont déjà plus que suffisantes pour se faire une idée.

:: Conclusions

Nous avons reporté l'analyse réalisée par Anthony, qui comprend également des fragments de code réel. Pour pouvoir accomplir une analyse toute aussi précise du malware ainsi que de l'ensemble du software qui vous parvient au format compressé, vous devez absolument posséder une bonne connaissance de l'Assembleur des processeurs modernes et avoir une bonne maîtrise des outils utilisés. Vous devez savoir reconnaître le bon outil pour effectuer les tâches nécessaire ou atteindre l'objectif que vous vous êtes fixé. Telle est la base pour étudier des malwares et virus, mais aussi des systèmes de protection, failles de sécurité et, au final, le fonctionnement de l'ensemble du software existant. Et comme le disait Cypher (dans le film Matrix) "à la fin vous vous y habituez: moi, le code, je ne le vois même plus, je ne vois que de belles blondinettes, des brunes, et de longues cuisses"...

Scripta MANENT

L'imprimante laser couleur que vous venez d'acheter pourrait devenir votre pire ennemi...

D'après une légende métropolitaine informatique, Bill Gates aurait réussi à écrire MS-DOS dans son garage, en s'aidant de codes sources dérobés aux programmeurs d'autres entreprises. Le plus drôle dans cette histoire, c'est la façon dont il s'est procuré ces codes sources: en allant les dénicher dans les poubelles ! Info ou intox, on s'interroge tout de même sur la façon dont il a pu reconnaître avec précision les imprimés qui concernaient les codes sources, parmi toutes ces tonnes de paperasses quotidiennement rejetées par les entreprises (surtout à cette époque là !). Aujourd'hui, cette légende devient réalité. En effet, ceux qui souhaitent obtenir des informations à partir d'une impression, n'ont presque plus d'effort à faire, à condition toutefois de savoir où regarder.

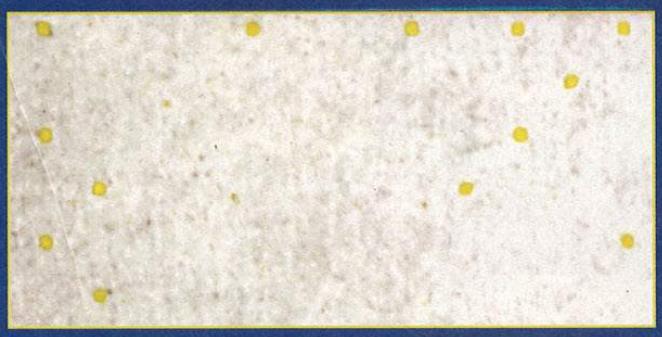
:: Attention faussaires

Ce n'est pas un scoop, mais le sujet reste d'actualité, car les études liées à cette découverte sont en cours. Tout a commencé par l'énorme progrès technologique réalisé par l'informatique au cours de ces dernières décennies: jusqu'au milieu des années 80, les imprimantes étaient des imprimantes à marguerite (elles imprimaient par le biais d'une roue dotée de caractères fixes, appelée justement marguerite, comme pour les machines à écrire) ou dans le meilleur des cas, des imprimantes matricielles (où les caractères étaient formés par les aiguilles d'une tête d'impression qui frappaient l'arrière du ruban encreur pour le pousser sur le papier).Avec quelques centaines d'euros, n'importe qui peut s'acheter une imprimante laser couleur à même de produire des impressions si précises, qu'elles semblent tout droit sorties d'une imprimerie. Et le danger est justement là: de telles impressions pourraient permettre de reproduire du matériel original - même s'il est protégé par des filigranes ou autres astuces - de façon si précise qu'on ne pourrait plus le distinguer de la copie.Une manne pour les faussaires du monde entier ! Qui n'a jamais souhaité imprimer quelques billets avant de sortir avec sa copine ?

:: Marqué à vie

En 2005, l'Electronic Frontier Foundation a réussi à cracker un code imprimé discrètement par les imprimantes laser Xerox sur chaque impression. Il s'agit de microscopiques points jaunes, presque invisibles à l'œil nu sur le fond blanc du papier, et disposés de façon différente selon la date et l'heure d'impression et le numéro de série de l'imprimante ayant servi à cette dernière. Maintenant que vous connaissez leur existence, vous n'aurez aucun mal à dénicher ces points sur les feuilles sorties des imprimantes incriminées. Mais jusqu'à ce qu'EFF les découvre, on ignorait totalement leur signification. Certains pensaient même qu'il s'agissait de couleurs ayant bavé sur la feuille.

Des points jaunes quasi invisibles, pourtant ils sont bien là !



Les voilà, vus au microscope grossissant.

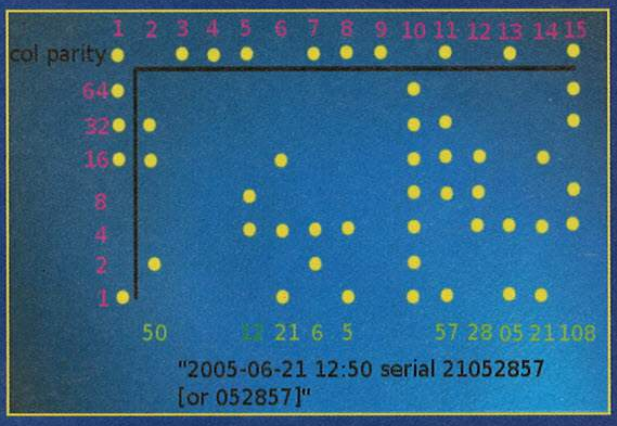
:: A l'affût des points

Si vous ne disposez pas d'un microscope assez puissant, vous pouvez dénicher les fameux points jaunes en appliquant quelques petites astuces. La plus simple exige une source de lumière bleue (aujourd'hui, de nombreux porte-clés avec LED, éclairent en bleu) : en projetant la lumière bleue de biais sur une feuille sortie d'une imprimante laser, vous verrez apparaître de petites taches sombres disposées de façon assez régulière le long de la marge de la page. Eh oui, nos points jaunes sont bien là ! Dans tous les cas, il faut avoir un œil de lynx pour les voir, dans la mesure où ils sont vraiment tout petits. Vous pouvez par ailleurs vous aider de la technologie: si vous disposez d'un scanner haute résolution (autour de 4 800 dpi de préférence pour pouvoir agrandir l'image de façon adéquate, tout en restant nette), vous pouvez reprendre l'impression au format électronique et la transférer ensuite dans un programme de PAO. Là, en séparant les trois canaux de couleur RGB et en n'analysant que le canal bleu sans oublier de zoomer, vos petits points devraient apparaître sous la forme de points sombres.

:: Déchiffrons-les !

EFF est parvenue à identifier très précisément la signification de certains de ces points jaunes, selon le schéma que nous allons dès à présent déchiffrer. Les points sont disposés en matrice, un rectangle de 15 bytes correspondant chacun à 8 bits, dont seuls 7 sont pris en compte, le dernier étant le bit de parité. En les reportant sur un graphique, vous aurez les 15 bytes sur l'axe X, et les bits de chaque byte sur l'axe Y. Vous pourrez lire facilement le contenu du code, une fois que vous connaîtrez sa signification. Le schéma doit être lu de droite à gauche. On trouve dans l'ordre:

- **byte 15**: inconnu, souvent à 0, mais constant pour chaque imprimante ; il pourrait être lié au modèle ou à la configuration de cette dernière ;
- **byte de 14 à 11**: le numéro de série de l'imprimante, unique et constant pour chaque imprimante ;
- **byte 10**: séparateur, tous ses bits sont toujours paramétrés et il semblerait qu'il ne contienne aucune information ;
- **byte 9**: non utilisé ;
- **byte 8**: année sans le siècle (2009 sera donc représenté par un byte de valeur 9) ;
- **byte 7**: mois où la page a été imprimée ;
- **byte 6**: jour où la page a été imprimée ;
- **byte 5**: heure de l'impression (il pourrait s'agir de l'heure UTC mais aussi d'une heure mal paramétrée dans l'imprimante) ;
- **byte 4 et 3**: non utilisés ;
- **byte 2**: détail de l'impression ;
- **byte 1**: a les bits de parité de rang.



La table de décodage dénichée par EFF.

Si vous trouvez ces points jaunes dans votre imprimante, alors vous ne serez plus sans ignorer que celui qui récupérera votre impression pourra remonter jusqu'à son auteur, à travers le numéro de série indiqué. Si vous les dénichez, vous pouvez décoder leur signification à l'aide d'un simple script mis à disposition par EFF à l'adresse suivante: http://w2.eff.org/Privacy/printers/docucolor/. Il est clair que la traçabilité de vos impressions dépend également d'autres facteurs: il faut forcément avoir un document, comme une facture ou un bon de tout type, pour savoir que ce modèle précis d'imprimante est en votre possession. La situation est donc bien plus dangereuse pour une grande entreprise que pour un particulier, mais attention, car on ne sait jamais...

Vous trouverez la liste des imprimantes testées par EFF à l'adresse http://www.eff.org/Privacy/printers/list.php, avec les résultats correspondants. Ne pas trouver de points jaunes ne signifie pas pour autant que l'on est à l'abri: à l'adresse http://cobweb.ecn.purdue.edu/~prints/, vous trouverez des informations sur d'autres techniques appelées "printer forensics" qui permettent de retrouver la trace d'une imprimante à partir d'une simple impression.

WEB MARKET

Comment la folie commerciale s'est-elle emparée du Net ?

On nous a récemment offert un vieil ordinateur portable peu performant, pour voir si nous pouvions en tirer quelque chose. Après avoir identifié le modèle exact, nous avons lancé le navigateur et tapé la marque et le sigle, à la recherche d' informations supplémentaires.

:: Achetez-moi, je suis à vendre

Rien. Les deux premières pages de Google étaient bourrées de liens vers des sites vendant des batteries et mémoires de rechange pour ce type d'ordinateur. Ce n'est qu'en troisième page seulement, à moitié caché parmi les autres sites, que nous avons fini par dénicher un lien vers une page du service d'assistance clients du fabricant, où nous avons pu trouver les informations dont nous avions besoin. Mais pourquoi diable ce site n'est-il pas apparu en premier dans notre recherche ? Internet ne devrait-il pas représenter la principale source d'informations ? Quelle question ! En réalité, c'est l'esprit commercial qui a conquis le Web ! L'ennui c'est que Google tout comme les autres moteurs de recherche sont atteints par ce phénomène: seuls des liens à but commercial apparaissent au début de la recherche et bien en vue des internautes. Le reste des informations arrive bien après.

:: Un peu d'histoire

A l'aube du Web, les informations disponibles online étaient limitées. En général, il suffisait d'accéder au site souhaité et d'y rechercher les infos en feuilletant les menus internes. Mais le Web s'est développé très rapidement. De vieux sites rendent l'âme, de nouveaux sont créés chaque jour et les informations changent d'emplacement ou de forme et, malheureusement, finissent parfois par être oubliées car obsolètes. Dans ce marasme de changements, on a donc songé à créer des systèmes d'indexation pour guider les recherches. Ainsi sont nés les premiers moteurs de recherche qui, au départ, n'étaient que de simples répertoires (bases de données de sites remplies le plus souvent manuellement suivant les indications). Ce système n'a fonctionné que peu de temps: les informations à cataloguer étaient considérables et les ressources (à savoir temps et capacité de travail) trop peu nombreuses.
La solution a donc consisté à automatiser le plus possible le processus, en développant des programmes appelés spiders. Un spider (araignée en anglais) n'est rien d'autre qu'un robot, un software qui fonctionne en toute autonomie, qui part d'une adresse donnée et parcourt tous les liens qu'il trouve, en cataloguant

dans une base de données le contenu des pages rencontrées. Lorsque vous effectuez une recherche sur le Web, vous accédez aux informations entrées dans la base de données du moteur justement par le biais de ces programmes.

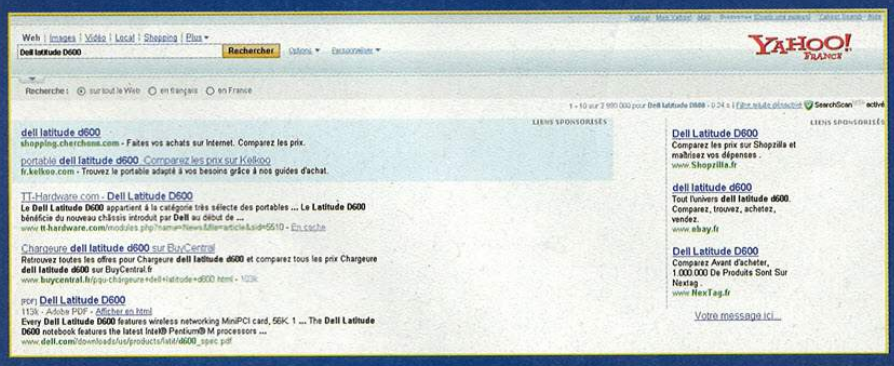
:: L'approche actuelle

En réalité, il ne s'agit pas d'une réelle nouveauté: j'ai un espace qui permet à ceux qui naviguent de trouver un site parmi des millions, pourquoi ne pas faire payer les entreprises pour que leur site s'affiche parmi les premiers résultats de recherche ? Sur le plan commercial, c'est une idée géniale, mais la "supercherie" a vite été découverte. Il semblait en effet impossible que chaque recherche ramène toujours à des sites commerciaux et néglige les approfondissements sur les termes recherchés. Sous la pression du public et des autorités, les Google, Yahoo, Altavista et autres ont donc dû désigner clairement les sites publicitaires (dans Google, ces sites sont affichés sur un fond coloré et une mention indique qu'il s'agit de "liens commerciaux"). On continue de trouver des pages et des pages de liens vers des sites commerciaux, et les informations qui nous intéressent sont souvent reléguées au second plan.

:: Des requins parmi les navigateurs

Les moteurs de recherche ont sans doute commis l'erreur d'avoir "donné le La" à la transformation du Web en un grand supermarché en ligne: sur le Web on gagne de l'argent, et même pas mal ! La prolifération de sites commerciaux s'effectue donc à un rythme bien effréné que celui des sites d'information pure. Si les moteurs de recherche se chargeaient auparavant d'exalter les sites commerciaux dans les résultats, à présent ce n'est plus la peine, car ils sont tellement nombreux que les spiders doivent en passer des milliers avant de trouver un site d'information. Il est logique que leur base de données regorge de sites qui tentent de vous vendre l'élément que vous avez cherché et non de vous informer sur votre recherche. Et les spiders ne font rien d'autre que leur métier: ils parcourent le Net et cataloguent ce qu'ils trouvent.

Nous avons recherché un modèle de PC portable pour trouver des informations sur sa structure et le service d'assistance du fabricant, mais nous n'avons pas eu de chance...



Avec Yahoo, la chance nous sourit davantage: nous avons toujours des liens sponsorisés au début des résultats, mais aussi le lien vers ce qui nous intéresse.

:: Défendez-vous

Inutile de rester passif face à cette tendance commerciale du Web, à moins d'être réellement intéressé par l'achat d'un bien. Il existe des techniques de recherche qui vous permettent de filtrer les résultats obtenus aux contenus purement commerciaux. Et mieux vaut les connaître si vous ne souhaitez pas devenir des zombies de la carte de crédit. Tout d'abord, mémorisez les commandes que vous pouvez entrer dans le champ avec les termes à rechercher, pour limiter et filtrer le plus possible les informations affichées. Le signe moins: si vous l'insérez immédiatement avant un mot, tous les sites qui le contiennent seront écartés.

Commencez par varier les sources de vos recherches en fonction des éléments recherchés: pour des informations de culture générale, mieux vaut partir de Wikipédia et suivre, à la limite, les liens externes proposés. Le Web est fait de personnes qui le parcourent et le peuplent quotidiennement, et non par des entreprises commerciales et des robots. Si vous recherchez la solution à un problème spécifique, cherchez-la dans un newsgroup et non sur le Web, vous aurez plus de chance de trouver quelqu'un qui l'a déjà trouvée avant vous...

MOTEUR, ÇA TOURNE

Réalisez d'excellents films en dompant les moteurs graphiques des jeux vidéo ! Voici comment procéder...

Le "hacking" peut être interprété de nombreuses façons, mais le principe de base reste le même: modifier un objet ou une technologie, et lui faire faire une action pour laquelle il n'a pas été développé à l'origine. Un "simple" jeu vidéo peut ainsi être modifié pour créer un film de qualité. Cette technique s'appelle le "Machinima", un mot-valise formé à partir de "machine" et de "cinéma". Elle consiste à intervenir sur les technologies qui donnent vie à votre jeu préféré, pour le commander dans tous ses aspects et réaliser des films dignes d'Hollywood. Modèles 3D, niveaux, animations, sons, musiques... sont quelques-uns des éléments prêts à être recyclés dans votre production cinématographique. Et ce, sans compromettre la qualité, puisque la définition graphique et sonore des

Si vous n'avez pas le temps de chercher le Body Shop sur www.lessims2.fr, cliquez sur Téléchargements et rerchez le fichier à partir du moteur de recherche du site

tous derniers titres n'a rien à envier à celle de la télé et du cinéma. Si vous souhaitez donc devenir un réalisateur confirmé, mais que vous n'avez pas un sou en poche, suivez ces instructions pour exploiter un jeu vidéo à la fois remarquable et répandu dans le monde entier, j'ai nommé The Sims 2. Amusement garanti !

:: Etape 1: jouez-y !,

Avec plus de 100 millions de copies vendues, dans ses différentes versions, The Sims est le jeu PC le plus répandu de tous les temps. Son second volet dispose entre autres d'un moteur graphique (à savoir l'ensemble des fonctions qui calculent et affichent l'image du jeu) digne de respect et, surtout, largement modifiable. Pour bénéficier des fonctions machinima du chef-d'œuvre de Will Wright (créateur également des séries Sim City et de Spore), vous devez tout d'abord connaître le jeu. Donc, tous à vos souris et vos claviers ! Allez-y, testez-le encore et encore... Pour commencer, créez un groupe de personnages qui représentera votre «cast». Pour ce faire, utilisez le Body Shop: si vous avez installé la version complète de The Sims 2 sur votre ordinateur, lancez-le en sélectionnant Démarrer/Tous les programmes/EA Games/The Sims 2/The Sims 2 Body Shop. Dans le cas contraire, téléchargez-le, gratuitement sur le site suivant: **www.lessims2.fr**.

Si vous n'avez ni le temps ni l'envie de chercher le Body Shop sur **www.lessims2.fr**, cliquez sur Téléchargements et recherchez le fichier à partir du moteur de recherche du site.

Après avoir créé quelques personnages, voici venu le moment de passer au jeu à proprement parler: si vous ne l'avez pas encore achetée, procurez-vous également l'extension Nightlife (vous la trouverez à prix réduit dans plusieurs magasins online). Elle n'est certes pas obligatoire pour faire du machinima avec The Sims 2, mais elle étend pas mal les possibilités cinématographiques du titre.

Après avoir créé votre cast, et vous être quelque peu familiarisé avec le jeu, créez également votre «set» virtuel. Lancez le titre en sélectionnant Démarrer/Tous les programmes/EA Games/The Sims 2/The Sims 2 et, à partir du menu principal, cliquez sur Choisir un quartier où jouer. Faites défiler la liste affichée et cliquez sur Choisir un quartier personnalisé. Puis, cliquez sur le scénario de votre choix, en spécifiant les paramètres manquants, tel que le nom et Sélectionnez un terrain (Vert ou Désert). Après avoir créé le fond du set, placez-y un premier bâtiment. Vous pouvez "l'acheter", en appuyant sur la touche F2 et en sélectionnant celui que vous souhaitez, ou encore le construire. Dans le second cas, après avoir appuyé sur F2, sélectionnez Terrains vides puis la dimension du terrain (le terrain moyen fera très bien l'affaire). Dès lors, place à l'imagination, en exploitant les outils mis à disposition par l'interface, pour modifier le terrain du lot et y construire un grand bâtiment. Comme premier set, un bâtiment avec quatre murs, un plancher, une porte et quelques fenêtres, fera largement l'affaire.

:: Place au hacking

Une fois votre cast et vos sets créés, vous êtes prêt à modifier The Sims 2 pour le transformer en un puissant outil de création de machinimas. Quittez le jeu et, à partir de Windows, allez dans le sous-dossier Programmes/EA Games/The Sims 2/TSData/Res/Config. Dès lors, ouvrez le fichier globalProps.xml à l'aide du Bloc-notes ou d'un éditeur de texte. Si vous utilisez Windows Vista, du fait des paramètres de sécurité, vous serez peut-être obligé de copier le fichier ailleurs pour le modifier, et donc de le recopier dans le sous-dossier, en remplaçant l'original (dans ce cas, créez une copie de sauvegarde). Cherchez la chaîne:

```
<AnyBoolean
key="allowCustomContent"
type="0xcba908e1">true</
AnyBoolean>
```

Sous cette dernière, ajoutez la chaîne:

```
<AnyBoolean key="testingCheatsE
nabled" type="0xcba908e1">true</
AnyBoolean>
```

Et enregistrez le fichier. En fait, vous venez d'activer le mode "cheat" de The Sims 2. Lancez le jeu, téléchargez le quartier (votre "set") créé juste avant et, à partir de la console de jeu, appuyez sur la combinaison de touches Ctrl+Shift+C. Vous ferez ainsi apparaître une ligne dans la partie supérieure de l'écran. Tapez-y l'instruction: et appuyez sur Entrée.

```
boolProp enablePostProcessing true
```

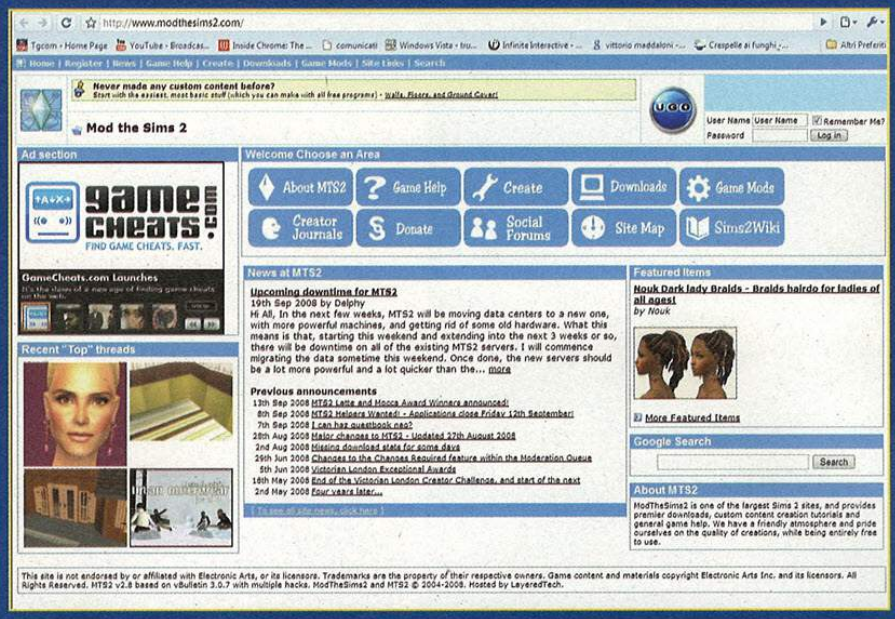
Appuyez à nouveau sur la combinaison de touches Ctrl+Shift+C, tapez la commande, et appuyez sur Entrée.

```
boolProp testingCheatsEnabled true
```

Suivez la même procédure pour entrer d'autres commandes:

```
boolProp useEffects false
AllMenus On
moveObjects On
Aging Off
```

Scènes nocturnes ou danse langoureuse ? L'extension Nightlife est vivement conseillée !



www.modthesims2.com est le principal site dédié au modding et hacking du chef-d'œuvre de Will Wright.

Une fois ces "cheats" activés, quittez le jeu et allez vous enregistrer, gratuitement, sur le site www.modthesims2.com.
Puis, téléchargez le fichier TS2Studios0_4.BETA.zip, que vous trouverez sur le lien http://modthesims2.com/showthread.php?t=100738. Il s'agit de The Sims 2 Studio, qui ajoute des fonctionnalités de studio de cinéma au jeu. Ouvrez le fichier téléchargé et extrayez le fichier TS2Studios04B.package, dans le dossier documents/EA Games/The Sims2/downloads. Lancez The Sims 2 et préparez-vous à tourner votre premier film machinima. Tout d'abord, créez une "famille", en utilisant les personnages du cast et en associant leurs caractéristiques souhaitées, comme les Aspirations. Une fois cette opération achevée, téléchargez votre "quartier" et placez à l'intérieur du set les différents membres de votre "famille".
Eunsuite, en suivant la même procédure, ajoutez au quartier un second bâtiment et d'autres acteurs virtuels à l'intérieur: vous l'utiliserez comme "réservoir" d'acteurs prêts à être introduits dans le set.
A la fin, vous vous retrouverez avec un quartier composé de deux bâtiments, dont l'un est le set à proprement parler, avec des acteurs à l'intérieur de chacun. Maintenant, ajoutez un peu d'argent au compte virtuel de chaque bâtiment: il suffit d'entrer à l'intérieur, d'appuyer sur la combinaison de touches Ctrl+Shift+C, de taper motherlode et d'appuyer sur Entrée.
Puis, allez à l'intérieur du bâtiment-set, appuyez sur F5, sélectionnez Vidéo/Niveau de performances et assurez-vous que Cacher les objets soit paramétré sur Off. Retournez à la console de jeu et, à partir de là, appuyez sur Ctrl+Shift+C. Tapez letterbox 0.2 et appuyez sur Entrée. Puis, tapez exit et appuyez à nouveau sur Entrée, pour fermer la fenêtre d'insertion des commandes.

:: Quelques mouvements de caméra

Le moment est venu de désactiver le son: l'enregistrement vidéo sera ainsi plus fluide et vous pourrez y insérer un doublage "sérieux" une fois le film réalisé.
A partir de la console de jeu, appuyez sur F5 et cliquez sur Options du visuel. Dans Acquisition du son des films, cochez la case Off et, pendant que vous y êtes, paramétrez Temps max d'enregistrement des films sur une valeur supérieure aux 60 secondes par défaut, par exemple 600. Appuyez sur F1 et retournez au jeu.
Une fois dans le set, appuyez sur la touche P, pour mettre la partie en pause, et positionnez les acteurs et objets divers et assortis. Une fois cette opération achevée, appuyez sur V pour lancer les "prises de vue". Déplacez la caméra (W, A, S ou D): un "mouvement de caméra" sur une scène fixe, c'est plutôt pas mal comme première expérience. A la fin, appuyez à nouveau sur V et enregistrez le film réalisé.

Une façon simple et rapide de se faire de l'argent. Uniquement valable sur The Sims 2...

Voici le format "letterbox" activé, un format qui se marie bien avec les nouveaux téléviseurs panoramiques 16/9.

Avant de commencer les prises de vue, mieux vaut faire un casting pour sélectionner acteurs et figurants.

Pour donner du mouvement à l'ensemble, retirez le mode pause et filmez vos acteurs tandis qu'ils s'animent. Dans la mesure où ils sont également gérés par l'intelligence artificielle, certaines scènes risquent de devenir trop "spontanées" et quelque peu hors contrôle: mais au fond, ils vivent leur vie, non ? Dans ce cas, pas de panique: à partir du film obtenu, vous couperez les scènes inadaptées ou superflues, à l'aide d'un software de montage vidéo.

:: Tous à vos commandes

Il existe un autre moyen pour contrôler sans hésitation les Sim-acteurs. Vous aviez créé auparavant deux bâtiments avec deux casts distincts y résidant.
A présent, ajoutez un troisième bâtiment, en le construisant sans porte ni fenêtre: vous l'appellerez donc "set-prison". En maintenant enfoncée la touche Shift, cliquez ensuite sur la boîte aux lettres correspondante, et sélectionnez Invite all Neighbours.
Une fois que les acteurs arrivent devant le set-prison, appuyez sur la touche F2 (Mode achat), appuyez sur la combinaison de touches Ctrl+Shift+C et activez le cheat MoveObjects true.
Une fois activé, cliquez sur un acteur et "glissez-le" à l'intérieur du set-prison. Puis, en maintenant enfoncée la touche Shift, cliquez à nouveau sur l'acteur que vous venez de déplacer et, dans le menu affiché, sélectionnez MAKE SELECTABLE. A partir de ce moment là, l'acteur passe entièrement sous votre contrôle.
Pour étendre les actions mises à disposition de vos acteurs, utilisez également The Sims 2 Studio, installé précédemment. A partir de la console de jeu, et avec un acteur sélectionné, appuyez sur F2 (Mode achat) ; et cliquez ensuite sur Hobby. En faisant défiler la liste d'objets, vous apercevrez une "boîte noire".
Double-cliquez dessus et placez-la ensuite dans un coin du set, caché si possible de la caméra. Passez au Mode vifs et cliquez sur la boîte.
Un menu complet s'affichera ainsi, rempli d'animations alternatives prêtes à rendre votre film machinima encore plus captivant.
Testez également leur côté spectaculaire: des larmes désespérées aux éclats de rire insouciants, tout y est pour satisfaire même les réalisateurs les plus exigeants.
Pour effectuer de nouvelles prises, suivez la procédure déjà vue: un "clap", même virtuel, qui pourrait bien vite vous ouvrir les portes d'Hollywood !

The Sims 2 Studio, ajoutez de nombreuses animations excitantes pour votre machinima...

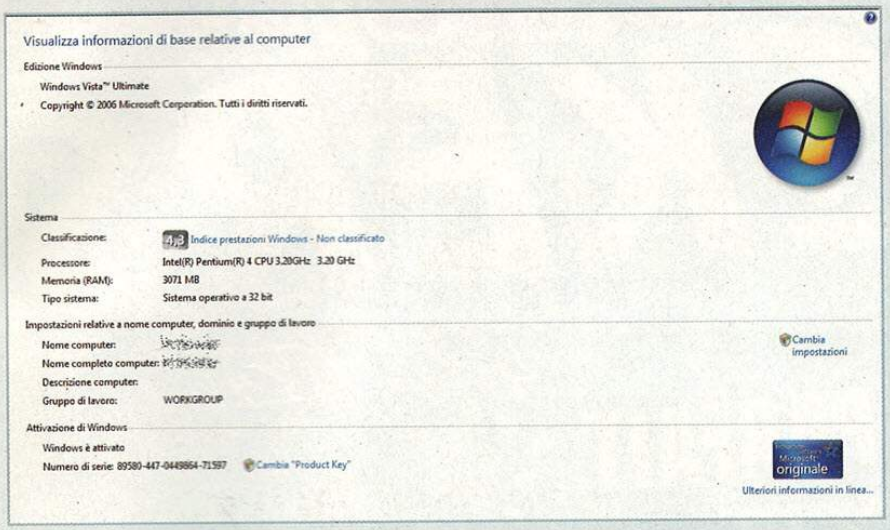
GOOGLE PHONE: UN HACK PARFAIT !

A quelques semaines de la sortie du "G1", nombreux s'en sont donnés à cœur joie pour dénicher ses fonctions et procédures ! Attention, ça va décoiffer !

Une certaine confusion règne sur le T-Mobile G1, également appelé "Google Phone". Une confusion liée justement à son nom: le bon, c'est le premier, tandis que le second ne reflète pas totalement la réalité puisque ce téléphone N'a PAS été développé par Google, mais par High Tech Computer corporation. Google s'est en revanche chargé de développer le software qui anime le dispositif, autrement dit l'Android tant clamé. Un système d'exploitation pour mobile qui n'est autre qu'une petite merveille: basé sur Linux (ouah !), il est totalement ouvert et adaptable aux dispositifs portables les plus variés. Pourtant la version installée dans le G1, celle de départ, a quelque peu péché par présomption, en manifestant de nombreux bugs qui, par chance, mise à jour après mise à jour, ont diminué en nombre ainsi qu'en termes de gravité. Bien qu'il soit difficile d'élaborer des procédures de hacking fonctionnant sur n'importe quel G1 (elles dépendent énormément de la version installée), nous avons souhaité nous y essayer... En voici deux qui ont déjà fait couler beaucoup d'encre !

::Installer les applications

Voyons comment installer des applications tierces sur le téléphone d'HTC. On sait que bien qu'Android soit un système d'exploitation ouvert, l'ajout de softwares extérieurs est à la merci des seuls développeurs. Et de ceux qui ont le SDK entre leurs mains, à savoir l'environnement de développement. La première étape consiste en effet à télécharger le SDK, que vous trouverez à l'adresse suivante: code.google.com/android/intro/installing.html. Après avoir téléchargé le fichier zip qui le renferme, extrayez son contenu en notant les dossiers de destination. Essayez de conserver ceux par défaut, notamment les sous-dossiers tools et samples. Si vous utilisez Windows, sélectionnez dès à présent Start/Computer et, à partir de cette fenêtre, cliquez en haut, sur Propriétés système. A gauche cliquez sur Paramètres système avancés. Puis, cliquez



Cet article évoque certes l'utilisation du SDK dans Windows, mais le site dédié liste également les procédures pour Mac et Linux

sur Variables d'environnement. Dans la section Variables système, faites défiler la liste et double-cliquez sur Path. A la fin de la chaîne Valeur variable, ajoutez tools/. Cliquez sur OK sur toutes les fenêtres, pour les fermer. Une fois le SDK installé, téléchargez les drivers qui permettront de brancher le G1 au port USB de votre ordinateur. Vous les trouverez directement sur http://dl.google.com/android/android_usb_windows.zip. Une fois cette opération achevée, passez à votre G1 tant adulé: à partir du menu, sélectionnez Settings puis Application settings, et activez Unkwown sources. Puis, toujours à partir de Settings, sélectionnez Application settings puis Development. A partir de cette fenêtre, activez la rubrique USB debugging. Branchez votre téléphone à votre ordinateur, par le biais d'un câble USB et ce, uniquement après avoir effectué ces opérations. Puis, installez les drivers que vous aviez préalablement téléchargés. A présent, tout est prêt pour pouvoir installer une application quelconque sur votre G1. Le téléphone d'HTC est reconnu par Windows comme un "ADB Interface", ou un nom du même style. Les applications pour Android sont au format APK. Pour les installer, il vous suffit de copier le fichier souhaité dans un dossier du disque dur. Puis, directement à partir de votre mobile, lancez une commande du type adb install c:\dossier, où c:\dossier indique le parcours et le dossier refermant le fichier APK.

:: Le "fameux" bug

Le G1 a déjà défrayé la chronique des hackers après avoir fait l'objet de l'un des plus gros bugs de ces derniers temps. Un bug actif jusqu'au firmware version RC29, tandis que les versions suivantes l'ont, par chance, corrigé. Pour connaître la version installée sur votre téléphone, sélectionnez Menu/Settings/About phone, à partir du menu principal. Observez ensuite la chaîne qui suit Build number. Si elle se termine par RC29, ou une version inférieure, alors votre dispositif est encore "sensible" au bug. Comment ça marche? Suivez les instructions suivantes:

premere RETURN

digitare REBOOT

premere di nuovo RETURN

Le téléphone, comme par magie, interprète la chaîne comme une commande système, en relançant le software du dispositif. Ce n'est là qu'un exemple des conséquences dévastatrices de ce genre de bug. Les hackers avertis voudront connaître la raison de cette erreur qui réside dans le software du G1. Il s'agit de quelques lignes de code contenues dans /init.rc. Et plus précisément :

```
## Daemon processes to be run by init.
##
service console /system/bin/sh
    console
```

Vu ? Quatre lignes de code laissées par erreur activent une console qui intercepte les textes écrits comme des commandes (en admettant que les textes correspondent effectivement à des commandes !).

A la commande reboot que l'on vient de voir, ajoutez par exemple cat. Cette opération désactive le shell, et donc le bug jusqu'au redémarrage suivant de la machine. Un moyen efficace pour limiter d'éventuels dommages, mais déconseillé si vous avez l'intention de "tester" encore la première version officielle d'Android sur un dispositif commercial. Un début qui, certes, laisse à désirer en termes de qualité, mais qui nous permet de nous adonner à notre activité favorite : le hacking... Et qui sait, sans doute reviendrons-nous prochainement sur le sujet avec quelques instructions avancées !

Le "G1" sortira en France début 2009 (en mars/avril semble-t-il).

TOUS LES MEILLEURS SOFTWARE 100% utile

HACKERS MAGAZINE

L'ORDINATEUR PARFAIT:
NETBOOK HACKER VERSION

TOP 100 BY HM
LES MEILLEURS PROGRAMMES HACKING

EN KIOSQUE

M 04586 - 25 - F: 2,00 € - RD
BELGIQUE/LUXEMBOURG: 2.4 € - CANADA: 3.25 $
SUISSE: 4 CHF - TOM: 490 CFP - DOM: 2.5 € - MAROC: 25 MAD
WLF PUBLISHING