PIRATE INFORMATIQUE
N°5
JUILLET/AOÛT 10

PIRATE INFORMATIQUE

2€ SEULEMENT

EXCLUSIF

NOUVELLE TECHNIQUE DE PIRATAGE DES CARTES BANCAIRES !

SON INVENTEUR PARLE D'UNE VÉRITABLE BOMBE. LES BANQUES ESSAIENT D'ÉTOUFFER L'AFFAIRE

HACKING

TABNAPPING : LA NOUVELLE MENACE PHISHING

KEYLOGGERS : COMMENT ÇA MARCHE ? COMMENT S'EN PROTÉGER ?

VOTRE VOITURE AUSSI PEUT ÊTRE PIRATÉE !

PIRATAGE

SHAREAZA : L'INTERVIEW

FIREFOX EN FEU AVEC FIRETORRENT

L'USURPATION D'IDENTITÉ EST À LA MODE

POKER ET PARIS EN LIGNE

TRICHE, FRAUDE ET VOLS DE COMPTES : ALL IN POUR LES PIRATES !

100% INFOS 0% INTOX !

HACKING, COMPTES CRACKÉS, TÉLÉCHARGEMENTS, ANONYMAT, DÉBRIDAGE, MOTS DEPASSE, GÉNÉRATEUR DE CLÉS WIFI

BEL : 3 € - DOM : 3,90 € - CAN : 5,95 $ cad - POLAS :
L 12730 - 5 - F: 2,00 € - RD

LE MAGAZINE NOUVELLE GÉNÉRATION

EN KIOSQUE

NOUVEAU !

PIRATE INFORMATIQUE

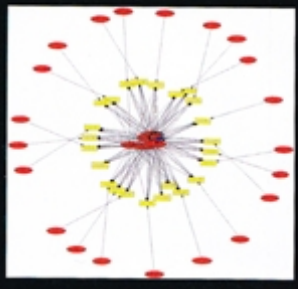
100% LIBRE

Pirate informatique#5 - Juillet/Août 2010, une publication du groupe ID PRESSE (www.idpresse.com) - Directeur de la publication : David Côme - Rédacteur en chef : Benoît Bailleul - Collaborateur : Damien Bancal, Malik Brahmi.

IPAD DE QUOI

Victime de son succès, l'iPad est déjà victime de problèmes de sécurité. L'opérateur exclusif sur le sol américain (AT&T) a récemment révélé que près de 114 000 adresses email d'utilisateurs avaient été piratées. C'est d'autant plus amusant que parmi ces personnalités figurent des personnes connues comme des stars du petit écran ou des chefs d'entreprise. En utilisant les identifiants associés à chaque carte SIM intégrée à un iPad 3G, ces hackers ont réussi à voler des milliers d'adresses e-mails accolés à ces identifiants personnels sur le site de l'opérateur mobile américain : facile. Même s'il faut bien sûr obtenir le mot de passe pour que la boucle soit bouclée, les pirates vont bien trouver dans le lot des génies qui auront choisi «god» ou «jesus». Pas de chance pour Apple puisque quelques heures après la présentation par Steve Jobs du dernier iPhone, un hacker s'est vanté d'avoir «jailbreaké» (débloqué) l'appareil ! Attention, cette prouesse est à mettre entre parenthèses puisqu'il ne s'agit que d'une version bêta de l'OS. On espère néanmoins que le système d'exploitation subira des retouches avant la sortie de l'appareil en France...

Location d'un bot pirate à l'heure



Vous connaissez les botnet ? Ces réseaux de PC contaminés par un Trojan ou un backdoor permettent à des pirates de lancer des attaques DoS (Denial of Service : une opération qui consiste à saturer de requêtes un site pour le faire exploser) ou de s'enrichir avec du spam. Si vous voulez vendre du Viagra contrefait ou attaquer le site d'un concurrent, il est possible de louer ces botnets aux criminels qui les ont créés. Une récente étude menée par Verisign a permis d'estimer le coût moyen de location. Même si les prix varient en fonction de la tête du client et du parc de PC contenus dans ce réseau, ce genre de service coûte en moyenne 9 $ l'heure ou 67 $ pour la journée. Il n'y a bien sûr aucune garantie et pire, les choses peuvent se retourner contre vous puisque bien souvent les pirates proposent aux victimes de payer pour pouvoir se venger. Les seuls à s'enrichir sont encore une fois les «black hat»...

Ils font le bonheur des pros

Caméras cachées, micros invisibles... Désormais, grâce à Internet, le matériel d'espionnage professionnel est exposé à la convoitise de tous. James Bond, François Mitterrand et Richard Nixon les auraient réclamés !

Anti-KGB

Cet appareil est un appareil professionnel qui détecte les microphones clandestins, les émetteurs portables et les caméras miniatures. Il est, également, capable de détecter les réseaux WiFi, les connexions Bluetooth, etc. Grâce aux LED multidirectionnelles, vous savez dans quelle direction chercher si l'appareil détecte des transmissions suspectes.

Prix : 169 €

www.1discounter.com

Un coca ?

Le «soda espion» est le plus petit appareil en haute résolution, temps réel, caméscope numérique jamais produit. Très facile à utiliser, un bouton placé sous la canette permet d'enregistrer discrètement toutes les preuves instantanément. Les enregistrements sont stockés dans une mémoire interne de 4 Go, avec une autonomie de 2 heures d'enregistrement en continu. La batterie interne se recharge via la connexion USB.

Prix : 129 €

www.1discounter.com

Un scientifique s'injecte un virus... informatique !

Étonnante et inquiétante, telle est la découverte du docteur Mark Gasson, chercheur à l'Université de Reading. Il a réussi à introduire un virus informatique dans la puce RFID qu'il s'était greffé dans la main. Il démontre ainsi que les implants, tout comme les ordinateurs, sont vulnérables à des cyber-attaques. La médecine s'inquiète quant à de possibles attaques contre des pacemakers par exemple. À la lumière de cette découverte, devons-nous accepter les puces sous cutanées, au risque de voir les machines prendre leur revanche sur l'Humanité ?

«Hackers Wanted» hacké !

Sam Bozzo n'aura plus à se plaindre que son documentaire, sur le monde des hackers, ne trouve pas de distributeurs. Son œuvre a été piratée et mis à la disponibilité du public sur le réseau P2P. Espérons que le succès soit au rendez-vous pour faire connaître un peu plus le monde fascinant du hacking. Entre criminalité et héroïsme, terrorisme et patriotisme et d'autres valeurs propres à chacun. Vous pouvez le trouver facilement en stream grâce à Google...

HADOPI pipot !

Les envahisseurs débarquent ! Les premières lettres by HADOPI débarquent dans les boîtes mails des «pirates». D'un lyrisme déconcertant, elle vous annonce que *«l'acte frauduleux a été commis tel jour à telle heure avec telle adresse IP»*. N'en riez pas, car vous *«n'avez pas la possibilité de contester le premier avertissement»*. Rassurez vous... cet e-mail est un faux dont le but serait de noyer d'e-mails le Ministère de la Culture. On ne sait toujours pas quand partiront les vrais courriers. Faites nous le savoir lorsque vous en recevrez un !

Vice sisters

Ces jumelles numériques permettent de capturer des vidéos et des photos très facilement. Le modèle CVMU-DC07 est conçu pour tous ceux qui ont besoin de filmer et voir tous les détails (événements sportifs, scènes, surveillance, etc.) et d'enregistrer de la vidéo ou des photos en même temps sur une carte SD. Pour plus de polyvalence, le Long Ranger est livré avec une option de sortie TV permettant la lecture directe de ce que vous avez enregistré sur votre téléviseur.

Prix : 280 €

http://toutpourvous0.surinternet.com

À la trace !

Une balise aimantée très simple à utiliser. Elle est équipée d'une carte SIM Vodafone que vous pouvez recharger en ligne. Mettez-le en marche et placez-le sous le véhicule à surveiller. En mouvement, les positions sont envoyées régulièrement et enregistrées sur le serveur du site vendeur. Il est possible de garder un historique ou de recevoir un SMS ou un email d'alerte quand le traceur franchi une zone géographique définie par vos soins.

Prix : 499 €

www.espion-on-line.com

LimeWire en garde sous le coude

Accusé et condamné aux USA pour permettre l'échange de fichiers illégaux, LimeWire est encore dans la tourmente. La RIAA (Recording Industry Association of America) réclame plus d'un milliard de dollars correspondant à 150 000 dollars par morceau piraté (cela fait donc 6666,6666... titres. Faut-il y voir un signe ?) Les 13 maisons de disque soutenues par la RIAA accusent maintenant la société de mettre ses fonds à l'abri pour éviter d'avoir à payer cette amende record. On a un peu de mal à comprendre l'acharnement contre le Lime Group car LimeWire avait été un des seuls logiciels à proposer un filtre contre le téléchargement de fichiers qui ne bénéficiait pas de l'autorisation des auteurs. De surcroît, LimeWire étant un logiciel libre, d'autre «clone» reprendront le flambeau. Vous connaissez Frostwire ?

Souriez, vous êtes HACKÉS

MSN déchaîne les passions sur la Toile et les personnes qui cherchent à pirater ce logiciel sont légions. Il ne s'agit pas forcément de brigands aguerris mais aussi de gens normaux voulant espionner l'activité de leur proche. Quand ces personnes reçoivent dans leur boîte aux lettres une invitation pour télécharger un outil permettant de pirater soi-même des comptes Windows Live Messenger, ils ne se méfient pas. Pourtant, cet e-mail constitue la première étape d'un plan frauduleux de récupération de données ! En analysant le fichier HackMsn.exe, un bon antivirus reconnaîtra un backdoor, une porte dérobée qui permettra d'ouvrir un accès vers les informations de votre ordinateur : numéros de série des logiciels, mots de passe, etc. Quand il n'y aura plus rien à voler, votre PC ira rejoindre ses petits camarades victimes dans un réseau botnet (plusieurs milliers de PC zombies)... Dans le même genre, des pirates ont réussi à faire passer une belle compilation de malwares et backdoors pour un kit d'installation d'Android. La mode tue.

Sale temps pour les ATM

Vous vous souvenez du passage de Terminator 2 où John Connor s'attaque à un ATM (distributeur de billets) avec une machine électronique ? Et bien ce type d'attaque n'est peut-être plus de l'ordre de la science-fiction ! En effet les 28 et 29 juillet prochains, Jack Barnaby, directeur de recherche chez IOActive devrait expliquer lors de la conférence Black Hat comment un rootkit pourrait permettre d'utiliser différentes failles dans les distributeurs de billets. Déjà l'année dernière, Jack voulait présenter un logiciel capable de lancer des attaques sur Internet contre une marque d'ATM bien connu. Il avait été sommé par son employeur de l'époque (Juniper Networks) d'annuler cette présentation. Le titre de l'exposé ? "Jackpotting Automated Teller Machines". Il n'en fallait pas plus pour que les gens s'intéressent à la «science». Dans le même temps, aux USA, Thor Alexander Morris a réussi à reprogrammer un ATM pour qu'il donne des billets de 20$ à la place de coupure de 1$. En tapant 400 $, il récupérait 8000 $ sans pour autant que son compte soit débité de cette somme. Loin d'être un pirate spécialisé dans les transferts bancaires, ce dernier n'a eu qu'à lire la notice de certains ATM de marque Tranax et Triton. Le mot de passe d'origine permettant d'accéder aux réglages usine n'est généralement pas changé par les commerçants. Trop gourmand, notre petit malin a partagé son secret et le FBI a mis la main sur lui par l'intermédiaire d'un indic... Pas de chance.

LIBRE ET ENGAGÉ

+ CD OFFERT !

VOTRE MAGAZINE Nouvelle Génération

Tabnapping : le phishing 2.0 !

Une attaque phishing standard : un lien dans un email qui redirige vers un formulaire qui reprend exactement le design d'un site que vous connaissez bien (ici Free). En remplissant le formulaire, vous tendez le bâton pour vous faire battre...

À force de parler des cas de phishing, nos lecteurs sont bien informés des risques de telles attaques. Il ne faut pourtant pas sous-estimer les fripons qui sévissent sur Internet. Plusieurs sources rapportent qu'un nouveau type de phishing connaît de plus en plus de succès sur la Toile : le Tabnapping. Comment ça marche et comment s'en protéger ?

Comme tout Internaute prudent, vous faites particulièrement attention aux e-mails frauduleux que vous recevez parfois d'une soit-disant banque ou d'un soit-disant FAI. Vous faites bien puisque comme vous le savez, il s'agit la plupart du temps d'un lien redirigeant vers un faux site où l'on vous demandera toutes les informations nécessaires pour vous escroquer de l'argent. Depuis que ces attaques existent, non seulement les personnes se méfient mais certains navigateurs permettent de repérer ces sites frauduleux (Vous aussi, vous avez aimé la pub pour Windows 7 avec la blonde qui surfe en terrasse ?). Il n'en fallait pas plus pour que des petits malins inventent une nouvelle variante du phishing (ou hameçonnage) : le Tabnapping ou Tabjacking. Si le nom varie d'un site de sécurité à un autre, le but ne change pas : dérober des informations aux Internautes.

Le principe

Derrière ce nom barbare quin'a pas encore de traduction en français (nous proposons «fourbonglerie») se cache une technique qui utilise une méthode nouvelle de surf : nos chers onglets. Avec le Tabnapping, terminé les faux emails qui,

en plus d'être bourrés de fautes d'orthographe, fonctionnaient moins bien au fur et à mesure que les médias relayaient ce genre de piège. Ici, il s'agit de l'exploitation d'une possibilité JavaScript qui permet de changer un onglet sans modifier l'URL (le lien qui apparaît dans la barre d'adresse). En clair, vous cliquez sur une page infectée qui a un peu de mal à se charger. Qu'à cela ne tienne, vous changez d'onglet et reprenez votre lecture. Seulement voilà, la page infectée va se changer en page Gmail, Paypal ou eBay en toute transparence. Dans la plupart des cas, la victime oublie la page qui ne se chargeait pas et tombe sur une fausse page dont le design lui est familier ! Sans réfléchir, la victime entre ses identifiants Gmail ou Paypal et le mal est fait !

Très facile du tomber dans le panneau

Pour mieux comprendre, nous vous invitons à regarder cet exemple totalement inoffensif. Tapez ce lien sur votre navigateur : www.azarask.in/blog/post/a-new-type-of-phishing-attack. Il suffit ensuite d'ouvrir un nouvel onglet (sous Firefox, il suffit de cliquer sur le «+» à côté de l'onglet principal) et de faire une recherche sur Google, par exemple. Alors que toute votre concentration se dirige maintenant vers votre nouvel onglet, l'ancien se transforme discrètement en une page familière (ici une page Gmail). L'Internaute inattentif se dira que son Gmail s'est déconnecté et rentrera ses identifiants (dans notre exemple, il ne s'agit que d'une image mais il est bien sûr possible de réaliser un véritable formulaire imitant l'interface d'une banque ou d'un service Web). Le pire, c'est qu'une fois les informations récupérées, vous serez basculé vers votre vrai Gmail qui n'a jamais été déconnecté ! Pour l'instant, cette technique ne fonctionne que sous Chrome et Firefox et ce, même si l'option «NoScript» est activée.

Un ciblage plus précis

Attention, il est possible de cibler encore plus ce type d'attaque. Par exemple, un Internaute qui n'aurait pas de compte Gmail serait fort surpris de voir une interface Gmail sortir comme ça de nulle part. Le Webmaster du site qui a révélé le problème, Aza Raskin, a conçu un programme qui permet de savoir quel site social utilise le visiteur de son site. Si un méchant pirate dispose d'un site avec un peu de trafic (un site de warez, par exemple), il lui suffit avec un simple JavaScript de déterminer quel utilisateur utilise quel site social. Appelé SocialHistory.js, ce JavaScript utilise une fuite du code CSS (www.azarask.in/blog/post/socialhistoryjs). Vous savez, sans doute, que les navigateurs affichent avec des couleurs différentes les liens visités et les liens qui ne l'ont jamais été. Et bien, ce script utilise cette option pour questionner la victime. Le programme ne permet pas d'avoir la liste complète des liens visités mais il autorise le questionnement. Il suffit alors de demander si le visiteur X a aussi visité Facebook, Paypal, Gmail, etc. À chaque fois, le programme répond par oui ou non. Il suffit de trouver un site fréquemment utilisé pour tendre un piège beaucoup plus «ciblé». Le concepteur du programme explique que ce type de programme, à l'origine utilisé pour adapter une page à un utilisateur (en plaçant des boutons «Facebook» ou «MySpace» sur une page visité en fonction des sites visités par l'utilisateur) peut donc servir à piéger les Internautes. Même si le système n'est pas parfait, Aza affirme que son script connaît un taux de succès de plus de 80 %. Mieux vaut redoubler de vigilance...

Un exemple sans risque...

Usurpation d'identité : quand les victimes deviennent coupables

Très difficile à prouver et relativement peu puni en France, l'usurpation d'identité peut prendre différentes formes. C'est un véritable cauchemar pour les victimes qui sont parfois soupçonnées d'être des délinquants. Quels sont les chiffres relatifs à ce problème, comment réagir et éviter de se faire blouser ?

D'après une étude de YouGov commandé par Verisign (un spécialiste d'infrastructure réseau), 10 % des internautes français ont été victimes d'usurpation d'identité au cours des 12 derniers mois (1). Ce chiffre qui paraît énorme comprend en fait toutes les formes d'usurpation d'identité, y compris la fraude à la carte bancaire. Subtiliser l'identité d'une personne n'est pas si difficile que cela. Il suffit de connaître un nom, une date de naissance, une adresse et le nom des parents de la victime. Grâce à ces premiers éléments et avec un peu d'habilité on peut retrouver d'autres informations comme le numéro de sécurité sociale. Les fraudeurs ne se privent pas pour fouiller vos poubelles ou voler dans votre boîte aux lettres à la recherche de RIB ou de toutes autres informations bancaires.

Allo ? C'est pour un sondage

Le faux sondage téléphonique est aussi un classique. Au début les questions sont d'ordre général puis plus les minutes passent et moins le «sondé» se méfie sur la nature personnelle des questions. Le but est parfois de se faire une «vraie fausse» carte d'identité et de collecter assez d'information pour obtenir un prêt bancaire, des prestations sociales ou pour éviter de payer des amendes. Avec Internet, c'est encore plus facile. C'est incroyable le nombre d'informations qu'il est possible d'obtenir grâce à un réseau social ou un blog. En plus de ces techniques, il faut ajouter le phishing (ou hameçonnage) qui consiste à faire croire à un email émanant de votre FAI ou d'une société que vous connaissez (banque, boutique en ligne, eBay, etc.) pour vous soutirer des renseignements. Chaque année, en France, on recense 213 000 cas d'usurpation d'identité, un chiffre énorme au regard du nombre de cambriolages (150 000) ou de vols d'automobile (130 000). En moyenne, la somme dérobée s'élève à 1 300 € et 25 % des victimes se plaignent de ne pas avoir pas été remboursées. Outre les trous dans le budget ou le traumatisme psychologique (le fait de devoir prouver «être soi-même» y est pour quelque chose !), les conséquences pour les victimes peuvent prendre des proportions désastreuses puisque 15 % d'entre elles ont été frappées d'interdiction bancaire et 13 % ont été assignées devant un tribunal.

Quid de la loi ?

D'après l'article 434-23 du code pénal, le fait de prendre le nom d'un tiers, dans des circonstances frauduleuses et sans l'accord du tiers, est puni de 5 ans de prison et de 75 000 euros d'amende. De plus, le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45 000 euros d'amende. Notez que vous avez un délai de 3 ans pour agir en justice. Prouver sa bonne foi n'est pas une mince affaire puisque la victime ne peut attaquer que s'il y a escroquerie, faux manifeste ou diffamation. En clair, utiliser la boîte mail d'un tiers n'est pas en soi punissable : il faut que le pirate s'en serve pour tromper des personnes ou les injurier. Le projet de loi LOPPSI devrait changer la donne puisqu'il prévoit d'étendre un peu les dispositions liées à ce genre de problème. Même si les usurpations d'identité numérique représentent une partie infime des faits d'usurpation, les cas sont de plus en plus fréquents...

www.securisezvotreidentite.com

Les précautions à prendre

1. Protégez votre ordinateur en installant un antivirus et un pare-feu (ou en paramétrant correctement celui déjà présent sur votre système). Déconnectez-vous d'internet lorsque vous n'êtes pas en ligne et, si vous utilisez un ordinateur portable, créez un mot de passe protégeant l'accès à vos informations.

2. Protégez vos mots de passe. Ne communiquez pas vos mots de passe, modifiez-les souvent et n'en choisissez pas que l'on peut facilement deviner.

3. Assurez-vous que le site Web sur lequel vous êtes est sécurisé. Avant de saisir vos données de paiement sur un site Web, assurez-vous que l'URL commence par https, le « s » signifiant « sécurisé ». Si un site comporte de nombreuses erreurs typographiques ou ne présente aucune information de sécurité, évitez-le.

4. Ne téléchargez pas les pièces jointes et ne cliquez pas sur un lien figurant dans un courrier électronique, à moins que l'expéditeur ne soit une personne de confiance. Ne fournissez jamais d'informations confidentielles par courrier électronique. N'oubliez pas que les sites Web financiers ne vous demanderont jamais de leur communiquer vos noms d'utilisateur, mot de passe, PIN ou toute autre information confidentielle... contrairement aux fraudeurs !

5. Assurez-vous d'utiliser un réseau Wi-Fi sécurisé (le système WPA2 est le minimum). Protégez votre réseau sans fil personnel par un mot de passe et évitez d'effectuer des achats ou de consulter vos comptes en banque et autres sites Web financiers depuis un réseau Wi-Fi public.

Que faire en cas d'usurpation d'identité ?

Dès que la victime se rend compte de l'usurpation d'identité, elle doit immédiatement porter plainte contre X au commissariat ou à la gendarmerie. N'hésitez pas à prendre conseil auprès d'un avocat ou de votre protection juridique car les conséquences sont parfois dramatiques : fichage à la banque de France, prélèvement de sommes importantes sur votre compte, menace de saisie, etc. Dès qu'un juge aura tranché en votre faveur, il faudra faire parvenir la copie du jugement aux organismes qui vous prennent pour un filou : votre banque, la Banque de France, CAF, sécurité sociale, etc.

(1) Réalisée auprès d'un échantillon de 1 001 adultes entre les 12 et 18 février 2010.

SHAREAZA 2

EXCLUSIF !

SHAREAZA : l'interview du chef de projet

Site hacké, menace des majors, nouvelle version, le «project manager» Nicolay Rapopov, alias Ryo-oh-Ki, a bien voulu répondre à nos questions concernant le petit monde de Shareaza...

Shareaza piratée par l'industrie musicale ?

Il faut remonter dans le temps pour comprendre cette histoire. En 2007, aidée par la toute nouvelle loi DADVSI, la SPPF (Société civile des Producteurs de Phonogrammes en France) décide de porter plainte contre Shareaza. Mais l'organisme se heurte à un problème : Shareaza est un logiciel libre et ses développeurs sont anonymes. La SPPF ne se démonte pas et réclame plus de 2,5 millions de dollars à la personne qui gère le nom de domaine. Le 20 décembre 2007, à la grande surprise de l'équipe de Shareaza, un autre site a pris le nom de domaine www.shareaza.com ! Des dizaines de milliers de personnes téléchargent alors ce faux Shareaza qui se comporte comme un spyware...

Savez vous combien de personnes utilisent Shareaza dans le monde ? En France ?

Les statistiques d'activité du réseau Gnutella 2 sont disponibles à cette adresse : http://crawler.trillinux.org. Mais attention, beaucoup d'Internautes utilisent le logiciel en tant que client BitTorrent ou eMule. Il n'est donc pas possible de se faire une idée précise.

Combien de personnes travaillent sur le projet et comment vous organisez-vous en tant qu'équipe ?

Je pense qu'il y a environ 10 personnes dont 5 sont des développeurs actifs. Depuis le début, seulement 11 personnes ont participé au code de Shareaza. Il y a deux ans, un des développeurs japonais [CyberBob, NDLR] a commencé à créer son propre «Fork» : Shareaza Plus.

Le fondateur Michael Stokes fait-il toujours parti du projet ?

Non, il a arrêté sa participation après la mise en place de la version 2.0.0.0. Personne ne sait où il est à présent...

Auriez-vous un scoop concernant la prochaine version de Shareaza ?

La version 2.5 est sortie le 1er décembre 2009, il est encore trop tôt pour en parler mais nous aimerions apporter le support du protocole BitTorrent DHT [les torrents trackerless qui fonctionnent sans serveur, NDLR] depuis que The Pirate Bay est en passe de devenir entièrement «trackerless».

Combien d'argent dépensez-vous chaque mois pour le projet ?

0 $! Ce projet n'a pas d'argent. Les participants sont volontaires...

Pouvez-vous nous en dire plus concernant le faux site Shareaza ? S'agit-il de personnes que vous connaissez ou juste des étrangers qui veulent faire de l'argent sur votre travail ? Pensez-vous poursuivre ces «pirates» ?

La société MusicLabs LLC a obtenu le nom de domaine shareaza.com grâce à Jon Nilson. C'est une personne étrangère au projet mais qui s'est vu donner le nom de domaine (en tant que personne de confiance) par Mike Stokes à l'époque où ce dernier a voulu se mettre à l'écart du projet. Il semblerait que Monsieur Nilson se soit fait menacer de poursuite (étant alors le seul intermédiaire disponible via Whois) par la SPPF. Comment le nom de domaine a été reversé à MusicLabs, nous n'en savons rien. C'est dorénavant la société Discordia qui est propriétaire de la marque «Shareaza» aux USA et il est même dangereux pour nous d'utiliser ce nom ! Nous avons besoin de toute l'aide juridique possible !

Être en charge du projet Shareaza, ça marche avec les filles ?

Mais nous avons une «fille», l'âme de l'équipe : Kath (elle a 60 ans et plusieurs petits-enfants !)

www.shareaza.com

http://sourceforge.net/projects/shareaza

LE 1ER MAGAZINE BITTORRENT

NOUVEAU !

L'avenir du numérique chez votre marchand de journaux

NOS VIES PRIVÉES...

DANS LES MAINS DES GÉANTS D'INTERNET

Gentiment appelé «pourriel» par nos amis Québécois (contraction de «pourri» et «courriel»), le spam est un véritable problème depuis le début des années 90. Outre la publicité, les chaînes de mails qui colportent les «hoax» atterrissent aussi dans votre boîte à lettres et vous gâchent peu à peu la vie. Gros plan sur ces fléaux des temps modernes...

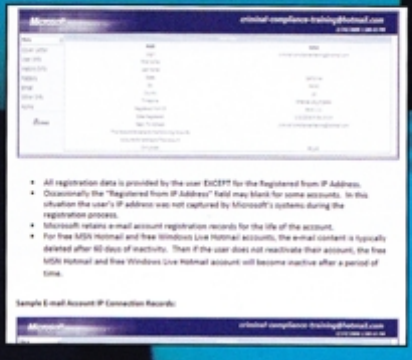
MÊME LES JEUX VIDÉO

En février dernier, une affaire faisait grand bruit chez les joueurs de World of Warcraft de l'éditeur Blizzard Entertainment. Un jeune américain, soupçonné d'escroquerie en ligne, était arrêté grâce à son compte World of Warcraft. Le FBI confirmait que l'homme avait été remonté grâce à son jeu vidéo en ligne préféré. Il aura fallu aux agents américains de suivre l'adresse IP du pirate, celle qui lui permettait de se connecter à WOW pour le retrouver, en live, à son domicile.

Il y a quelques semaines, l'excellent site Internet Cryptome.org - sur lequel il est possible de trouver des centaines de fichiers allant du secret à l'ultra-secret s'étant échappés du gouvernement américain, de l'armée ou d'entreprises informatiques - diffusait des documents qui permettaient de comprendre les données que possèdent les géants de l'Internet comme Microsoft, Facebook, Paypal, eBay. Des données sensibles, privées, qui nous appartiennent mais qui, un jour, ont été fournis aux entités nommées. Des informations qui se retrouvent dans les mains de tiers électroniques. Des informations que pourraient fournir, un jour ou l'autre, ces géants à la justice, sur une simple réquisition judiciaire.

Microsoft ! Vos papiers !

Commençons par le maître de l'univers informatique, j'ai nommé Microsoft. Pour le cas de Windows Live Mail, Microsoft possède et sauvegarde sur une durée de 60 jours, les adresses IP des connexions, le login, le nom, le prénom, le lieu de résidence de l'abonné, l'adresse IP ayant permis la création du compte. Loin d'être négligeable, les policiers peuvent accéder à l'ensemble des e-mails si ces derniers sont stockés en ligne. Si les missives ont été téléchargées et effacées du webmail de Microsoft, l'éditeur américain indique ne plus y avoir accès. Pour Windows Live ID, en plus des données sauvegardées via Live Mail, Microsoft archive les dates et heures de connexion. Pour Windows Live Space et MSN, les services de Microsoft peuvent fournir les contenus privés mis en ligne et

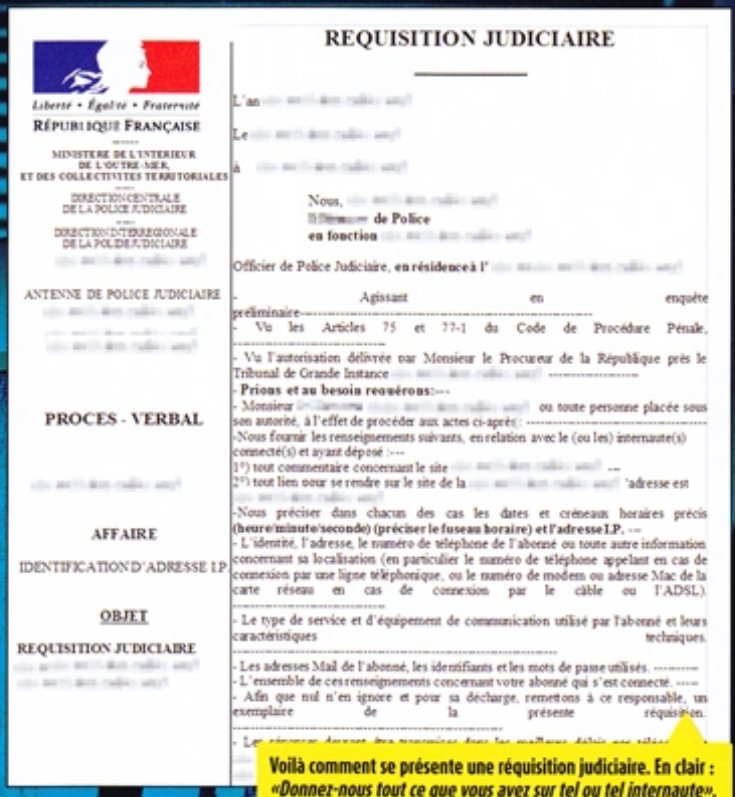


les moyens de paiement associés au compte MSN, à un IP enregistré, etc.

Facebook et les sales gosses

Passons maintenant du côté de chez Facebook. Le plus gros «bot espion» de la planète indique dans un document baptisé «Facebook Confidential and Proprietary», qu'il est capable de fournir en trois ou quatre semaines, l'identité complète (email, adresse, etc.) d'un internaute concerné par une enquête. IP, date de naissance, emails connus, compte Messenger ID, numéro de téléphone, adresse et données concernant la période liée à l'activité illicite. Les logs Facebook seraient conservées 90 jours. «*Contactez Facebook si vous avez un besoin spécifique avant de nous délivrer une citation à comparaître ou un mandat*» s'émeut l'équipe de Mark Zuckerberg. Une émotion qui passe très rapidement à l'image de l'affaire ayant visé la ville alsacienne de Ribeauvillé. Plusieurs dizaines d'élèves seront exclus du collège des Ménétriers, en février 2010, pour insultes. Il aura suffi à la justice de réclamer à Facebook les informations numériques des adolescents pour retrouver les collégiens.

Côté business, eBay et Paypal ont mis en place une procédure de cybersurveillance qui, normalement, ne laisse aucune chance aux pirates. eBay a établi un partenariat avec Leadsonline (www.leadsonline.com) afin de faciliter et accélérer toute demande judiciaire. «*Un services disponible 24h/24h et 7 jours sur 7 pour les clients enregistrés chez Leadsonline*, explique le document eBay/PayPal Law Enforcement Guide. *Leadsonline offre deux services distincts pour aider les forces de l'ordre dans les enquêtes d'eBay : recherche dans le site eBay et sur Internet (eBay) Drop-Off Store Search.*» eBay/Paypal peuvent fournir ainsi l'IP et l'heure de l'enregistrement d'un compte, L'IP et l'heure de l'enregistrement d'une annonce, La liste complète et l'historique des enchère, Les données bancaires (CB, etc.) Pour Paypal, le document interne indique qu'il est possible aussi à la filiale d'eBay de communiquer en plus le numéro de sécurité sociale (pour les USA), les noms, adresses, numéros de téléphone, adresses e-mail ; l'IP à chaque ouverture de session ; Les comptes bancaires ajoutés au compte PayPal.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR
DE L'OUTRE-MER,
ET DES COLLECTIVITES TERRITORIALES

DIRECTION CENTRALE
DE LA POLICE JUDICIAIRE

DIRECTION INTERREGIONALE
DE LA POLICE JUDICIAIRE

ANTENNE DE POLICE JUDICIAIRE

PROCES - VERBAL

AFFAIRE

IDENTIFICATION D'ADRESSE I.P.

OBJET

REQUISITION JUDICIAIRE

REQUISITION JUDICIAIRE

L'an

Le

à

Nous,
de Police
en fonction

Officier de Police Judiciaire, **en résidence à l'**

Agissant en enquête préliminaire

- Vu les Articles 75 et 77-1 du Code de Procédure Pénale,

- Vu l'autorisation délivrée par Monsieur le Procureur de la République près le Tribunal de Grande Instance

- **Prions et au besoin requérons:**

- Monsieur ou toute personne placée sous son autorité, à l'effet de procéder aux actes ci-après :

-Nous fournir les renseignements suivants, en relation avec le (ou les) internaute(s) connecté(s) et ayant déposé :

1°) tout commentaire concernant le site

2°) tout lien pour se rendre sur le site de la 'adresse est

-Nous préciser dans chacun des cas les dates et créneaux horaires précis **(heure/minute/seconde) (préciser le fuseau horaire) et l'adresse I.P.**

- L'identité, l'adresse, le numéro de téléphone de l'abonné ou toute autre information concernant sa localisation (en particulier le numéro de téléphone appelant en cas de connexion par une ligne téléphonique, ou le numéro de modem ou adresse Mac de la carte réseau en cas de connexion par le câble ou l'ADSL).

- Le type de service et d'équipement de communication utilisé par l'abonné et leurs caractéristiques techniques.

- Les adresses Mail de l'abonné, les identifiants et les mots de passe utilisés.

- L'ensemble de ces renseignements concernant votre abonné qui s'est connecté.

- Afin que nul n'en ignore et pour sa décharge, remettons à ce responsable, un exemplaire de la présente réquisition.

Voilà comment se présente une réquisition judiciaire. En clair : *«Donnez-nous tout ce que vous avez sur tel ou tel internaute».*

Ce qu'en dit la loi Française

En France, comme dans plus en plus de pays, l'hébergeur est responsable des contenus créés par des personnes agissant sous son autorité ou son contrôle. En gros, le fait que vos intervenants numériques possèdent un compte « membre » sur votre site Internet vous rend responsable de leurs écrits dans votre forum, blog, Vous pensiez que le post de «bebert59» sur l'entreprise X n'avait qu'un intérêt limité, détrompez-vous. L'administrateur ne peut s'exonérer de sa responsabilité en invoquant qu'il n'a pas connaissance des informations litigieuses qu'il met en ligne. Si «Bebert59» annonce que l'entreprise X est truffée de voleurs, vous devenez, aux yeux de la loi responsable des écrits de votre ami numérique. La LCEN (Loi sur la confiance dans l'économie numérique - www.legifrance.gouv.fr) pose le principe d'une responsabilité conditionnée par la connaissance ou non du contenu illégal diffusé sur un support numérique. Pas d'obligation de modération, mais obligation de conserver les données qui permettront d'identifier les posteurs (IP, email, adresse, date d'enregistrement, de diffusion des messages). Le webmaster, l'administrateur d'un forum, liste, tombent aussi sous le coup de la loi du 29 juillet 1881 (provocation aux crimes et délits, apologie des crimes de guerre, propos racistes, fausses nouvelles susceptibles de troubler l'ordre public, injures, diffamation, etc.)

Hacker une voiture

en un tour de clé

L'informatique embarquée dans nos véhicules est-elle sécurisée ? Des pirates informatiques pourraient-ils modifier le comportement de conduite ? Afficher des informations erronées ? Science-fiction il y a encore quelques semaines, des chercheurs américains prouvent que nos voitures pourraient devenir les prochaines victimes de la génération Hacker.

Des chercheurs des universités de Californie et de Washington ont démontré, en mai dernier, que pirater l'informatique d'une voiture n'était pas si compliqué que ça. Pour parfaire leurs explications, les étudiants ont créé le logiciel CarShack, un petit module informatique qui vise les unités de contrôle électronique intégrées dans les véhicules modernes. Mission de CarShack, intercepter la communication entre les différentes unités de contrôle et d'y injecter de fausses données à partir de la prise OBD-II (On Board Diagnostic System Information). Une prise qui permet à votre garagiste de brancher son portable et de diagnostiquer le moindre pépin mécanique de votre voiture. Les chercheurs indiquaient que l'attaque n'est pas aisée. Il faut du matériel et certaines connaissances techniques et informatiques. Mais la démonstration réalisée a eu de quoi laisser pantois. Une fois CarShack lancé, il était possible de lire un compte à rebours sur le tableau de bord de la voiture. Une fois le décompte terminé, l'auto s'est mise à klaxonner, le moteur s'est arrêté et les portes se sont bloquées.

Une prise OBD-II vers USB. Avec ce type d'adaptateur et le logiciel CarShack, il est possible de contrôler différents points d'une voiture. Ça n'arriverait pas sur ma 4L...

Difficile à mettre en œuvre le piratage automobile ? D'après le journal Auto Plus, pas plus que de briser la glace de la plage arrière de votre automobile. Dans son numéro 1113, l'hebdomadaire explique comment des contrefaçons des logiciels et des prises de diagnostic pour les Renault et les Peugeot/Citroën ont été achetés via Internet. Bilan, il a été possible de prendre en main un Scenic et une 308. Pour 120 euros, Auto Plus a également commandé un ouvre-portes déverrouillant les serrures des voitures. Pour 1 725 euros, un boîtier et une carte permettant de se fabriquer une fausse clé électronique.

Clé de voiture sans fil

Les nouvelles clés, portes d'accès pirates ? En 2007, des chercheurs réussissaient à cracker le système de clé de démarrage des Chrysler, Daewoo, Fiat, General Motors, Honda, Volvo, Volkswagen, et Jaguar. Lors de la conférence CRYPTO 2007, les chercheurs ont expliqué comment ils avaient

Les puces RFID utilisées dans les clés de démarrage sans contact sont très petites mais pas si sécurisées que cela...

réussi à pirater le «key-fob system», les clés de démarrage sans contact. La démonstration a été faite sur une Toyota Prius. Pour réussir ce tour de passe-passe, le voleur devait trouver la gamme (range) de connexion de la clé RFID de la key-fob system afin de casser le cryptage. Pour réussir ce vol, il suffisait au pirate de s'asseoir à côté du conducteur de l'automobile ou être proche de ce dernier. Grâce à un appareil sans fil, le chiffrement 64 bits avait volé en éclat en une heure. Les commandes à distance ne sont pas exsangues de problèmes à l'image de l'affaire ayant visé un loueur américain de véhicules. Un ancien employé, mécontent à la suite de son licenciement, va réussir à immobiliser une centaine de voitures en lançant une commande informatique, via le logiciel de «sécurité» Emergency Start System (ESS). ESS contrôlait les automobiles louées. Il aura suffi d'un clic de souris pour bloquer les autos.

Des mots de passe comme s'il en pleuvait !

En 1991, Ronald Rivest, un informaticien de talent améliore l'algorithme de chiffrement MD4 et créer le MD5, le Message Digest 5. Cette fonction algorithmique de hachage est extrêmement présente sur Internet pour certifier des empreintes numériques. Nous allons vous expliquer pourquoi, aujourd'hui, il est fortement conseillé de passer à autre chose.

En 1996, une faille qualifiée de grave, car permettant de créer des collisions à la demande, était découverte dans le MD5. Il faudra attendre huit ans pour que les doutes sur la fiabilité du MD5 ne soient plus une légende. Une équipe chinoise découvrait et démontrait que le MD5 devait être abandonné pour des algorithmes plus solides tels que SHA-256, RIPEMD-160 ou Whirlpool. Si des logiciels tels que le mythique John the ripper est capable de brute forcer un mot de passe MD5, des internautes malicieux ont trouvé encore plus simple pour mettre à jour le précieux sésame caché derrière les 32 mystérieux caractères (128 bits). Cette solution miracle ? Des sites Internet qui regroupent des centaines de millions de mots de passe et leurs traductions au format Message Digest 5. Bref, il suffit d'intercepter un hash dans un site Web ou une base de données pour obtenir un mot de passe valide presque à chaque coup !

Rednoize - md5.rednoize.com
Simple, efficace, Rednoize vous propose de rechercher le hash d'un mot de passe dans une base de données de plus de 58 millions de password. À noter une option dédiée aux sésames chiffrés en SHA-1. L'outil va trouver le MD hash e10adc3949ba59abbe56e057f20f883e en 0.001608 seconde.

MD Crack - md5crack.com
Pas besoin d'être un génie pour comprendre l'intérêt de MD5 Crack. MD5 Crack est un malin, sa base de données n'est rien d'autre que Google. Bref, le moindre hash trouvé sur le géant de la recherche web se retrouve sur MD5 Crack. Les auteurs du site mettent rapidement aux pas les utilisateurs «MD5 Crack utilise Google pour cracker les mots de passe». Le site affiche les dix dernières recherches effectuées. Un outil pour calculer son MD5, MD5, SHA-1 est disponible. Une seconde pour nous sortir 123456.

Md5decryption - md5decryption.com
L'intérêt de MDdecryption est de pouvoir trouver une réponse à un hash parmi plus de 1,3 millions de mots, mais aussi et surtout, de créer son propre hash MD5. Juste un détail, de taille. Le mot de passe que vous avez créé en MD5 se retrouvera ensuite dans la base de données pour toute recherche de déchiffrement. Bref, vous l'aurez compris, à éviter !

Pass Cracking - passcracking.ru
Nos amis russes [Il faut toujours avoir un ami russe, NDLR] proposent Passcracking. Belle bête informatique qui permet de cracker du MD5 à la demande. Derrière le portail, des dictionnaires rainbow. Ce n'est pas automatique, il faut s'inscrire et lancer une demande soit par le forum, soit par SMS. Un projet ambitieux mais bigrement efficace.

Hash Cracking - hashcracking.com
23 565 170 de possibilités, voilà ce que propose Hash Cracking. L'option «Upload world list» est très intéressante pour ceux qui souhaitent participer à la communauté des MD5 hash killer. Les propositions seront ensuite intégrées dans la base de données de hashcracking.com. Notre test permet de trouver le mot de passe 123456 en 0.004101 seconde.

Hash killer - hashkiller.com
Opencrack est un système où tout le monde peut contribuer à cracker du MD5. Il vous suffit de télécharger une liste de hash à décortiquer. e10adc3949ba59abbe56e057f20f883e nous a été cracké en 0.003 seconde. À noter que ce mot de passe est à titre d'exemple et à ne surtout pas utiliser. Il est piraté depuis le 01 novembre 2009.

Paris et Poker en ligne

UN UNIVERS IMPITOYABLE

À l'aube de la nouvelle loi sur les jeux d'argent en ligne, il nous semblait tout naturel de vous proposer un dossier sur ce sujet. Entre les failles des casinos en ligne, les pirates qui arrivent à «voir» les cartes au poker et les taux de redistribution mensongers, le monde des casinos en ligne est-il si sécurisé que cela ?

Les premières rumeurs de triche sur des sites de poker ont commencé en 2008 sur le site Ultimate Bet.

Phil Hellmuth, figure emblématique du Texas Hold'em (la règle de poker «à la mode») a gagné un pot conséquent avec une main perdante ! Le joueur professionnel est en effet «super users» de la poker room (comprenez par là qu'il est payé pour jouer et apporter sa notoriété au site). En plus d'avoir joué sa faible main de façon très agressive le joueur, habitué aux excès, a copieusement provoqué l'assistance. Il n'en fallait pas plus pour que le site soit accusé de tricherie. Il semblerait qu'une déconnexion sauvage soit à l'origine du problème et même si l'adversaire malheureux a été dédommagé, la rumeur se répand...

Le cas Cereus

Dernièrement, Ultimate Bet a encore fait parler de lui par l'intermédiaire de la société Cereus (responsable de ce dernier et d' Absolute Poker). Il s'agit cette fois d'une vulnérabilité avérée qui permettait de voir les cartes des joueurs adverses en pleine partie ! Un sniffer qui décrypte les mains à la volée grâce à l'interception de hash MD5 (voir notre article page 17). Vous trouverez la démonstration en vidéo (et en anglais) ici : **www.youtube.com/watch?v=AAQDEXJdbQc**. Bien sûr, la faille a été corrigée mais nous pouvons nous poser des questions sur la sécurité de ces sites. Combien de temps cette faille a permis aux tricheurs de spolier les honnêtes gens ? Sur son blog, le champion canadien Daniel Negreanu ne s'est pas privé pour enfoncer le clou. Selon lui, Ultimate Bet est *«la gangrène de la communauté poker depuis 10 ans»*. Selon lui, les responsables du site étaient conscients de la faille mais ils ont préféré continuer et garder le site ouvert. Apparemment très remonté, «Kid Poker» (qui a déjà eu maille à partir avec UB.com à cause d'une histoire de prix mensonger) se lance dans des explications techniques : *«Apparemment à ce que j'ai entendu, une simple calculatrice Windows suffisait à craquer leur logiciel»*. Même si nous n'en sommes pas là, il faut bien reconnaître que le hack de hash MD5 n'est pas vraiment un tour de force du point de vue technique...

Daniel Negreanu n'est pas tendre avec Ultimate Bet...

Les techniques de triches

Sur les sites de poker, il existe aussi d'autres techniques pour tromper la chance. Certains joueurs jouent ensemble sur la même table : ils se donnent leurs mains au téléphone pour tromper les probabilités et jouer à fond la main qui a le plus de chance. Certains n'hésitent pas non plus à se connecter avec 2 ordinateurs et deux IP différentes pour éviter d'avoir à partager les gains avec un compère. Il est bien sûr possible de vous plaindre auprès de l'Assistance du site pour qu'ils fassent une enquête mais attention de ne pas crier au loup toutes les 5 minutes... La façon la plus censée de combattre la triche est d'arrêter de jouer. Ce faisant, vous arrêtez de participer au butin qui est la cible première des contrevenants. Plus de gogo, plus de magot !

Jongler avec les cotes n'est pas tricher !

On peut parfois gagner à coup sûr sans pour autant tricher. Dans le monde des paris en ligne, on appelle ça les «surebets » ou paris sans risque. À l'origine créer pour décrire les paris avec des côtes inférieures à 1.20 (pour 1 € parié, vous en gagnez seulement 1.20 € en cas de victoire), le terme désigne aussi une méthode qui permet de jongler avec les différences de cotes entre deux bookmakers. Miser pour une victoire de A sur tel site et une victoire de B sur un autre. En fonction des sommes engagées, il est possible de gagner quelque soit le résultat. Voici deux liens permettant d'y voir un peu plus clair et remplis de bons conseils :

www.parierenligne.com/guide/surebet.html www.pariezmieux.com/surebets.html

Les martingales magiques : une arnaque

Attention aux sites qui vous conseillent telle ou telle méthode pour gagner à coup sûr à la roulette. Comme ce joueur qui au détour d'un blog conseillait de jouer sur un site un euro sur le rouge ou le noir. Si vous gagnez, vous doublez la mise. Si vous perdez, vous devez miser 2 euros sur la même couleur. Au niveau des probabilités, ce type de stratégie ne vaut rien (autant miser complètement au hasard) mais si la personne déclare avoir décelé une faille dans un casino en particulier, il s'agit d'une arnaque. Ils sont souvent complices d'un site particulier qui vous fera gagner gros avec de l'argent virtuel et une fois mis en confiance, vous détrousseront partie après partie...

Les vrais bandits ne sont pas manchots

On voit des publicités pour les casinos en ligne un peu partout sur le net : pop-up, spam, site Internet, etc. Avec des promesses de taux de redistribution allant de 95 à 98 %, les chalands sont appâtés facilement.

Attention car même si les casinos ont fait des progrès depuis le début des années 2000, il est bien difficile de cerner la localisation géographique des serveurs, le siège social de la société et l'identité des véritables exploitants. Le fonctionnement de ces sites, pourtant interdits au regard de la loi française (et qui resteront bannis même avec la libéralisation des jeux) est tout aussi obscur pour les internautes. Avant de succomber à la fièvre du jeu, prenez bien le temps de lire le règlement et les conditions. Il s'avère en effet parfois un peu difficile de récupérer les sommes gagnées. L'arnaque fréquente consiste pour le casino de décréter que la carte qui a servi à alimenter le compte ne peut pas servir à récupérer les sommes (avec à chaque fois une bonne excuse : somme trop faible, trop importante, etc.) Le client est donc invité à demander un retrait par chèque. Le problème c'est qu'en choisissant cette option, la somme se retrouve amputée à cause de différents intermédiaires. Pire, certaines banques françaises refuseront parfois de vous créditer de la somme car pour elles, il s'agit de blanchiment pur et simple...

Les casinos lavent plus blanc !

Dès que l'on parle d'argent sur le Web, on pourrait penser que les administrateurs regardent de plus près à ne pas voir leurs clients se faire piller ! Sachez qu'il n'en est rien et que les casinos en ligne servent parfois les intérêts seuls du gérant. En effet, à l'instar d'un vrai casino, les casinos en ligne peuvent servir à blanchir de l'argent. C'est pour cela que les casinos sont très réglementés en France (alors qu'ils poussent comme des champignons dans les pays de l'Europe de l'Est). Si un mafieux veut blanchir de l'argent sale, la méthode est la même qu'avec un casino "réel". Il suffit d'être propriétaire du casino et y faire perdre des complices. Résultat : le casino a fait des gains parfaitement légaux en apparence, et son propriétaire peut en disposer sans être inquiété légalement. Malheureusement, à l'inverse des paris et des salles de poker, les casinos en ligne ne se verront pas octroyer de licence pour officier légalement en France. Nombreuses sont les

sociétés qui sont maintenant domiciliées dans des paradis fiscaux. Et même si certains casinos sont au-dessus de tout soupçon, on oublie souvent les centaines d'autres qui ne perdent jamais à la roulette ou au black jack ! Et pour vous plaindre, bonjour le mal de tête... Heureusement, les sites de casinos en ligne ont un petit avantage par rapport à leurs homologues de la vie réelle puisque des logiciels permettent de vérifier l'activité des joueurs : qui joue avec qui, utilisateurs avec plusieurs identifiants, activité suspecte, gagnant qui défient les lois de la probabilité, etc. Mais là où des personnes peuvent se voir être interdit de casino dans la vraie vie, le manque de dialogue entre les sites occasionne certains problèmes puisque l'inscription dans une liste noire permet tout de même aux tricheurs de jouer sur d'autres sites. À l'inverse il est tout aussi difficile de trouver des listes de site ne respectant pas les règles. Avant de claquer votre loyer dans un casino en ligne, veillez à ne pas mettre les pieds dans un nid de vipères...

Les sites à éviter :

- www.mondo-casinos.com/liste-noire-casinos.php
- www.topdescasinos.com/listenoiredescasinos.htm
- www.jeux-de-casinos.com/blacklist.php

Insolite

Black jack Card Counter est l'application iPhone qui fait sensation en ce moment. Il s'agit d'un logiciel permettant de compter les cartes au Black jack. Pour la modique somme de 2,39 €, vous pourrez donc connaître les probabilités d'obtenir une carte gagnante selon la méthode «Hi-Low» de Harvey Dubner. Ce que les héros du film Las Vegas 21 font avec leur tête, vous pourrez le faire facilement avec votre téléphone ! Attention, même s'il est autorisé de compter les cartes, l'utilisation d'un gadget électronique est formellement interdite. Pour en savoir plus sur ce système : www.guide-blackjack.com.

Loi sur les jeux en ligne

À l'approche de la Coupe du Monde, on en parle de plus en plus : la France va lâcher du leste concernant les jeux d'argents. La Française des Jeux et le PMU ne seront donc plus en position de monopole. La loi a été promulguée le 12 mai dernier et les premières licences ont été attribuées au début du mois de juin. Pour les opérateurs de paris et de poker en ligne, plus question de tricher après cette date ! L'Autorité de régulation des jeux en ligne (ARJEL) doit veiller à ce que les sites respectent un certain nombre de contrainte mais aussi d'écarter les sites n'ayant pas de licence du paysage Internet français. Même si à présent aucun site de jeux en ligne n'a été poursuivi, la donne pourrait être différente début juin avec les premières licences distribuées. Officiellement pour lutter contre l'argent sale, le gouvernement protège en fait l'ancien monopole de la Française des jeux ainsi que les bons élèves qui rejoindront leurs rangs. La nouvelle autorité de régulation, accompagnée de cyber-douaniers, espère parvenir à bloquer, par le biais de décisions de justice, l'accès aux sites étrangers grâce à l'aide des fournisseurs d'accès à Internet.

arjel
Autorité de régulation des jeux en ligne

On peut malgré tout se poser des questions sur la capacité de l'ARJEL (Autorité de Régulation des Jeux En Ligne) de garantir l'étanchéité du marché français quand on voit le nombre de sites qui proposent paris sportifs, poker ou courses hippiques. D'autant que le public s'est familiarisé avec des marques à ce jour toujours «illégales» comme 888, Betway, Unibet, etc.

Pas d'interview!

Alors qu'ils venaient d'obtenir l'agrément de l'ARJEL (et qu'ils n'étaient donc plus considérés comme sites illégaux), Betclic et Bwin et France-pari (qui gère aussi Sportnco) n'ont pas souhaité répondre à nos questions d'ordre technique concernant la sécurité de leur site. Sont-ils dépendants d'une plate-forme dont ils loueraient les services ou n'ont-ils tout simplement pas envie de disserter de la sécurité, nous n'en saurons rien. On peut bien sûr se dire que l'ARJEL a pris toutes les dispositions pour que ces sites répondent à différentes exigences en matière de sécurité mais qui sera responsable en cas de litige ?

La liste des opérateurs agréés : www.pre-arjel.fr

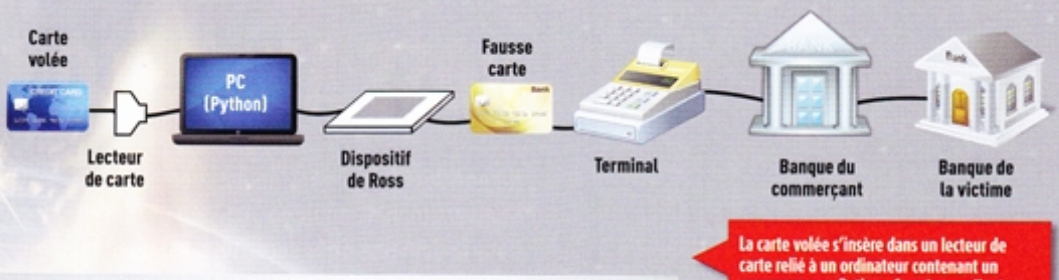
Les cartes bancaires ÉCHEC et MAT...

Révélée au début de cette année, vous n'avez probablement pas entendu parler de cette faille dans le système EMV des cartes bancaires. Découvert par un universitaire de Cambrigde, il s'agit ni plus ni moins d'une bombe que les médias, par manque de connaissance ou par ignorance, n'ont pas été nombreux à relayer. Voyons de quoi il retourne...

Le système EMV (pour Europay – Mastercard – Visa) est le standard international de sécurité des cartes de paiements. Apparu en 1995 et profitant de la technologie des cartes à puces, l'EMV est devenu, en 2006, le principal mode de paiement en France depuis l'aménagement du parc des anciens terminaux de paiement. Plusieurs autres pays européens qui se sont ralliés progressivement ces dernières années à la carte à puce sont aussi concernés. L'EMV concerne 730 millions de cartes en circulation dont 500 millions de cartes en Europe et 60 millions en France. Jusque-là considéré comme une forteresse imprenable, ce système a récemment été mis à mal par une équipe de chercheur de l'Université de Cambridge. Ces derniers ont trouvé le moyen de faire croire au terminal de paiement que le code secret est bon quel que soit le code tapé. Attention, il ne s'agit pas d'une «yes card» (une carte bancaire trafiquée qui fait dire «oui» à chaque fois) mais bel et bien d'une carte volée à Monsieur Tout-le-monde.

La faiblesse de l'EMV

Rien de magique là-dedans. Il s'agit d'une attaque «man-in-the-middle» («l'homme au milieu» en français) où un appareil relié à un PC trafique les informations entre la carte et le terminal (la machine que l'on vous tend pour rentrer la carte et le code). L'EMV doit d'abord authentifier la carte (vérification que les données n'ont pas été altérées) puis le propriétaire (vérification que le code appartient bien à cette carte) et enfin autorise la transaction. La faille centrale du protocole est que l'étape de la vérification du code PIN n'est jamais explicitement authentifiée. Lors d'une transaction, le terminal peut soit demander la vérification du code PIN



La carte volée s'insère dans un lecteur de carte relié à un ordinateur contenant un programme en Python. Ce même ordinateur est relié au fameux appareil «man-in-the-middle» de Ross. Un autre câble part de ce dernier pour relier une fausse carte bancaire (qui a les mêmes dimensions mais qui n'est que le prolongement de la carte volée). Il ne reste qu'à cacher l'ordinateur et l'appareil dans un sac à dos et le fil relié à la fausse carte dans votre manche. Le serveur ou le vendeur n'y verra que du feu. Il ne reste qu'à avoir un minimum d'imagination pour le code puisqu'ils sont tous valides !

ou la vérification de la signature (un simple certificat qui prouve que la carte n'a pas été clonée). En effet, il existe toujours des cartes qui ne requièrent que la signature. Ce sont des demandes spécifiques que la banque reçoit pour des personnes qui ne peuvent pas retenir un code ou pour les malvoyants, par exemple. Comme le terminal peut passer à l'une ou l'autre de ces vérifications, il suffit de faire croire à la machine que la carte ne requiert pas de PIN et comme la réponse de la carte n'est pas authentifiée, la transaction passe comme une lettre à la poste...

Interception de données

Une interception de données entre la carte et le terminal peut tromper ce dernier en lui faisant croire que le code a été vérifié sans qu'il ne le soit vraiment. De son côté, la carte croira que le terminal ne supporte pas le protocole de vérification à base de code et ce, même si le marchand dispose d'une connexion avec le réseau bancaire. Selon l'article de Ross Anderson, il est possible de se confectionner un tel dispositif pour moins de 200 $. La taille de l'appareil pourra paraître sans doute un peu suspecte mais Ross a déjà commencé à la miniaturiser. De surcroît, il n'est pas absolument nécessaire d'avoir un PC puisque cet élément peut facilement être implémenté dans l'appareil. Il faut aussi rappeler que les vendeurs ou serveurs détournent souvent le regard au moment de la transaction pour laisser le client mettre sa carte et composer son code. Il est alors facile d'utiliser un stratagème pour masquer le fil qui relie la fausse carte au dispositif (voir photo). Pire, le marchand peut être complice et, dans ce cas, il n'y a aucune parade. Le client qui s'est fait voler sa carte n'a presque aucun recours puisque le PIN est déclaré valide et dans ce cas, la banque ne rembourse pas la victime qu'elle accuse de négligence.

Faites sauter la banque !

Selon le Figaro, le Crédit Agricole, le Crédit Mutuel, la Banque Postale ou encore BNP Paribas sont mobilisés pour prévenir un scénario d'attaque mais depuis la révélation de la découverte, c'est le silence radio. Les banques ont, en effet, très rapidement fait des déclarations à la va-vite concernant ce type d'attaque. Avant même que Ross Anderson ne publie ses recherches, les banques se sont empressées de déclarer qu'un tel type d'attaque était seulement réalisable dans un laboratoire (pourtant Ross a fait des démonstrations de son système devant des journalistes sagement attablé dans un bar). Gilles Guitton, Président du Conseil de Direction du Groupement des cartes bancaires a même confirmé à nos confrères de 01net que *«le risque demeure extrêmement limité»* et que *«le scénario de Ross Anderson fait partie de ces travaux universitaires qui nous aident à anticiper les attaques qui pourraient se produire un jour»*. Ou comment renvoyer le «geek de Cambridge» à son rang de rat de laboratoire... Pour elles, le dispositif était trop volumineux pour ne pas attirer l'attention, le fait que les transactions sur Internet et les retraits au distributeur ne soient pas affectés leur semblait suffisant. On a pu lire ensuite que seul les petits montants pouvaient être «hacké» car le *«leurre ne trompe pas les serveurs lorsqu'il y a une demande d'autorisation»*. C'est évidemment totalement faux.

L'INTERVIEW DE ROSS ANDERSON

Né en 1956, Ross Anderson est chercheur à l'université de Cambridge, écrivain et consultant dans le domaine de la sécurité. Il est aussi membre de la Royal Society. Lui et son équipe sont à l'origine de la découverte de cette faille. Malgré un emploi du temps très chargé, il a quand même trouvé le temps de répondre à nos questions...

En France nous avons un problème avec les cas de Full Disclosure (le principe de divulgation publique d'un problème de sécurité) et je suis sûr que vous avez déjà entendu parler du cas de Serge Humpich [qui a eu des démêlés judiciaires suite à la découverte d'une faille dans le système de la carte bancaire, NDLR]. Avez-vous rencontré des problèmes avec vos révélations ?

Nous sommes très prudents en ce qui concerne ce risque. Il nous est déjà arrivé auparavant de subir des menaces légales des banques pour nous forcer au silence dans le but de continuer de tromper leur client. C'est pour cela que cette fois nous avons été particulièrement attentifs. Nous avons en effet prévenu l'ECB (la Banque Centrale Européenne), l'APACS (l'ancien nom de L'UKPA qui regroupe plusieurs organismes financiers au Royaume-Uni), la Réserve Fédérale et la police de manière simultanée. Trois de ces organisations n'ont rien fait du tout à l'exception de l'ECB qui a prévenu les banques et les sociétés de cartes bancaires dans les pays de la zone Euro.

Lorsque vous avez parlé du problème à la Financial Service Autority (le régulateur des services financiers au Royaume-Uni) du problème, l'on-t-il pris au sérieux ?

Eux, non plus n'ont rien fait du tout.

Quelle est la taille de l'appareil qui a permis cet exploit ? Avez-vous une photo ?

Vous pouvez le voir dans notre article (www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf) mais nous avons maintenant un autre appareil de la taille d'un paquet de cartes à jouer.

Pendant notre conversation, vous m'avez dit que la version des banques française était fausse [nombreux sont les médias qui ont demandé des informations complémentaires aux banques sans vérifier les informations, NDLR] et qu'il s'agissait d'une tentative maladroite d'étouffer l'affaire. Pourquoi ferait-il une telle chose ?

Les banques françaises ont apparemment mal compris notre article et en ont déduit qu'il s'agissait d'une énième version d'une attaque à base de «Yes card». Ils ont averti la presse alors que nous demandions 45 jours pour préparer notre article et bien comprendre tout le processus. Ils ont évidemment préféré n'en faire qu'à leur tête et se sont couverts de ridicule.

Pensez-vous que l'ensemble de l'infrastructure bancaire doit changer ou qu'un petit «patch» peut être suffisant ?

Réparer cette faille spécifique demandera au minimum des changements au niveau de la fin de la chaîne. De toute façon, la sécurité du système EMV est tellement pauvre qu'il y a encore des surprises à découvrir. Le système a besoin d'une refonte totale. Nous avons déjà prévenu la Réserve Fédérale Américaine qu'elle ne devrait pas autoriser l'EMV sur leur territoire en l'état.

Avez-vous utilisé cette technique pour payer des vacances au Bahamas à votre équipe ?

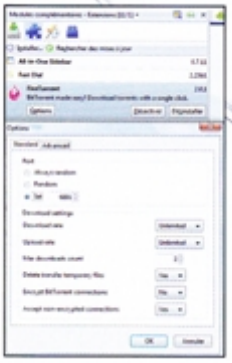
Nous ne pouvons pas ! Cette année, la FCC (Financial Cryptography Conference) se déroulait à Ténérife mais la société espagnole qui nous a vendu les billets d'avion était si dépassée que nous avons dû envoyer notre paiement CB, par fax ! :-)

Les Torrent via Firefox !

Pourquoi le téléchargement de Torrent ne pourrait pas se faire via son navigateur ? C'est en effet plus discret qu'un client complet lorsqu'on est pas chez soi... Opera intègre depuis très longtemps un module de ce genre mais rien ne se profile à l'horizon pour Explorer ou Firefox. Heureusement, ce dernier permet d'ajouter des extensions pour diversifier un peu ses capacités...

https://addons.mozilla.org/fr/firefox

Si vous ne téléchargez pas souvent via le protocole BitTorrent, vous n'avez probablement pas de client dédié à cette tâche. Le problème, c'est que lorsque vous tombez sur un fichier Torrent, vous vous retrouvez comme une poule ayant trouvé un couteau. Pourquoi votre navigateur ne pourrait pas se charger de télécharger du Torrent comme il télécharge via le protocole HTTP ? Internet Explorer ne permet pas de réaliser ce genre de chose et Opera, qui est très à l'aise avec le protocole Torrent, n'est pas du goût des aficionados de Mozilla Firefox. La solution pour le navigateur qui monte c'est d'ajouter une extension appelée FireTorrent.



L'unique solution sous Firefox

Bitfox étant encore en cours de développement et FoxTorrent tardant à passer à la version 3.0 du navigateur, c'est actuellement la meilleure solution pour butiner du Torrent sans se prendre la tête... FireTorrent s'intègre directement au gestionnaire de téléchargement de Firefox en ajoutant un onglet Torrent à ce dernier. Du côté des options, c'est du grand classique : choix de la plage de ports, réglage du débit et du nombre de téléchargements ou encore réglages du proxy.

ATTENTION !

Lorsque vous installez une extension Firefox pour la première fois depuis un site, le logiciel devrait vous afficher un avertissement. Il suffira de cliquer sur **Autoriser** en haut à droite puis de redémarrer le navigateur à la fin du processus...

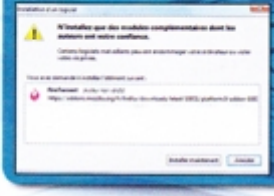
Vos débuts avec FireTorrent

1 LA BONNE VERSION

Pour être sûr d'avoir la dernière version du plugin, allez sur cette page **https://addons.mozilla.org/fr/firefox** et tapez **FireTorrent** dans **Recherche de module** en haut.

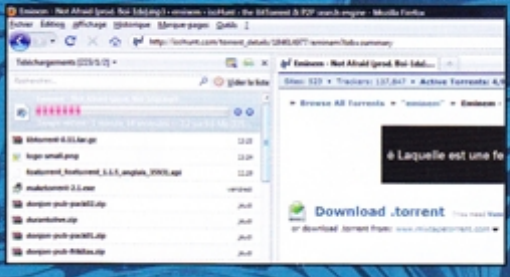
2 L'INSTALLATION

En cliquant sur **Ajouter à Firefox**, vous devriez obtenir cet avertissement. Pas de souci ici, cliquez sur **Installez maintenant**. Il faudra fermer toutes les fenêtres de Firefox et en rouvrir une pour que le changement soit pris en compte (ou cliquez sur **Redémarrer Firefox** dans le panneau de gauche).



3 LE TÉLÉCHARGEMENT

Dans ce même panneau, vous pourrez cliquer sur **Options** pour avoir accès aux différentes fonctionnalités. Une fois vos petits réglages effectués (ou pas), il ne vous reste alors qu'à cliquer sur le lien Torrent que vous désirez et comme par magie (après avoir spécifié son emplacement définitif), il sera téléchargé comme n'importe quel fichier !



Attention aux keyloggers !

Plus rarement appelé «enregistreur de frappe», les keylogger sont des dispositifs (logiciels ou matériels) qui permettent d'enregistrer tout ce que vous tapez au clavier. Le but est bien sûr de surveiller l'activité d'un ordinateur mais ils peuvent aussi se retourner contre vous puisque la plupart sont invisibles ! Voyons comment les détecter et les utiliser...

Les keyloggers ont pour fonction d'enregistrer dans le plus grand secret tout ce que vous tapez sur un clavier d'ordinateur pour transmettre ces données, via Internet, à la personne qui l'a placé sur votre PC. On peut facilement deviner pourquoi un individu ferait une telle chose : récupérer des mots de passe, espionner vos emails (et ce, même si vous utilisez un logiciel de cryptage !), surveiller vos recherches sur Internet, etc. Certains keyloggers plus aboutis permettent aussi d'enregistrer le nom de l'application en cours, la date et l'heure à laquelle elle a été exécutée ainsi que les frappes de touches associées à cette application. Les claviers virtuels qu'utilisent les banques en ligne, par exemple, sont donc obsolètes puisqu'un keylogger peut même créer une vidéo qui enregistrerait toute l'activité de votre bureau. Un véritable fléau puisque votre compte bancaire, Paypal, eBay ou votre webmail ne sont plus à l'abri !

À quoi ça ressemble ?

Il existe deux types bien distincts de keylogger. Les keyloggers «matériels» sont de petits dispositifs placés entre la prise du clavier et l'ordinateur. Ils ressemblent à un adaptateur mais attention, ils enregistrent tout sur une mémoire interne. Ce type de dongle est tout de même assez rare et à moins d'être la victime d'un

UN KEYLOGGER DANS LA MAFIA

Dans leur lutte contre le crime organisé, le FBI utilise aussi des keyloggers. En 2002, les collègues de Mulder et Scully ont placé un keylogger matériel sur l'ordinateur d'un membre d'une famille du crime organisé. Le problème, c'est qu'aucun mandat n'avait

été obtenu. La Cour Suprême des États-Unis a tranché : le FBI n'avait pas besoin d'une autorisation pour enregistrer les frappes sur le clavier d'un ordinateur (alors que la défense voulait apparenter le keylogger à une mise sur écoute qui, elle, nécessite un mandat spécial).

espion ou d'un détective privé, il y a peu de chance de trouver ce genre de matériel sur votre PC. Faites tout de même attention si vous surfez d'un cybercafé, par exemple... Il existe aussi des claviers avec keylogger intégré ! Ici, aucune parade possible puisque le dongle est invisible et les antispyware passeront à côté bien sûr... Si vous voulez voir à quoi ressemble un dispositif de ce type : **www.spycop.com/keyloggerremoval.htm**

Les keyloggers «logiciels»

Mais les keyloggers les plus répandus sont ceux qui prennent la forme de logiciel. Rien à voir avec un espionnage ciblé puisque la plupart du temps les victimes sont contaminées via un malware (trojan, ver, etc.) contracté par Internet. Ils ne nécessitent donc pas un accès physique à la machine pour la récupération des données collectées. À l'inverse de leurs équivalents «matériels», ces keyloggers ne sont pas limités par la taille de leur mémoire puisqu'ils utilisent le disque dur de leur victime. Ils peuvent donc enregistrer beaucoup plus de choses (captures d'écrans, vidéos, listes de contacts, etc.) Il faut donc être particulièrement vigilant lorsque vous utilisez un ordinateur qui n'est pas le vôtre (école, bibliothèque, cybercafé, etc.)

Comment s'en débarrasser ?

Malheureusement, les keyloggers passent parfois entre les mailles des antivirus ou des antispywares. Le trojan responsable de l'infection est éliminé mais pas le keylogger qui reste actif. Pour être sûr d'éradiquer toute présence d'un enregistreur, il va falloir utiliser un logiciel spécialisé comme Anti Keylogger Shield. Même si ce dernier est payant, sa version démo pourra scanner votre PC gratuitement. Il faudra, par contre, débourser 30 € pour éradiquer le mal ou essayer avec un spyware gratuit comme Spybot. Si vous êtes sûr d'être infecté mais qu'aucun logiciel ne détecte votre problème, il va falloir passer à la vitesse supérieure ! Cela passe par la prise d'un «cliché virtuel» du contenu du disque dur. Il s'agit, en fait, de surveiller toutes les modifications de fichiers effectuées par les programmes. Si un logiciel agit de manière louche ou si votre base de registre a connu des modifications, vous le saurez ! Pour faire de tels «clichés», il existe plusieurs solutions telles que Snapshot Spy Pro (qui permet aussi d'accéder aux informations relatives à votre PC en ligne) et ArkoSoft System Snapshot (gratuit).

Surveillez votre ordinateur avec KGB Free Keylogger

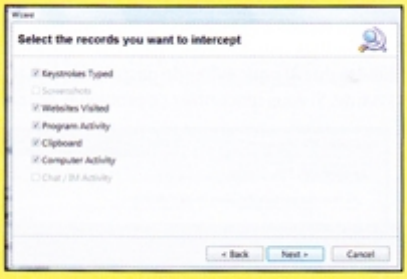
Il existe quantité de keyloggers (Invisible KeyLogger Stealth, etc.) mais nous avons choisi de vous parler de KGB Free Keylogger. Même si le logiciel a été remplacé par Refog Keylogger, nous préférerons cette vieille version à cause de sa gratuité. Attention, KGB n'est pas tout à fait transparent puisque le logiciel apparaît parmi les logiciels installés. Il faudra mettre la main à la poche pour bénéficier d'un vrai keylogger d'espions. Néanmoins, la version gratuite suffit pour surveiller ce que font vos enfants...

1 TÉLÉCHARGEMENT

Si vous désirez la dernière version du logiciel (obligatoirement payante), rendez-vous sur **www.trialpay.com** et remplissez les champs nécessaires à votre inscription. Nous vous conseillons néanmoins de faire une rapide recherche sur Google pour trouver un site qui propose KGB Free Keylogger.

2 LA SURVEILLANCE

Pendant l'installation, le logiciel vous demandera de choisir la langue (anglais, par défaut) ainsi que le type de surveillance que vous voulez opérer : **Keystrokes typed** (touche de clavier), **Website visited** (les sites Internet), **Program Activity**, **Computer Activity**, etc.

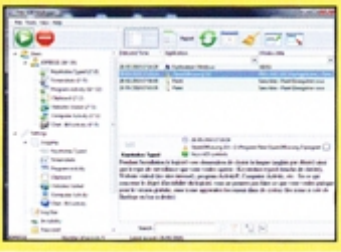


3 INVISIBLE ?

Notez qu'une icône apparaîtra forcément dans le systray (les icônes à côté de l'horloge, en bas à droite). Il est possible de la masquer en faisant un clic droit et en sélectionnant **Hide**. Pour faire revenir le logiciel, il faudra appuyer simultanément sur **Ctrl** + **Alt** + **Maj** (ou **Shift**) + **K**.

4 L'INTERFACE

Sur le panneau principal, en cliquant dans la colonne de gauche sur **Keystrokes Typed**, vous aurez accès à tout ce qui a été tapé (sélectionnez le logiciel sur la droite). Dans **Clipboard**, il est possible de regarder tous les copier-coller, etc. Cliquez sur le balai en haut pour nettoyer ce que vous avez déjà vu.



LES ASTUCES DE LA RÉDACTION

Débrider le stream de YouTube
avec la Livebox Orange

Il s'agit d'un problème bien connu de certains abonnés d'Orange : une lenteur affligeante lors d'un visionnage de vidéo en stream sur YouTube ou d'autres sites de stream américains. Il s'agit apparemment d'un acte délibéré du FAI pour éviter de gaspiller de la bande passante. Si vous rencontrez ce problème, nous avons

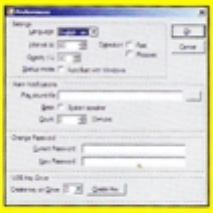
la solution ! Il suffit de changer vos DNS et opter pour ceux de Google. Allez dans le Panneau de configuration, puis dans le Centre réseau et enfin Gérer les connexions réseau. Sélectionnez la connexion pour laquelle vous souhaitez configurer les nouveaux DNS et faites un clic droit puis cliquez sur Propriétés. Ici, vous pouvez être invité à entrer un mot de passe administrateur ou une confirmation. Cliquez sur Protocole Internet version 4 (TCP/IPv4), puis cliquez sur Propriétés. Cliquez sur Avancé et sélectionnez l'onglet DNS.
Remplacez ces adresses avec les adresses IP des serveurs DNS de Google: 8.8.8.8 et 8.8.4.4.
Redémarrez votre connexion ! Attention, avant de changer de DNS, il faudra bien noter les anciens chiffres au cas où vous voudriez revenir en arrière...

Surfez anonyme !
avec Vidalia Bundle

Bien connu des internautes prudents, Tor est un réseau qui permet de surfer de manière anonyme. Le principe est simple, le réseau dirige vos requêtes Web au travers d'un ensemble de "nœuds" cryptés. Chacun des nœuds ne «connaît» que le nœud précédent. Il est donc particulièrement compliqué de remonter jusqu'à la source. Ce pack propose une approche complète et efficace pour les utilisateurs de Firefox. Il comprend le serveur/client Tor, le proxy Privoxy, l'interface graphique Vidalia qui permet de paramétrer Tor, et l'extension TorButton pour Firefox. Comme Tor ralenti les connexions, vous pouvez choisir de le désactiver quand bon vous semble. Bon surf !

https://addons.mozilla.org/fr/firefox

Une clé USB qui ouvre votre session
avec Predator



Si vous n'aimez pas trop qu'on vienne sur votre PC sans être invité, il existe plusieurs solutions comme le verrouillage de session (raccourci clavier touche Windows + L). Le problème, c'est qu'on vous demandera à chaque fois de taper votre mot de passe. Predator sécurisera l'accès à votre ordinateur en transformant une de vos clés USB en véritable cadenas numérique. Vous n'aurez qu'à la retirer pour verrouiller votre session et il vous suffira de la réinsérer pour en débloquer l'accès sans avoir à saisir de mots de passe. Il y installera une clé secrète composée de 112 caractères, lettres majuscules et minuscules, chiffres, caractères spéciaux ainsi que le nom de votre machine et la date. Ce fichier au format CTL sera régulièrement mis à jour afin d'éviter qu'une copie de votre clé serve à entrer. Vous pouvez bien sûr utiliser la clé USB comme unité de stockage puisque le logiciel ne prend que 9 Mo !

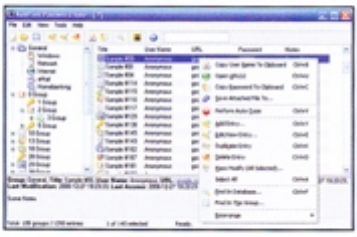
www.montpellier-informatique.com/predator

Générez vos clé WiFi
avec WiFi Key Generator

Comme son nom l'indique, WIFI Key Generator est un générateur de clés WEP/WPA/PSK. Si vous manquez d'imagination pour inventer une clé pour votre réseau WiFi, c'est la solution ! Le logiciel permet surtout de générer une clé de cryptage avec un degré de complexité suffisamment satisfaisant. Si vous avez peur qu'un malotru vous vole votre précieuse bande passante, n'hésitez plus ! WiFi Key Generator permet de générer des clés jusqu'à 256 bits. Il est également possible de rédiger une "passphrase" de 63 caractères pour qu'il puisse générer une clé correspondante. N'oubliez pas de l'enregistrer consciencieusement dans un fichier texte !

http://atlex.nl/index/wifigen

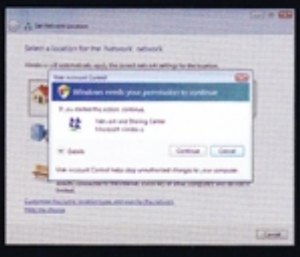
Un mote de passe général
avec Keepass Password Safe



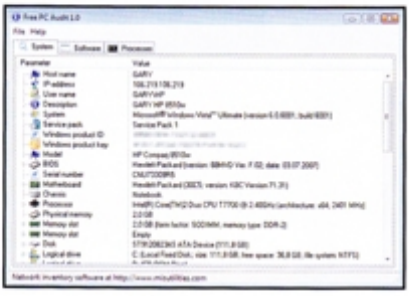
Keepass est une sorte de grand coffre-fort pour tous vos mots de passe. Il permet de stocker ces derniers dans un seul et même fichier. Utilisant les algorithmes AES et Twofish, Keepass protège toute cette base de données par un seul et unique mot de passe. Il est aussi envisageable de requérir l'utilisation d'un disque amovible (comme une clé USB). L'interface permet d'associer chaque mot de passe à une page Web, un commentaire, une date d'expiration. Il est aussi possible d'y attacher un fichier. Une fonction d'importation/exportation en mot texte ou XML permet de transférer la base de donnée depuis et vers d'autres logiciels.

http://keepass.info

Désactiver le pénible User Account Control
avec Windows Vista



Windows Vista intègre une nouvelle fonctionnalité nommée UAC (pour User Account Control). Son rôle est de contrôler l'administration de l'ordinateur en demandant une confirmation pour chaque exécution d'une tâche nécessitant un privilège élevé. Si cette fonctionnalité apporte une meilleure sécurité selon Microsoft, elle peut rapidement devenir très pénible. Pour supprimer ce fil à la patte, allez dans Démarrer, puis Panneau de configuration. Ouvrir le Panneau de configuration de Windows Vista, choisissez l'affichage classique sur la gauche et double-cliquez sur Comptes d'utilisateurs. Cliquez ensuite sur Activer ou désactiver le contrôle des comptes d'utilisateurs. L'UAC vous demandera une confirmation (la dernière !), cliquez sur le bouton Continuer. Dans la nouvelle fenêtre venant de s'ouvrir, décocher la case Utiliser le contrôle des comptes d'utilisateurs pour vous aider à protéger votre ordinateur et cliquez sur OK. Redémarrer enfin l'ordinateur !



Testez les résistances de votre PC
avec pcAudit

Si vous vous posez des questions sur la sécurité de votre PC, pcAudit est un petit logiciel très pratique. Aussi bien pensé pour les particuliers que pour les administrateurs réseau ayant des données importantes à protéger, ce dernier va envoyer des données depuis votre ordinateur vers un serveur d'Internet Security Alliance. S'il y parvient, il pourra alors déterminer les faiblesses de votre protection et vous propose une liste de conseils.

www.pcinternetpatrol.com

TOP SERVICES PIRATES

NEWSGROUPS

GIGANEWS > Usenet version «Giga»

Giganews est le leader du marché des fournisseurs d'accès à Usenet. Rapide, discret, puissant, les superlatifs ne manquent pas pour décrire ce service. Si vous ne connaissez pas Usenet, sachez qu'il s'agit d'un protocole qui permet de s'échanger des messages sur des sortes de forums. Depuis peu, Usenet est devenu l'ami des P2Pistes qui cherchaient un moyen rapide et anonyme de s'échanger des fichiers. Avec Giganews, vous bénéficiez de 14 jours gratuits alors foncez...

http://fr.giganews.com

TÉLÉCHARGEMENTS MUTUALISÉS

LEECHPACK
Tout pour «leecher» !

LeechPack, c'est le petit dernier des services de type «Seedbox» comme Furk ou Btaccel qui permet via une interface de télécharger des fichiers Torrent mais aussi des fichiers issus de RapidShare ou MegaUpload. L'intérêt d'un tel service réside dans la suppression des protocoles incriminés par HADOPI. Ce n'est pas vous qui téléchargez sur torrent ou les sites ci-dessus mais bien LeechPack, qui ensuite vous proposera un lien direct vers le fichier qui vous intéresse. Vous pouvez même éteindre votre ordinateur pendant ce temps ! Cerise sur le gâteau, le téléchargement est mutualisé. Si par exemple, vous voulez télécharger un fichier qu'un autre utilisateur a déjà récupéré, vous rapatriez directement le fichier via le protocole HTTP. Après l'offre d'essai gratuite de 3 jours, vous devrez débourser 10 € par mois pour profiter des 30 Go de stockage.

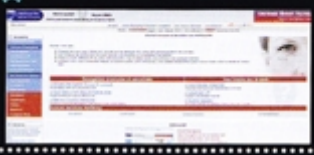
www.leechpack.com

SURF ANONYME

NETSCOP
C'est net !

La seule façon d'effectuer un surf anonyme consiste à passer par un serveur intermédiaire qui se connectera aux sites web que vous visitez à votre place et vous renverra à son tour les pages. Ce serveur est dit mandataire ou «proxy». Pour votre fournisseur d'accès vous vous connectez toujours au même serveur et pour le site distant, vous n'existez pas ! Il faudra juste s'attendre à un temps de connexion plus long car les paquets de données doivent circuler de votre ordinateur au proxy, du proxy au site web, puis la même chose en retour...

www.netscop.net



FAUSSES IP

IPFUCK > Hadopi dans la tourmente

Vous avez sans doute déjà entendu parlé du logiciel Seedfuck. Voici l'extension IPFuck pour Firefox qui débarque ! Ce plugin permet de générer de fausses adresses IP censées détourner l'attention des futurs trackers de l'Hadopi. En clair, un site ou un serveur visité va enregistrer 4 connexions différentes dont trois seront complètement fausses. Il s'agit donc d'essayer de pourrir le réseau avec des IP contrefaites et mettre la société Trident Media Guard dans l'embarras...

http://ipfuck.p4ul.info

MULTIMÉDIA TOP

TUBESURF
Recherche vidéo

Tube Surf est un moteur de recherche très intuitif qui agrège des vidéos provenant de plusieurs sites en particulier celles provenant de Yahoo, MySpace, YouTube et Google-Video. On regrette l'absence d'autres géants de la vidéo en ligne. L'interface de l'outil est aussi simple que celle de Google pour toujours autant d'efficacité.

http://tubesurf.com

MASSIVE MUSIC QUIZ
Blind test

Connaissez-vous vraiment tout dans le domaine de la musique ? Il est temps que vous passiez alors au niveau supérieur en faisant chauffer vos neurones. Un quiz grandeur nature s'offre à vous. Pour participer, il suffit simplement de vous inscrire et de choisir l'univers musical (parmi la trentaine proposée) qui correspond à vos goûts...

http://fr.massivemusicquiz.com

MEDIACONVERTER
Conversion vidéo en ligne

Plus besoin de vous prendre la tête pour convertir vos vidéos dans un format spécifique. Le site Mediaconverter vous propose de le faire en ligne quelques clics. Mediaconverter propose deux versions. La gratuite permet de uploader une vidéo de 100 Mb et d'autres options de base. En revanche, les possibilités sont plus étendues sur la version Payante.

www.mediaconverter.org

POUR TOUS VOS BESOINS, TOUTES VOS ENVIES

LE MEILLEUR DU WEB !

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !