

PIRATE

INFORMATIQUE



SEPT / OCT 09



2€
SEULEMENT

CARTES DE CRÉDIT, WIFI, PIRATES, CRYPTAGE, VPN,
DISTRIBUTEURS, P2P, VIDÉOS, EMAIL, BTACCEL,
NOTMYIP, ANONYMAT, PROXY, MUSIQUE, CRACK,
IPREDATOR, WAREZ

N° 1 EXPLOSIF !

L 12730 - 1 - F: 2,00 € - RD



**Ils veulent restreindre nos libertés
pour gagner toujours plus,**

**Ils veulent faire de demain une prison
où nous aurons le droit de nous taire,**

**Ils veulent nous transformer en veaux
consommateurs et aux ordres...**



**Ayez le courage de refuser cette situation en
votant, en vous informant, en vous instruisant
pour ne pas accepter cette fatalité!**

PIRATE INFORMATIQUE

100% LIBRE

PAGE 06-07

Qui sont
les pirates ?



PAGES 08-13

CARTES
BANCAIRES

Paiement
en ligne :
attention
danger !



Vidéo,
musique :
c'est
gratuit,
profitez en !

PAGES 14-15

PAGES 16-17

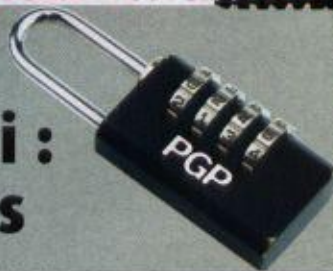
SEEDBOX

Téléchargez
en tout
anonymat
100% sur
(F**K hadopi)

I FICK HADOPI

PAGES 20-21

Anonymat garanti :
Cryptez vos emails



PAGES 26-27

Trackers
privés
Piratez
votre
ratio
torrent



PAGES 22-25

PROXY, IP, VPN :
TOUT POUR
agir à couvert
et sans risque



BTACCEL



"Piratez tout ce que vous pouvez, le reste suivra !"

LOGICIEL ANTI-PORNO : DU RÉPIT POUR LES CHINOIS

Le déploiement du logiciel de filtrage des sites pornographiques sur le territoire chinois, qui était censé commencer dès le 1er juillet dernier a finalement été repoussé par le gouvernement chinois à une date encore indéterminée. Pas de fanfaronnade cependant Messieurs les Chinois ! Un responsable du ministère de l'Industrie et de la Technologie de l'Information a précisé que "C'est juste une question de temps". Green Dam-Youth Escort, le barrage-vert, est en quelque sorte une gentille attention du gouvernement chinois pour protéger la jeunesse de son pays des dérives occidentales. On a craint un moment que le logiciel ne soit installé de force dans tous les ordinateurs. En fait les particuliers n'auront pas obligation de l'installer.



Par contre, le porno dans les espaces publics, il faut oublier. Les professeurs de l'Université du Michigan ont décelé de nombreuses failles dans le logiciel et jugent que "Si Green Dam est distribué sous sa forme actuelle, il va affaiblir de manière significative la sécurité informatique de la Chine". Selon les officiels américains et européens, sous couvert de lutte contre la pornographie, les autorités chinoises pourraient s'en servir comme moyen de contrôle et de censure. Certes...

La réponse du berger à la bergère

Suite à la plainte de l'association anti-piratage MAPINET, le ministère portugais de la culture a décidé la fermeture de 28 "sites pirates" qui annexent des données



protégées par le droit d'auteur. Bien évidemment, ce qui devait arriver...

arriva et le site de MAPINET s'est fait hacker. Pendant plusieurs heures, le site a bien malgré lui redirigé automatiquement ses visiteurs vers les plus grands sites de BitTorrent : The Pirate Bay, isoHunt and Demonoid

Alien fête ses 30 ans sur internet

A l'occasion des 30 ans du film *Alien*, un documentaire «anniversaire» est diffusé sur la toile en téléchargement gratuit. *Alien Makers* livrera aux fans de science-fiction tous les secrets du film culte. Vous pouvez le trouver sur le site d'actualité culturelle, Stars-buzz.com



L'infrastructure numérique US, une priorité nationale



Peu avant l'été, le cyber-président américain Obama a tenu un discours très attendu sur la sécurité informatique américaine : "Désormais, notre infrastructure numérique - les réseaux et les ordinateurs dont nous dépendons tous les jours - seront traités comme ils devraient l'être: comme un enjeu stratégique national. La protection de cette infrastructure sera une priorité nationale. Nous ferons en sorte que ces réseaux soient sécurisés, fiables et résistants."

Anonymat=Terrorisme ?

Au Royaume-Uni, deux individus ont été poursuivis pour avoir refusé de fournir leurs clés de chiffrement aux autorités britanniques. Elles tombent ainsi sous le coup d'une loi anti-terroriste adoptée en Octobre 2007 et risquent la bagatelle de cinq années d'emprisonnement.



ALBERT GONZALEZ : LA TENTATION ÉTAIT TROP FORTE

Un ancien informateur du gouvernement des États-Unis est suspecté d'avoir orchestré le détournement de 130 millions de comptes bancaires, entre 2006 et 2008. Albert Gonzalez, 28 ans, avait collaboré auparavant avec les services secrets américains pour les aider à capturer des pirates informatiques... avant d'en devenir un lui-même. Déjà emprisonné depuis 2008 pour des fraudes à la carte, les enquêteurs le placent maintenant au centre de la plus grande amaque à la carte bancaire jamais décelée sur le sol américain. Avec ses deux complices russes, il aurait mis au point un système très sophistiqué pour effectuer des intrusions dans les bases de données, de Payment Systems, une plate-forme de paiement, de la chaîne de dépanneurs 7-Eleven, de la chaîne de magasin d'alimentation Hannaford Brothers et de plusieurs autres grandes entreprises. Il pénétrait leurs réseaux informatiques pour y placer des mouchards. Les données pillées étaient envoyées vers des serveurs aux USA, en Lettonie, aux Pays-Bas et en Ukraine, pour y être vendues. Il encourt la prison à perpétuité.



Bagarre entre policiers et pirates australiens

La police australienne a réussi un gros coup en réalisant une pénétration toute en douceur d'un forum abritant pas moins de 5000 voyous de l'informatique pour mettre la main sur ses membres. Sauf que... l'intrusion, pas si discrète que ça, avait été remarquée et que dans le même temps un pirate avait réussi à forcer le système informatique de la police fédérale et à accéder aux preuves accumulées par les fédéraux contre les pirates du forum. Leur base de données MySQL n'était même pas protégée par un mot de passe... Du côté des pirates australiens, on est plié en quatre.



Radiohead distribue sa musique via Mininova !



Le groupe anglais est non seulement l'un des meilleurs de sa génération, mais il a aussi compris qu'à l'ère du numérique, la distribution musicale devait évoluer. Ils donnent en cadeau leur dernier single "These Are My Twisted Words" sur leur boutique Waste et ont même placé un lien direct pour le télécharger sur Mininova.org. La Major EMI qui déteste profondément Mininova doit s'arracher les cheveux. Elle s'est fait plaquer par les cinq mecs de Radiohead il y a cinq ans...

Alerte au piratage sur PayPal !

Zataz rapporte qu'un pirate sévit depuis le 18 août sur le site de paiement en ligne Paypal. "Vous nous avez informés avoir oublié votre mot de passe Paypal. Cliquez sur le lien ci-dessous pour vérifier cette adresse email et créer un nouveau mot de passe". Ne cliquez pas ! Vous seriez détourné vers un site piraté qui abrite une fausse page d'identification Paypal. Le pirate vous subtiliserait alors votre login, votre mot de passe...puis votre argent.



Le CIC dans le collimateur de pirates humoristes

Décidément la banque CIC inspire beaucoup les pirates informatiques et semble créer des vocations. Après l'attaque risible au Phishing d'un pirate analphabète (...comme ses pieds) l'an passé, le CIC a été une nouvelle fois victime ce mois d'août d'une grossière tentative de « hameçonnage » des identifiants de connexion de ses clients. La fausse page imitant le site de la banque affiche une vignette clignotante "Alerte de phishing". Il ne manque pas d'ironie celui-là...





Pirates, vous avez dit pirates ?

En automne il n'y a pas que les feuilles des arbres qui tombent. Cette année c'est aussi les premiers e-mails d'avertissement aux internautes récalcitrants qui vont tomber, puis les premières lettres recommandées, puis les premières sanctions. Et comme l'automne c'est bientôt, mieux vaut se préparer dès maintenant... et lire ce qui suit.

Toute personne commettant des délits ou des crimes dont l'objet ou l'arme est lié à l'informatique est un pirate informatique, selon la définition communément acceptée. Faire acte de cyberpiraterie, c'est s'introduire dans un système informatique, prendre connaissance, modifier ou détruire des données, sans l'autorisation explicite de ses propriétaires. Les pirates sont éclectiques et leurs activités sont diverses et variées : de la copie illicite de logiciels, à la fraude à la carte bancaire, en passant par le piratage de lignes téléphoniques et le détournements de fichiers... De la petite délinquance jusqu'à la cybercriminalité internationale.

Who's who ?

Lamers, hackers, phreakers, crackers, hacktivistes, etc. Ne les confondez pas ! Vous les chagrineriez et votre PC en serait bon pour la casse. Stop !!! Voilà déjà un cliché à briser : Tous ne sont pas de méchants voyous rêvant de chaos, de destruction et d'anarchie. Les hackers par exemple. "Hacker", le mot fait frémir ou rêver, en tout cas fantasmer. Ils forment une communauté de programmeurs expérimentés et de spécialistes des réseaux qui est apparue avec l'informatique. Au temps des premiers mini-ordinateurs

et des premières expériences de l'ARPA-net (l'ancêtre d'Internet), ils étaient déjà là. Des *hackers* ont créé Internet. Certains d'entre eux ont créé le fameux système d'exploitation *Unix*. D'autres animent *Usenet* pendant que d'autres encore font tourner le *World Wide Web*. Bref, sans eux, Internet ne serait pas Internet. Ils sont des experts des systèmes d'exploitation qui cherchent des failles de sécurité pour mettre en évidence les vulnérabilités des systèmes mais s'interdisent leur exploitation malveillante. Ils se contentent d'avertir les autorités du problème. On les appelle aussi "white hat hackers" pour bien les différencier des "black hat hackers", les "crackers", les méchants. Beaucoup moins scrupuleux, les *crackers* cherchent des failles eux aussi, mais à des fins nuisibles, souvent pour en tirer un bénéfice personnel. Parmi eux, les *phreakers* sont spécialisés dans le vol d'unités téléphoniques dans les autocommutateurs. Ce qui intéresse les *carders* c'est la réalisation de fausses cartes bancaires. Pour faire simple, **les hackers construisent, les crackers détruisent.** Comme l'informatique et l'internet s'est largement démocratisé, les prétendants au statut de *hacker-cracker* a explosé. Ces sont les *Script-kiddies*. Dépourvus de compétences techniques ces *Script-kiddies*, ou tout simplement *kiddies*, n'en ont pas moins un fort pouvoir de nuisance car ils utilisent, sans les comprendre, des scripts qui leur permettent de prendre le contrôle de leur cible. Ce sont généralement de nouveaux usagers inexpérimentés dans le domaine du *crackphreak* utilisant les mêmes outils que les "experts". Les *Lamers* aussi brillent par leur incompetence informatique mais leur



LES HACKTIVISTES ANTI-AHMADINEJAD

Alors que des émeutes secouaient l'Iran au début de l'été, un groupe d'activistes anonyme a lancé un appel au piratage de sites officiels iraniens : "A tous les pirates informatiques du monde. Vous n'aviez jamais rêvé de pirater un gouvernement Fasciste ? Voici votre chance. Aidez-nous, s'il vous plaît dans cette cyberguerre de grande envergure". Plusieurs sites référencés par le groupe ont été mis hors d'état de nuire pour un temps, dont la page officielle du président réélu, ahmadinejad.ir.



soif de destruction à coup de chevaux de Troie et de petits virus en tous genres. Les véritables *hackers* exécutent ces rigolos de l'informatique qui courent après la gloire.

Les hacktivistes

Quand "technologie" et "militantisme" se rencontrent, quand "hacker" et "activisme" se combinent, l'hacktivisme naît. Le hacking s'est peu à peu politisé et le militantisme s'est modernisé. Les hacktivistes ont compris toute la puissance qu'ils pouvaient tirer des nouvelles technologies de communication

pour véhiculer des idées boycottées par les canaux traditionnels de l'information. Ces néo-militants agissent par des opérations "coup de poing" technologiques : piratages informatiques, détournements de serveurs, remplacement de pages d'accueil par des tracts, etc. On les retrouve le plus souvent dans les luttes libertaires, anti-fascistes et altermondialistes. Les hacktivistes britanniques militants pour la cause animale sont parmi les pionniers du mouvement. Leurs actions visent régulièrement les sociétés spécialisées dans les tests de produits cosmétiques

et de médicaments sur les animaux, comme *Huntingdon*. Leur tactique ? Saturer les lignes téléphoniques, les serveurs informatiques, et même les boîtes postales. **(BOX1)** Certains hacktivistes mettent leur talent au service de mouvements religieux, d'autres se perdent dans des combats absolument farfelus et paranoïaques qui trouvent beaucoup d'échos avec les mouvements conspirationnistes très en vogue en ce début de XXI^e siècle. Enfin une partie marginale de l'hacktivisme verse dans l'extrémisme et prône la lutte armée pour faire valoir ses idées.

Les hackers de légende



Kevin Mitnick : Le plus célèbre des hackers réalise son premier coup d'éclat, mais aussi sa première détention, en s'introduisant dans un ordinateur du Pentagone en 1983. Il récidivera à de nombreuses reprises...



John Draper : aka "Cap'n Crunch" s'adonne au piratage de lignes téléphoniques à partir d'un simple sifflet offert dans une boîte de céréales. Il lance le mouvement phreaking.




Loyd Blankenship : Après son arrestation en 1986, "The Mentor" écrit "Le manifeste du hacker" qui deviendra la pierre angulaire de la contre-culture hacker.




Kevin Poulsen : L'actuel rédacteur en chef du magazine *Wired*, est arrêté par le FBI et condamné à 4 ans de prison pour ses multiples activités illégales.




Le hacking en 4 "coups




1994 : Levin réalise le plus gros "casse virtuel". Il s'infiltrer sur le réseau interne de la banque américaine Citibank, s'offre l'accès à plusieurs comptes et transfère 10,7 millions de dollars.



1999 : Jonathan James, 16 ans, s'introduit dans le réseau de la NASA, et dérobe plusieurs documents classés "secret-défense" pour une valeur estimée à 1,7 million de dollar, notamment le code source de l'International Space Station, une base spatiale.



2001 : La paranoïa anti-extraterrestres pousse Gary McKinnon à s'infiltrer chez la NASA, le pentagone, l'US army, etc. La plus grande attaque informatique contre des sites militaires de tous les temps.



2008 : Un pirate grec s'introduit dans les serveurs de Dassault Systemes et dérobe un logiciel qu'il revendra sur internet, causant des pertes pour Dassault estimées à 245 millions d'euros!



CARTES BANCAIRES

ALERTE ROUGE A LA FRAUDE !

La carte bancaire, c'est le moyen de paiement préféré des français, nous l'utilisons deux fois plus souvent que nos voisins européens. Il y a en 84 millions en circulation en France. Même si notre système de sécurité est réputé être l'un des plus sûrs au monde, il existe des failles et chaque jour on dénombre plus de six mille fraudes "à la carte" ! Au distributeur et sur Internet, comment les fraudeurs s'y prennent-ils pour mettre la main sur nos précieuses données bancaires et nous dépouiller de nos économies ?



Les techniques de piratage

A SAVOIR

Fin août, la plus grande arnaque à la carte bancaire a été révélée. Plus de 170 millions de cartes bancaires auraient fait les frais de cette arnaque. Albert Gonzalez qui a monté cette arnaque avec des complices russes devrait être condamné à la prison à vie alors que le préjudice s'élèverait à plusieurs dizaines de millions d'euros.

i

Fin le temps du vol à l'arraché, le plus souvent, votre carte est bien au chaud au fond de votre poche au moment où les voleurs vident votre compte car ils agissent maintenant tapis dans l'ombre, derrière un écran d'ordinateur. Leurs techniques sont de plus en plus sophistiquées, pour un maximum de discrétion... et un maximum de gains.

Le piratage de distributeur automatique

Le distributeur est piégé par deux dispositifs de piratage : un sur la fente d'introduction de la carte bancaire, le deuxième au niveau du clavier. Une fente pirate est installée sur la vraie, elle est équipée de capteurs qui vont intercepter les données de la bande magnétique de la

carte. Idem pour le clavier factice qui va enregistrer le code à quatre chiffres saisi par le client. Les fraudeurs les plus à la pointe n'ont même pas à se donner la peine de revenir sur les lieux du crime pour récupérer les précieux sésames, ils les transfèrent directement via le réseau téléphonique, au moyen d'une simple carte SIM de téléphone portable introduite

Distributeur piraté : Ne vous faites pas avoir !

Quand on tapote dessus, le clavier sonne creux ? Le clavier et la fente d'introduction de la carte ont un aspect plastique ? Le clavier paraît étrangement propre ou au contraire artificiellement vieilli ? Alors cet automate est suspect. A votre place, nous irions faire notre retrait ailleurs.



dans le dispositif de piratage. Il ne reste plus à nos pirates qu'à copier les données recueillies sur des cartes vierges ou périmées à l'aide d'une machine spécifique. Vous avez effectué un simple retrait au distributeur automatique, vous ne vous êtes rendu compte de rien, et pourtant, vous êtes la victime d'une fraude à la carte qui va peut-être vous coûter très cher. Plusieurs centaines de distributeurs sont piratés de cette manière chaque année. Le business est rentable, un distributeur piraté et ce sont plusieurs centaines de victimes potentielles qui se font délester d'une partie de leurs économies.

l'internaute. Parmi ces programmes, les "keyloggers" sont capables de reproduire les frappes sur le clavier de l'ordinateur fracturé et peut donc restituer au pirate les saisies de vos coordonnées bancaires. C'était la technique utilisée par des pirates informatiques arrêtés par la police tunisienne cet été, accusés d'avoir volé des milliers de données bancaires via Internet. Ils opéraient à l'aide de logiciels espions de type chevaux de Troie pour mettre la main sur les informations sensibles de leurs victimes. Pour se protéger, il faut équiper sa machine de logiciel anti-spyware (Spybot, Spyware Terminator, Trojan Remover, ...).

interface de navigation identique. Une technique qui a déjà fait plusieurs millions de victimes aux Etats-Unis et qui ne cesse de se développer, selon l'"Anti-Phishing Working group". En France, des clients de la Société Générale ont déjà fait les frais de ce type de pratiques.

Le piratage des cartes sur Internet

On achète de plus en plus sur internet : des livres, des vêtements, des billets d'avions, de l'électroménager, etc. Selon le Baromètre e-commerce de l'ACSEL, l'association de l'économie numérique, rien que sur le premier trimestre 2009, le volume de paiement effectués par cartes bancaires a été de 4 milliards d'euros pour 50 millions de transactions. En quelques secondes et quelques clics on a saisi son nom, le numéro, la date d'expiration et le code de sécurité de sa carte. Tout ce que demandent les pirates ! Pour eux, nos coordonnées bancaires sont accessibles sur internet aussi facilement qu'une recette de pâte à crêpe. Ils le disent eux-mêmes.

Les mouchards

Cette technique consiste à s'introduire "par effraction" dans l'ordinateur d'un tiers à l'aide de petits logiciels "Spywares" qui vont discrètement espionner les faits et gestes de

Comment font-ils ???

La fraude peut se faire à trois niveaux :

- En amont, au moment de la saisie clavier des données, grâce à l'intrusion d'un spyware dans votre ordinateur
- En interceptant vos informations sur de faux sites pour des magasins inexistantes ou sur des interfaces factices imitant des sites bien réels.
- En aval, en s'introduisant dans des serveurs mal-sécurisés de site de vente à distance notamment pour subtiliser les coordonnées bancaires de ses clients

Le phishing

Le phishing est une forme de piraterie très dangereuse qui consiste pour un pirate à intercepter à l'insu de l'internaute ses données bancaires en fabricant un site miroir qui laisse croire à l'internaute qu'il est sur le site web de sa banque alors qu'il est en réalité sur un site factice doté d'une

Craquer la porte de l'arrière-boutique

Les coordonnées bancaires des clients de sites de vente à distance sont stockées dans des serveurs sécurisés, en théorie. Si le serveur d'un de ces sites est mal sécurisé ou qu'un cracker un peu doué a décidé de forcer la porte pour s'introduire dans l'arrière-boutique, toutes les données bancaires de ses clients se retrouvent à sa merci. En quelques minutes, le pirate peut faire main-basse sur un véritable trésor de guerre. Une fois son forfait accompli, il a deux possibilités : se servir lui-même des données piratées pour effectuer des achats sur internet qu'il fera livré à une adresse anonyme ou, et c'est le cas le plus courant, il les revend. A qui et comment ? Rien de plus simple. A des personnes tierces, originaires des quatre coins du monde, rencontrées sur des forums d'un type un peu particulier, sorte de grandes brocantes en ligne pour gangsters numériques où s'achètent et se vendent des données bancaires piratées. On y trouve tout l'arsenal commercial traditionnel pour attirer le chaland : réductions, promotions, prix de gros, etc. Le prix des données dépend avant tout du pays de localisation du détenteur de la carte. On y négocie, en chattant, des numéros de cartes pour des prix pouvant descendre à un dollar l'unité ! Oui, pour ces requins du piratage c'est tout ce que vaut le contenu de votre compte... 5 ans d'emprisonnement et 375.000 euros d'amende, c'est ce qui leur pend au nez si jamais ils se faisaient attraper. S'ils continuent, c'est que le business doit être vraiment juteux.



Etat des lieux de la fraude à la carte SUR INTERNET

Selon le rapport annuel de l'"Observatoire de la sécurité des cartes de paiement" de la Banque de France, le taux de fraude à la carte pour l'année 2008 a augmenté par rapport aux années précédentes. Sur internet, le risque est beaucoup plus élevé, surtout les transactions vers les sites étrangers.

Le taux de fraude s'établit à 0,069% du total des transactions par carte, en légère augmentation par rapport à l'année 2007 où il était de 0,062%. Plus concrètement : Sur dix-mille opérations, sept sont frauduleuses. C'est peu et cela a fait dire au président de l'observatoire et gouverneur de la Banque de France Christian Noyer, lors de la présentation du rapport que : "La fraude sur les transactions par carte reste globalement bien maîtrisée en France". Sauf que le montant des fraudes s'élève à 320,2 millions d'euros ! (contre 268,5 millions en 2007).



Sur Internet, ce n'est pas une surprise, le risque de fraude augmente considérablement, 0,235%, soit 2,3 transactions sur 1000 effectuées sont frauduleuses. C'est 15 fois plus que pour les paiements de proximité et sur automate (réalisés au point de vente ou sur distributeurs de carburant, de billets de transport...) !! Le taux de fraude sur internet a un peu diminué en 2008 par rapport à l'année précédente mais, en volume, son préjudice a augmenté de 47% !

Que dit la loi ?

La "loi sur la sécurité quotidienne (LSQ)" du 15 novembre 2001 a mis en place "L'Observatoire de la sécurité des cartes de paiement". Depuis son entrée en vigueur, le détenteur d'une carte bancaire peut contester les opérations frauduleuses effectuées à distance. Il doit pour cela faire opposition par lettre recommandée avec avis de réception auprès de sa banque qui se trouvera alors dans l'obligation de recréditer le compte de son client dans un délai d'un mois à compter de la réception de la lettre et de rembourser les frais d'opposition et de renouvellement de la carte. La victime d'une fraude dispose de 70 jours à compter de la date de l'opération contestée pour faire une réclamation.



320 millions d'euros fraudés en 2008 !

Sur Internet, le risque de fraude est 15 fois plus élevé !

Entre 2007 et 2008, le montant des fraudes sur Internet a augmenté de 47% !

Les pièges à éviter

Les paiements effectués à distance (par internet, courrier ou téléphone) sont les plus risqués en termes de fraude. Dans le secteur de la vente à distance, toutes les branches ne sont pas touchées de manière équivalente. La branche "téléphonie et communication" a un taux de fraude deux fois supérieur à la moyenne de l'ensemble des paiements à distance. Les branches "santé, beauté, hygiène", "Equiperment de la maison, ameublement" sont aussi particulièrement exposées au risque de fraudes. A l'inverse, les branches "Assurances", "Alimentation" et "Jeux en ligne" apparaissent beaucoup plus sûres pour vos transactions bancaires en ligne.

Les transactions vers l'international, le point noir

Si vous effectuez un paiement sur Internet par carte bancaire sur un site étranger...croisez les doigts ! Presque deux transactions sur cent de ce type se soldent par une fraude ! 1,81% très précisément. Le montant du préjudice s'élève à 56 millions d'euros. La progression est très forte par rapport à l'année précédente où il était de 27,4 millions. Par rapport à une transaction en ligne effectuée entre un émetteur et un récepteur français, une transaction vers un site internet étranger est huit fois plus risquée.

Une transaction est huit fois plus risquée vers un site internet étranger !

Quelles solutions ?

Les sites marchands de vente à distance commencent pourtant à faire des efforts pour sécuriser les données bancaires de leurs clients en cryptant les données ou en octroyant au client un code d'identification qui n'est valable que pour une seule transaction après laquelle il est détruit. De leur côté, les banques ont ajouté un cryptogramme visuel à trois chiffres au dos de notre CB censé limiter le risque de fraude. Mais les failles sont nombreuses. En théorie, depuis le 1er janvier 2004 les sites marchands doivent systématiquement demander ce sésame au client pour valider une transaction. En pratique, on l'a tous constaté, ce n'est pas toujours le cas. La CNIL (Commission Nationale Informatique et Liberté) leur interdit de conserver ce cryptogramme dans leur base de données afin d'éviter qu'ils ne soient subtiliser en cas d'intrusion de pirates. Sauf si vous payez en plusieurs fois... De toute façon, ce cryptogramme n'est pas une protection inviolable pour des bandits de grands chemins.

"e-Carte Bleue" et "Payweb", des cartes bancaires virtuelles

Carte Bleue Visa a conçu un service e-Carte Bleue dédié aux achats en ligne sur des sites de vente à distance. A chacun de ses achats, l'internaute obtient en temps réel un nouveau e-numéro de carte, une date de validité et un numéro cryptogramme qui ne seront valides que pour un achat unique. Il permet donc d'acheter sur Internet sans jamais avoir à jeter en pâture sur la toile son numéro de Carte Bleue. Tous les achats effectués par e-Carte Bleue sont couvertes par les assurances affiliées à sa carte. Pour en bénéficier, il faut s'inscrire auprès de sa banque et télécharger le logiciel e-Carte Bleue. Mais tous les établissements bancaires ne proposent pas encore ce service, qui n'est d'ailleurs pas toujours gratuit. Il ne permet pas de régler des abonnements ayant des prélèvements périodiques ni de payer un service ou un produit qui nécessite la présentation de la carte bancaire réelle pour retirer la prestation. Le service "Payweb" fonctionne sur le même principe.



CB et sécurité : "sesame, ouvre toi !"

Au pays de la carte à puce, remettre en cause la sécurité de nos cartes bancaires est hautement tabou. Pourtant, une course folle est engagée entre les chercheurs en cryptologie, les autorités de contrôle...et les pirates. Son enjeu ? Notre argent !

Malgré les avertissements des spécialistes sur l'obsolescence de leur système face aux techniques modernes, le groupement interbancaire (GIE), l'organisme qui certifie les cartes bleues françaises, a utilisé plus de 15 ans durant un système prévu initialement pour ne durer que 5 années. Une négligence qui a failli nous coûter très cher... A la fin des années 1990, un développeur en informatique, Serge Humpich trouve la faille. Il tente alors de monnayer sa découverte auprès du GIE, qui préférera finalement l'attaquer en justice. En 2000, il est jugé et reconnu coupable de « falsification de cartes bancaires et d'introduction frauduleuse dans un système automatisé de traitement » et condamné à 10 mois de prison avec sursis. Quelques mois

après sa condamnation, il affirme : "Le GIE ne connaît pas les véritables faiblesses de son système. Une fraude à grande échelle est toujours possible." En cassant la protection logique employée sur les cartes bancaires françaises, Serge Humpich a mis

en évidence des failles techniques et de conception à corriger dans les cartes bancaires, censées être inviolables. Il a démontré la vulnérabilité générale du système qui régit les transactions des millions de cartes en circulation dans l'Hexagone.

La Carte Bleue en 10 dates

1967: Six banques créent la première carte de paiement en France : la Carte Bleue

1971: Apparition des pistes magnétiques sur les cartes et des premiers distributeurs automatiques

1973: Carte Bleue s'associe avec la société Bank Americard qui deviendra Visa, le plus important système de paiement par carte au monde

1986: La France joue un rôle de pionnier mondial avec l'introduction de la carte puce



La Yescard, la carte qui dit toujours "OUI".

C'est une carte à puce développée en 2001 par un groupe de hackers, vierge à l'origine, dans laquelle un programme et des données spécifiques sont programmées par un pirate. Elle se comporte comme un émulateur de carte bancaire dont la puce répond "OUI" quelque soit le code PIN à quatre chiffres saisi (Personnel Identifier Number), qui permet d'identifier le porteur de la carte.



Et aujourd'hui ? Et demain ?

Nos CB sont sécurisées par un cryptosystème qui permet de former une signature qui authentifie la carte bleue. Pour combler la faille découverte par Humpich, le GIE a été contraint de le renforcer en passant d'un système de cryptographie basé sur un algorithme de 96 chiffres au moment du hacking, soit 320 bits, à 230 chiffres, soit 768 bits. Parallèlement, l'ensemble des terminaux de paiement du système a dû être mis à jour, une opération qui a coûté plusieurs millions d'euros. En 2005, un laboratoire allemand a réussi à factoriser un nombre à 200 chiffres, comme l'avait fait Humpich pour les 96 chiffres. Alors combien de temps avant que des chercheurs mal-intentionnés ne parviennent à dépasser le GIE et à hacker notre système de paiement par CB ? Face à l'obsolescence des systèmes de sécurité en comparaisondes moyens dont disposent des pirates toujours plus à la pointe de la technologie et à la multiplication des fraudes, un nouveau standard international de carte à puce est entré en vigueur : le standard EMV, pour Europay, Mastercard,

Visa. Il a été adopté en France en 2004 et se déploie progressivement à tous les pays d'Europe. Outre une compatibilité totale entre les différents réseaux de carte bancaire, il renforce la sécurité de la carte bancaire française notamment par le biais de l'authentification du porteur de la carte. Selon des informations que la BBC s'est procurée au moi de mai dernier, VISA est en train de tester "Emue" une carte bancaire plus sécurisée en ce qui concerne surtout les paiement sur internet. Elle est dotée d'un petit écran qui génère un code aléatoire unique à chaque utilisation. Si sa technologie est concluante, elle pourrait être commercialisée dès la fin de l'année. Une vingtaine d'ingénieurs et d'anciens pirates de cartes bancaires travaillent en permanence à rechercher et à combler les failles de notre système. De leur côté, les pirates ne relâchent pas la pression, apâtés par des transactions en ligne qui ne cessent d'augmenter. Ils se livrent une véritable course technologique. Une course qui n' a pas de ligne d'arrivée. Soyez prudents !



Le grand casse de Maksym Yastremskiy

Le FBI était à ses trousses depuis déjà plusieurs mois quand Maksym Yastremskiy, plus connu sur la toile sous le pseudonyme de Maksik, a été arrêté dans une station balnéaire du sud de le Turquie en 2007. Ce pirate informatique, un ukrainien de 25 ans, s'était spécialisé dans la "capture" et la revente de données bancaires sur Internet. Il a plusieurs dizaines de milliers de victimes à son actif ! Le "casseur du siècle" passera les trente prochaines années dans les geôles tuques. Pas sûr qu'elle soient équipées d'une connexion Internet...

1993: Toutes les cartes bancaires françaises sont équipées d'une puce pour accroître leur sécurité

1997: Serge Humpich trouve une faille et fabrique les premières cartes doubles

2000: un cyber-pirate diffuse en ligne la clé fissurée de la CB sur Internet

2001: un groupe de Hackers développe des CB pirates, les "Yescard"

2002: Développement des e-Carte Bleue pour le paiement sécurisé sur internet

2002: Nouveau standard international EMV sécurisant les cartes à puce



ZIK Musique à volonté pour pirates repentis

Avec la répression qui promet de frapper de plein fouet tous les amoureux de la culture libre et du téléchargement, de nombreuses offres permettent de ne plus enfreindre les lois dictées par la dictature des lobbies, pardon je voulais dire les lois de la république sarkozienne. Pour des prix modiques ou même gratuitement vous pouvez désormais écouter à volonté et ainsi devenir un pirate repenté qui échappera au gendarme Hadopi...

WorMee

Impensable pour Orange de passer à côté du marché de la musique en streaming. L'opérateur vient de lancer sa propre plateforme pour concurrencer directement Deezer.

www.wormee.com

Deezer

Puisqu'on en parle... Pour sa 3^e version, le site s'est refait une beauté et a ajouté quelques fonctionnalités comme un égaliseur audio. Son catalogue de 4 millions de titres augmente à chaque nouvel accord avec les Majors.

www.deezer.com

Playlist

40 millions de fans s'échangent de la musique sur ce gigantesque Juke-Box.

www.playlist.com

Airtist

Visionner une publicité de 30 secondes en échange d'un téléchargement de mp3. Un service intéressant, mais dont la gratuité est toute relative. www.airtist.com

SkreemR

Un moteur de recherche de MP3 qui permet l'écoute en streaming et donne les liens directs pour télécharger les fichiers.

www.skreemr.com

Microsoft ?

Le mastodonte aussi se lance dans le streaming ! «Le site sera similaire à Spotify» annonce sa direction. Sera-t-il disponible en France?

Spotify

C'est peut-être le meilleur service de musique en ligne. Son environnement graphique inspiré d'iTunes est très réussi (normal, c'est suédois...) mais ce qu'il le distingue



le plus de ses concurrent c'est qu'il s'agit d'un logiciel à installer sur son PC et pas d'un site à ouvrir dans un navigateur. Basé sur la technologie P2P, les morceaux sont lancés presque instantanément et leur qualité sonore surclasse celle de tout les autres sites comparables. Quant aux catalogues...il compte six millions de titres. Demandez vite une invitation pour accéder à sa version bêta !

www.spotify.com

Jamendo

Deezer, Wormee, Beezik, ...tous ces sites jouent à fond le jeu des Majors et de la propriété intellectuelle. Jamendo ne mange pas de ce pain là et propose à l'inverse de la musique en licence ouverte. Les artistes mettent leurs albums à disposition sous des licences de type Creative Commons et Licence Art Libre. Ils sont rémunérés grâce aux dons des utilisateurs, au partage de 50% des revenus publicitaires du site et à la vente de licences d'utilisation commerciales de leur musique. Artistes membres de sociétés d'auteurs comme la SACEM, dégagez ! Jamendo permet l'écoute directe de fichiers audios, le téléchargement direct d'albums et leur diffusion sur les réseaux P2P. 10.000 albums sont dispo. Sympa.

<http://www.jamendo.com>



Beezik, le dernier buzzzzz

Lancé en juin dernier avec fracas, Beezik est la sensation de l'été. Attention, il ne s'agit pas ici de streaming mais de téléchargement, gratuit et légal. Gratuit car le site

tire ses revenus de la publicité et légal car il multiplie les accords avec la SACEM et les principales maisons de disques. Son catalogue est riche de deux millions de titres qui correspondent, selon Beezik, à 75% de l'offre présente sur les réseaux P2P, et envisage atteindre 90% rapidement. Le deal est simple : Avant de pouvoir télécharger un morceau, l'internaute choisi parmi quatre une publicité de dix à quinze secondes qu'il doit visionner. N'en profitez pas pour aller aux toilettes, vous devez vraiment la regarder. La faute à un système de contrôle ingénieux qu'on vous laisse découvrir... Pas question par contre de laisser les internautes exploiter les titres téléchargés ! Ils sont au format WMA de Microsoft et verrouillés (DRM) pour limiter leur copie. Chaque titre peut être transféré cinq fois sur PC, sur portable ou sur baladeur (pas de gravure sur CD). Plus anecdotique: chaque téléchargement donne droit à un certain nombre de points à dépenser auprès de sites de vente partenaires.

<http://www.beezik.com>



Véritable phénomène de société qui a véritablement explosé en quelques années, les services de vidéos sont désormais nombreux et vous pourrez trouver de tout. De la parodie au film, en passant par vos séries préférées, rien n'y échappe. Et si vous trouvez le contenu de certains trop aseptisé, tournez vous les russes de RuTube où la censure n'opère encore pas !

Nous avons misé sur le qualitatif et les sites moins connus.

METACAFE : Sur le podium

C'est le 133^e site le plus consulté au monde selon le classement Alexa et il est en troisième position pour les sites communautaires de partage de vidéos. Comme avec ses grands frères Youtube et Dailymotion, on peut uploader, visionner et partager des vidéos-clips. Il est relativement proche de ces sites à quelques différences près quand même: son système de référencement met plus



en valeur les vidéos selon le nombre de fois où elles ont été visionnées. Le site s'est fait connaître et s'est démarqué vraiment des autres en remettant des récompenses aux producteurs des vidéos les plus vues. Une distinction qui n'a plus l'air d'être encore d'actualité malheureusement...

www.metacafe.com

RUTUBE : pas une version russe de Youtube !

Alors évidemment c'est en russe... et c'est un problème pour les non-russophones, relativement nombreux en France. Pourtant le problème est largement surmontable une fois que le bouton «Rechercher» a été localisé. Le contenu francophone est limité mais si vous comprenez l'anglais, alors vous aurez la possibilité de visionner toutes vos séries favorites.

Surtout ne pas confondre Rutube avec une simple version russe de Youtube ! Alors que les grands sites du streaming vidéo sont de plus



en plus frileux sur la question du respect des droits d'auteurs, Rutube semble sourd aux invectives des ayants-droits. Vous trouverez donc nombre de vidéos que vous ne verrez pas ailleurs.

<http://rutube.ru/>

Facebook+Youtube= BEBO

BeBo est surtout connu dans le monde anglophone où il compte 25 millions d'utilisateurs (il est même numéro un en Irlande) mais il est aussi disponible depuis peu en version française. C'est un site communautaire qui a le culot de vouloir concurrencer Facebook



et Myspace et de faire évoluer le concept de réseau social vers le partage de contenu et notamment l'aspect vidéo.

www.bebo.com/

VIDEO

Visionnez ce que vous voulez, quand vous voulez !

YOURFILEHOST

Un hébergeur de fichiers en tout genre mais surtout de vidéos qui fait un carton au Japon mais reste encore peu connu par chez nous. Il semble s'être peu à peu spécialisé dans les vidéos «hard».

www.yourfilehost.com

VODAA

Il passe pour être un des métamoteurs de recherche de vidéo les plus efficaces. Son but est d'obtenir un résultat de recherche pointu, plutôt que de cataloguer toutes les vidéos des sites scannés.

www.vodaa.fr

REDTUBE

Une alternative à Youporn a envisagé avec le plus grand sérieux. Si l'on a plus de dix-huit ans seulement évidemment... www.redtube.com

YOUTOMB

Un projet initié par des étudiants américains qui recense les vidéos qui ont été effacées de Youtube pour des violations de copyright. Malheureusement on ne peut pas visionner les vidéos en question, seulement voir des captures d'écran et plein d'infos qui permettent d'en savoir un peu plus sur les mécanismes de la censure sur internet. <http://youtomb.mit.edu>

HULU

un site gratuit de vidéos à la demande lancé par News Corp., NBC Universal et Walt Disney qui diffuse les meilleures séries américaines (Heroes, Prison Break,...) et certains films de ces groupes médias. www.hulu.com

CRACKLE

Connu sous le nom de «Grouper» jusqu'en 2007, Crackle, propriété de Sony, diffuse des films détenus par la marque mais se veut surtout un tremplin pour jeunes artistes-internautes : il leur permet de diffuser leur propres vidéos et les met en relation avec des artistes confirmés signés sur la Major.



F...K HADOPI

Rien de plus facile avec une seedbox !

Avis aux téléchargeurs en série, aux fondus du P2P ! Il existe des solutions pour télécharger plus rapidement que jamais sur le Net: les seedboxes ! Après un carton aux Etats-Unis, elles se répandent maintenant en Europe.

Une seedbox est un serveur dédié équipé d'une ligne à haut débit en fibre optique qui permet des vitesses de téléchargement à des vitesses que des connexions lambda ne peuvent atteindre, 100Mbps/s au minimum ! On les utilise exclusivement pour les téléchargements BitTorrent. Ce sont en quelque sorte les Formules 1 du BitTorrent. Les fous du peer-to-peer ont donc maintenant la possibilité de télécharger un film en moins de 3 minutes avec une seedbox. Le serveur de la seedbox prend en charge la récupération sur son serveur des fichiers, via BitTorrent. Une fois que le torrent est téléchargé sur la seedbox, il vous suffit de rapatrier sur votre PC le fichier stocké sur le site. A ce moment là, la vitesse de téléchargement direct des données présentes sur votre seedbox vers votre ordinateur dépend bien entendu de votre propre bande passante (donc de votre box ADSL ou de votre modem). Le hic c'est que ces services ne sont pas gratuits et les prix sont parfois même assez prohibitifs. Ils varient en fonction des capacités de stockage du serveur et de la taille de la bande passante. Mais avec la multiplication des sites de locations, ils devraient s'orienter à la baisse rapidement et pourquoi pas devenir gratuits un jour ou l'autre.

Les avantages d'une seedbox

Outre la vitesse de téléchargement ultra-rapide qu'elles autorisent, les seeboxes ont suffisamment d'atouts pour s'imposer rapidement comme des solutions incontournables pour le téléchargement en P2P.

Sur les sites de P2P, les seedboxes permettent d'uploader à la même vitesse que le téléchargement, donc très rapidement. Comme la performance de vos téléchargements de torrent dépend, entre autre, du ratio entre les données que vous seedez (que vous mettez à disposition des autres utilisateurs) et que vous téléchargez, vous serez rapidement le roi des trackers et votre vitesse de téléchargement sera encore accélérée.

C'est la compagnie qui gère votre seedbox qui prend en charge les téléchargements, pas votre PC. Vous pouvez donc télécharger non-stop sans obstruer votre bande-passante.

Si votre fournisseur d'accès à Internet décidait de brider votre connexion et de limiter la quantité d'informations téléchargées par P2P, cela n'aurait aucune incidence sur votre seedbox car la location du serveur inclue aussi la

ASTUCE: LOUER UNE SEEDBOX A PLUSIEURS

Vous pouvez partager votre seedbox avec plusieurs personnes pour faire baisser les coûts de location en partageant simplement les logins et mots de passe.

A SAVOIR

Les +

- vitesse de téléchargement indépendant de votre connexion normale et de votre FAI

Les -

- les prix pas encore toujours abordables
- les meilleurs sites sont pris d'assaut
- manip' pas très évidentes pour les novices



location de la connexion par fibre optique qui n'est pas liée à votre FAI. Cela implique donc aussi une plus grande sécurité vis à vis des espions.

Nos conseils pour choisir une seedbox

Il y a plusieurs critères à étudier avant d'opter pour une seedbox:

Le prix: Les tarifs s'échelonnent pour la plupart des offres entre une quinzaine et une centaine d'euros. Si vous êtes riches vous trouverez même des offres de plusieurs centaines d'euros. Dans le cas contraire, souvenez-vous qu'une solution alternative consiste à partager une seedbox entre plusieurs utilisateurs. Notez aussi que ces services étant souvent États-Uniens, les prix sont presque toujours annoncés en dollar USD.

La taille du serveur: Il est possible de louer des serveurs avec une capacité de stockage limitée, de l'ordre d'une dizaine de Gb. Beaucoup d'offres proposent des disques durs de tailles avoisinant les 250GB, mais si vos moyens vous le permettent, et que vous en trouvez l'utilité, vous pouvez tout à fait louer des serveurs de 2000 Gb.

La taille de la bande passante: Elle conditionne la vitesse de chargement. Plus elle est élevée, mieux c'est. Des services offrent une bande passante de 100Mb/s, 200Mb/s, 1000Mb/s, et on vous annoncera souvent une bande passante illimitée.

Le nombre de torrents actifs simultanément:

La plupart des offres n'ont pas de restriction de trafic, mais certaines limitent le nombre de torrents actifs simultanément sur votre seedbox à moins de dix et parfois même seulement deux.

Les meilleures seedboxes

> Torrentflux



C'est sans discussion le plus populaire

des services de location de serveur de type seedbox. Pour seulement 5, 9 ou 15 USD par mois vous pouvez utiliser respectivement 2, 4 et 7 torrents simultanés. Une aubaine face à d'autres solutions souvent plus chères...qui va vous demander un peu de patience... car les inscriptions sont fermées et il faut s'inscrire sur une liste d'attente avant de profiter de ces services. www.torrentflux.com

WewillHostIt



Un Giga bite de stockage revient en gros à 1\$.

10GB pour 12\$, 20GB pour 20\$. La taille maximale de serveur étant de 55GB. Le nombre de transferts de torrent en simultané est illimité.

<http://wewillhostit.com/>

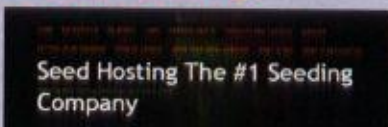
Seedbox Hosting

SeedboxHosting.com

Create content for your torrents

"Votre seedbox va envoyer votre ratio dans la stratosphère", c'est le site qui l'affirme. La bande passante et le nombre de fichiers torrent sont illimités. Pour 47 USD par mois vous aurez droit à 100Gb de stockage contre 1000Gb si vous vous fendez de 97 USD mensuels. Votre seedbox est accessible dès le paiement effectué, contrairement à beaucoup d'autres services où le délai est souvent de 48h. <http://seedboxhosting.com/seedbox/>

Seed Hosting



Deux possibilités s'offrent à vous : 45Gb de stockage et un maximum de 10 torrents

actifs simultanément pour 37 USD mensuels ou 100Gb et jusqu'à 20 torrents actifs pour 60 USD. La bande passante est de 100Mb/s dans les deux cas.

www.seed-hosting.com

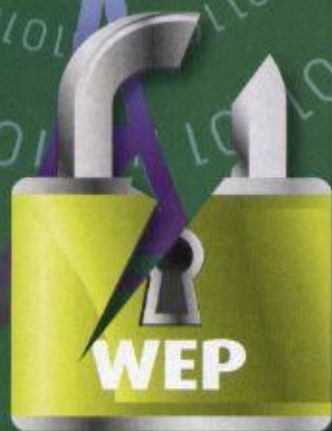
HADOPI



Cracker sa connexion WIFI !



Pour tester son niveau de sécurité



Votre connexion Wifi WEP est-elle réellement sûre ? Des pirates pourraient-ils un jour profiter d'une faille et s'introduire à votre insu sur votre réseau ? Le meilleur moyen de le savoir, c'est encore d'essayer soi-même de cracker sa propre connexion. Nous avons débroussaillé les meilleures pistes à suivre pour effectuer ce test de sécurité. Vous risquez d'avoir des (mauvaises) surprises !

PASSER AU WPA : EXEMPLE DE LA LIVEBOX

La plupart des équipements récents ont la capacité de protéger votre réseau avec le protocole WPA mais c'est à vous de le choisir et de le configurer. Dans l'interface de la Livebox, cliquer sur le menu «Réseau sans fil», puis dans la rubrique «Paramétrage du réseau sans fil» sélectionnez «WPA» dans la liste déroulante «Sécurité». Cliquez ensuite sur «Configuration WPA», saisissez une passphrase complexe et définissez le mode d'encryptage «AES» ou à défaut «TKIP».



Tous les équipements WIFI intègrent un système de chiffrement des données censé protéger des intrusions par des personnes extérieures au réseau. Ce protocole de chiffrement et d'authentification est le WEP, pour Wired equivalent privacy. Il s'appuie sur des mécanismes qui souffrent de graves lacunes de sécurité. Demandez à des sociétés comme TJX ou bien d'autres encore qui se sont fait littéralement piller par des pirates informatiques ! Bref, le WEP est une vraie passoire ! Pourtant il est encore très utilisé et reste le choix de chiffrement par défaut sur la plupart des équipements.

Les failles du WEP

Une clé WEP n'est pas régulièrement modifiée ce

qui laisse le temps à un pirate d'écouter et d'analyser les données échangées pour en déduire votre clé WEP. Pour colmater cette faille, ou plutôt cette crevasse du WEP, vous pouvez, faute de mieux, changer régulièrement votre clé, chaque semaine au minimum.

Du WEP au WPA : Les alternatives

L'utilisation d'un Virtual Private Network (Lire les pages 22 et 23) est une solution à envisager pour crypter vos données WEP et ainsi renforcer la confidentialité des échanges sur votre réseau mais il le ralentira à coup sûr. A l'heure actuelle, la solution la meilleure... disons la moins mauvaise et la plus simple à mettre en œuvre, c'est de passer aux

protocoles Wi-Fi Protected Access WPA ou WPA2. Ces protocoles de chiffrement ne sont pas inviolables mais ils sont plus récents et comblent la plupart des failles majeures du WEP, en renforçant notamment le chiffrement des données et l'authentification de leurs utilisateurs. Une clé WEP fait généralement 64 bits. Elle est composée d'une clé de chiffrement de 40 bits et d'un vecteur d'initialisation de 24 bits. WPA renforce le chiffrement de la clé qui passe à 128bits et le vecteur d'initialisation à 48bits. Mais le plus important c'est que sa clé temporaire est aussi modifiée régulièrement alors que celle associée au WEP est statique. WPA fournit une authentification au niveau de l'utilisateur qui se connecte à un réseau WiFi.



CHIFFRER ET DÉCHIFFRER

ses emails



chiffrer et
déchiffrer

Nous vous proposons d'apprendre à chiffrer/déchiffrer un texte et de signer/vérifier sa signature avec le système de cryptographie PGP (pour "Pretty Good Privacy") qui utilise la cryptographie à clé publique, qu'on appelle aussi chiffrement asymétrique. Le système génère une paire de clés : une clé publique et une clé privée. La clé publique est connue de tous alors que la clé privée n'est connue que de la personne à qui la paire de clés appartient. Seul le possesseur de la clé privée peut déchiffrer le message, c'est pourquoi il ne faut en aucun cas donner ou perdre la clé privée. Pour chiffrer et déchiffrer un message, vous avez besoin de votre clé privée ET de la clé publique de votre destinataire.

Avec FireGPG, vous pouvez faire deux choses : signer votre message ou le chiffrer, ou les deux à la fois. Signer son message n'a pas pour effet de chiffrer son contenu mais authentifie que vous êtes son émetteur. Vos messages

Yahoo!, Gmail, Hotmail, etc, presque tout le monde utilise ce type de webmail. C'est peu de chose de dire qu'elles sont vulnérables, ce sont de vraies passoires ! La Poste conserve-t-elle pendant un an des doubles de vos courriers ? C'est pourtant ce que font les FAI... A l'ère hadopienne, il vaut mieux se protéger, alors lisez ici comment chiffrer vos emails.

sont signés avec votre clé privée alors que votre clé publique permet aux destinataires de vérifier votre signature. Le chiffrer le rendra illisible à un éventuel espion, une "personne du milieu".

Les préparatifs : installer le matériel de cryptage

Nous allons utiliser FIREGPG, une extension pour Mozilla Firefox qui utilise le programme de cryptage "GNU Privacy Guard" pour traiter tout texte saisi dans Firefox, dont vos emails (Pour Mozilla Thunderbird, c'est l'extension Enigmail qu'il vous faut). L'installation ne pose aucun problème particulier, mais assurez-vous quand même à ne pas modifier le chemin d'installation par défaut car cela pourrait vous causer des soucis par la suite (C:\Program Files\GNU\GnuPG).

Pour trouver le plugin FIREGPG, c'est ici : <http://fr.getfiregpg.org/s/install>
Pour installer GnuPG, c'est par là : www.gnupg.org/download/index.en.html

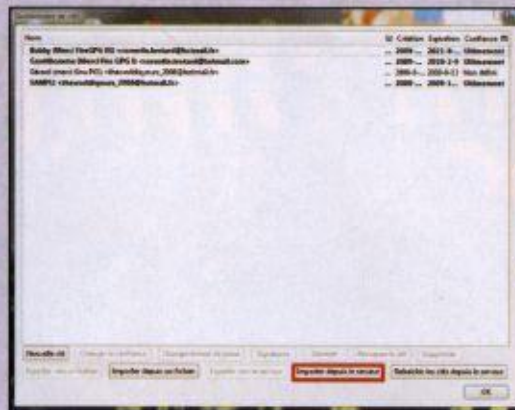


Démonstration : Chiffrez votre 1^{er} email !

Après avoir installé FireGPG puis GnuPG, dans Mozilla Firefox, cliquez sur l'onglet "Outils", puis ouvrez le menu "FireGPG", puis "Gestionnaire de clés" et cliquez sur "Nouvelle clé". La fenêtre suivante s'ouvre. Renseignez votre nom, votre email, choisissez un mot



de passe (solide si possible, avec moult chiffres et lettres, minuscules et majuscules). Définissez la durée de validité de votre clé. Vous avez la possibilité de choisir la longueur de la clé de chiffrement mais plus le cryptage est fort et plus la clé mettra du temps à se générer. Cliquez sur "Générer la clé". Firefox est sympa et vous conseille d'aller vous dégourdir les jambes ailleurs le temps pour



lui de faire son boulot.

Votre paire de clés est créée. Avant d'établir des communications chiffrées, vous devez partager votre clé publique avec vos contacts et importer les leurs. Utilisez pour cela les options "Exporter" et "Importer" du menu "FireGPG". Vous avez deux possibilités pour échanger vos clés : via le serveur ou en important/exportant par fichier que vous pourrez échanger en pièces jointes d'email, mais ce n'est pas la solution la plus sûre. Vous l'avez compris, pour recevoir vos messages secrets, vos contacts devront eux aussi en passer par ce petit tutoriel et installer le programme GnuPG et l'extension FireGPG.

L'étape finale

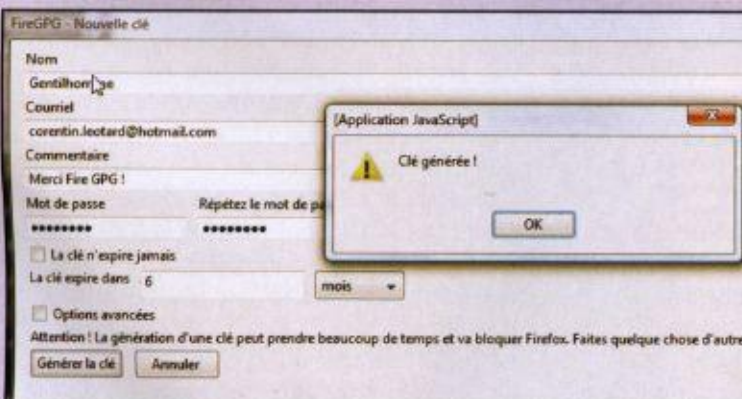
Préparez une belle lettre électronique à envoyer à votre meilleur copain, via votre webmail habituelle. Sélectionnez le texte que vous voulez garder

top-secret. Dans le menu "Outils" de Firefox, ouvrez le menu "FireGPG" et choisissez l'option "Chiffrier". Vous devez saisir votre mot de passe et sélectionner la clé publique du destinataire, votre meilleur copain, qu'il vous aura transmise au préalable.

Le texte que vous avez écrit est alors chiffré ! Il sera tout aussi simple de déchiffrer les messages qu'il vous enverra à son tour : "Outil", "FireGPG" puis

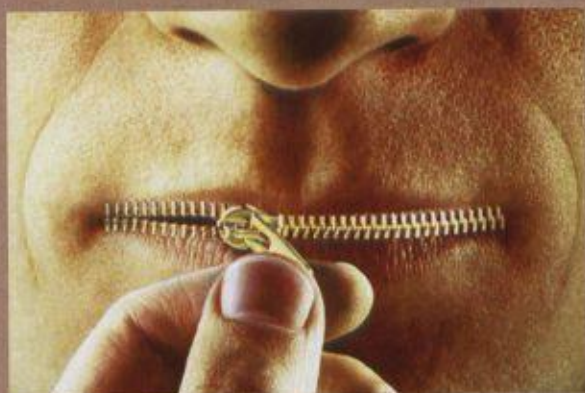


"Déchiffrer". Pour signer en plus vos messages, la procédure est la même, sauf que vous devez choisir l'option "Signer et chiffrer". Dans ce cas, FireGPG vous redemandera de saisir votre mot de passe.



Hadopi contourné !

en 1 mn !



En automne il n'y a pas que les feuilles des arbres qui tombent. Cette année c'est aussi les premiers e-mails d'avertissement aux internautes récalcitrants qui vont tomber, puis les premières lettres recommandées, puis les premières sanctions. Et comme l'automne c'est bientôt, mieux vaut se préparer dès maintenant... et lire ce qui suit.

Sur le Net aussi il vaut mieux sortir couvert, comme on dit. Et le VPN est un peu au P2Piste ce qu'est le préservatif au coureur de jupons : une protection indispensable. C'est une chose bien connue maintenant, sur le net les internautes sont identifiés par une adresse IP, sorte de plaque d'immatriculation attribuée par le FAI à chaque ordinateur ou serveur connecté à internet. La loi Hadopi est basée sur la collecte de ces adresses IP. Et c'est là qu'interviennent les services VPN. Ces "réseaux privés virtuels" permettent de préserver l'anonymat de l'internaute sur la toile en masquant son adresse IP réelle identifiée par le fournisseur d'accès à internet et en lui attribuant une adresse IP "venue d'ailleurs", souvent située dans un pays tiers. Pas d'adresse IP identifiable ? Pas de sanction ! Et voici comment Hadopi est déjà obsolète... Les VPN sont la solution la plus efficace à l'heure actuelle pour protéger son anonymat en surfant sur le net et sécuriser ses données. Ils ne ralentissent pas votre débit de connexion et ils cryptent et anonymisent absolument toutes vos activités en ligne.

C'EST QUOI EXACTEMENT UN VPN ?

Un réseau privé virtuel (VPN pour Virtual Private Network) repose sur un protocole dit de « tunnelisation », c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie. Les données cryptées entre les deux extrémités du VPN sont donc indéchiffrables pour tout utilisateur situé entre elles. Le tunnel sécurisé peut relier deux réseaux locaux ou deux machines.

"Le réseau est sous notre contrôle, pas le leur" TPB

De nombreux P2Pistes utilisent déjà, moyennant quelques dollars par mois, des services comme *World secure channel* (<http://world-secure-channel.com/>) ou *Vpnboy* (<http://www.vpnboy.com/>) pour

cachez leurs adresses IP aux fournisseurs d'accès à Internet. Sans surprise, ce sont les incontournables suédois de The Pirate Bay qui ont pris les choses en main en lançant avec fracas *IPREDator*, un service VPN pour contourner "leur" loi IPRED, sorte de Hadopi à la sauce scandinave. The Pirate Bay promet à ses abonnés un plus grand anonymat qu'avec les services VPN existants, moyennant une somme de cinq euros par mois. Il ne stocke aucune donnée de trafic et rassure : "Le réseau est sous notre contrôle, pas le leur". On trépigne juste d'impatience en attendant qu'il achève sa phase Beta et soit disponible pour tous, ce qui serait imminent à en croire TPB. Par chez nous aussi, un site français propose ce type de filet de sécurité aux internautes, directement inspiré de *IPREDator* : "Ipodah", donc Hadopi à l'envers. "Les communications entre votre PC et le réseau IPODAH sont chiffrées en 128 bits et l'adresse IP est remplacée par une adresse anonyme", explique les créateurs. Pour le moment il est encore dans une phase de test qui "débouchera dans les prochains mois sur une offre commerciale", assure l'équipe sans toutefois préciser le prix à payer pour ses services. Reste que, si TPB peut se prévaloir d'un savoir-faire et jouit d'un capital de confiance important auprès des internautes, on ne sait pas qui se trouve derrière le projet "Ipodah" et si ce qui se passe à l'intérieur du VPN est indéchiffrable de l'extérieur, les administrateurs du service peuvent eux vous identifier... alors prudence.



IPREDator: Le VPN selon The Pirate Bay



Pour une raison ou une autre, vous souhaitez surfer en toute discrétion. C'est votre droit et IPREDator vous permet de faire valoir ce droit à l'anonymat sur Internet. Sa technologie est pointue mais fort heureusement son installation, assez aisée, ne requiert pas de compétences informatiques particulières.

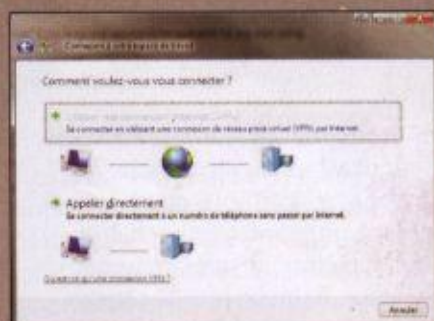


1 L'inscription : C'est simple et rapide : il suffit de saisir son nom, son identifiant, son adresse email et un mot de passe. Ensuite il faut passer à la caisse via le service de paiement Paynova qui va vous taxer de 149kr couronnes suédoises, soit un peu moins de 15 euros pour trois mois d'utilisation. Rapidement au cours du processus d'inscription, IPREDator rassure sur la légalité de l'entreprise et sur la protection des données.



2 Configuration de votre PC : Il reste à configurer votre PC pour pouvoir utiliser IPREDator. The Pirate Bay a eu la bonne idée de prévoir une page d'explications claires sur la marche à suivre, en fonction de votre système d'exploitation (Windows XP, Vista,...). Dans l'onglet "Connexion à un réseau" Cliquez sur "Connexion à votre espace de travail".

3 Cliquer ensuite sur "Utiliser ma connexion Internet VPN" afin de pouvoir accéder au fameux réseau privé virtuel IPREDator.



4 Il suffit ensuite de saisir l'adresse internet du service IPREDator (<https://www.ipredator.se>) et le nom de la destination (ipredator). Vous aurez alors à saisir une nouvelle fois votre nom d'utilisateur et votre mot de passe, et le tour est joué!



5 "My IP information": Comme tout s'est bien passé, voici ce que doit afficher l'écran. Il détaille les informations de votre connexion et confirme que, sur le web, vous êtes désormais...suédois !

My IP Information

IP Information

IP Address: 93.182.14... Whois | Reverse IP | Ping | DNS Lookup | Traceroute

Hostname: anon...ipredator.net

Blacklist Status: Clear

Remote Port: 49633

Protocol: HTTP/1.1

Connection: keep-alive

Keep Alive: 300

Location

Country: Sweden (SE)

Region:

City:

ISP: Se-viasturopa

Privacy



Changer d'adresse IP avec un serveur proxy

A chaque visite de site web, nous fournissons une grande quantité d'informations sur nous-même: localisation géographique, adresse, numéro de téléphone, emploi, numéro de carte bancaire, les mots-clés recherchés, les pages web consultées, etc. Même si le site est digne de confiance, nos informations restent sous la menace d'une intrusion de pirates. Voilà pourquoi l'utilisation d'un proxy peut s'avérer utile.

Vous êtes un jeune internaute dans un pays totalitaire, au hasard la Chine, et voulez accéder à un grand quotidien d'information étranger mais, manque de chance, il tombe sous la censure du gouvernement chinois. Moins dramatique quoique... vous êtes un français installé à l'étranger et vous souhaitez regarder les émissions de TV de chaînes françaises sur internet, M6 par exemple, ou alors suivre Roland Garros en direct sur le site de France 2. Impossible ! Ces contenus sont réservés aux adresse IP françaises... Vous voulez revenir sur un site ou un forum duquel vous avez été banni (injustement, cela va sans dire) auparavant. Autant de bonnes raisons pour s'auto-affecter une autre adresse IP qui ne permettra pas notre identification.

Un Proxy c'est quoi ?

Un proxy c'est un serveur qui fonctionne un peu comme un «cache» qui relaie vos requêtes et vos

réceptions lorsque vous surfez sur internet. Votre navigateur adresse ses requêtes à votre proxy, qui les transmet ensuite vers le site que vous souhaitez consulter. Lorsque ce site répond, c'est le proxy qui intercepte les informations envoyées avant de les rediriger vers vous. Votre adresse IP ne peut donc pas être identifiée sur les sites que vous visitez et ceux-ci ne pourront pas glaner d'informations à vos dépens.

Une solution : Les anonymiseurs en ligne

Si vous ne ressentez le besoin de cacher votre adresse IP que très ponctuellement, il n'est pas forcément nécessaire d'utiliser un logiciel tel que NotMyIP, que nous vous présentons juste après. Beaucoup de sites se sont spécialisés dans la mise à disposition de proxies anonymes. Pas besoin d'installer un logiciel, il suffit d'aller sur ces

sites (www.proxys.fr ou encore www.vrais.fr), de saisir l'adresse du site bloqué et sous couvert de son proxy, le site nous y emmène. L'un des pionniers, Anonymizer, propose depuis récemment une version française : <http://anonymizer.secuser.com>. Le service prévient que l'ouverture de pages web intervient après un délai car la bande passante est réservée en priorité aux titulaires d'un compte utilisateur Premium.

Jouons à se faire peur avec The Privacy.net

Vous n'êtes pas convaincus du bien fondé de l'anonymat sur internet, vous vous dites qu'après tout, vous ne sortez pas dans la rue le visage dissimulé derrière des lunettes noires, une fausse moustache et une perruque ? Allez donc faire un petit tour sur privacy.net pour tester votre anonymat sur la toile et



savoir toutes les informations qu'un serveur peut obtenir sur votre connexion, vous ne risquez pas d'être déçus... Le site analyse la confidentialité de votre connexion internet et vous montre toutes les infos qu'un site internet glane sur votre compte quand vous le visitez. Eloquent...même en anglais. www.privacy.net MyIpTest s'amusera quant à lui à vous géolocaliser en fonction de votre adresse IP. <http://myiptest.com>



DEVENEZ AMERICAIN AVEC NotmyIP

NotMyIP s'inscrit dans la liste de plus en plus nombreuse des logiciels de protection de la vie privée sur internet, les fameux «anonymiseurs». NotMyIP est une version dérivée gratuite du service Anonymity Gateway. Il vous permet de vous affecter trois adresses IP différentes des Etats-Unis. La version Premium Anonymity Gateway permet d'en obtenir quinze américaines, plus huit autres de pays tiers (Allemagne,

Canada, France, Irlande et Royaume-Uni). Mais pour un tel niveau de service, il faut payer, c'est 33\$ pour une année.

Rendez vous sur le site www.privacy-gateway.com/notmyip.html pour télécharger le logiciel NotMyIP. Il est très léger et son installation se résume à deux ou trois clics. Vous n'avez rien à faire, aucun paramètres à configurer ni quelque manipulation que ce soit.

passant par des connexions parfois très mauvaises. Aux Etats-Unis, les FAI sont beaucoup moins généreux en bande passante qu'en France.

- Certains anti-virus et anti-espions le détecte comme un virus, un cheval de Troie. Avira antivirus notamment. Pourquoi ? Car Anonymity Gateway suture des informations dans votre ordinateur.

- Il échoue à identifier l'adresse IP alors que tous les autres sites qui fournissent ce service en un clic au moyen d'un simple navigateur en ont été capables. Cela arrive rarement cependant.

Si NotMyIP ne parvenait pas à satisfaire vos exigences en matière de niveau d'anonymat et de performance de navigation, vous pouvez vous tourner vers d'autres logiciels de ce type, notamment *IP Privacy*, qui offre un service de plus grande qualité mais qui est malheureusement payant (www.privacy-pro.com).

Encore un peu de parano

Les proxies enregistrent toutes les communications qu'ils relaient entre vous et les sites que vous consultez, notamment vos adresses IP. Les données sont recueillies par la société qui gère le proxy. Il faut donc lui faire confiance et s'en remettre à elle... Pas facile quand on prête l'oreille aux rumeurs inquiétantes qui circulent concernant les proxies utilisés par les fournisseurs d'accès américains... Enfin, de plus en plus de sites utilisent des petites applications (Javas, ActiveX) pour identifier votre adresse IP réelle. On avance décidément sur des terrains très mouvants...

ASTUCE : Vous pouvez ensuite aller sur l'un de ces sites (www.mon-ip.com ; www.adresseip.com) pour vérifier que votre adresse IP a changé et que votre nouvelle est américaine.



- Téléchargez puis installez NotMyIP sur votre PC
- Lancez le logiciel qui vous donne automatiquement votre adresse IP
- Cliquez sur le bouton «Change IP» pour obtenir l'une des trois IP américaines dispo.

Rien ni personne n'est parfait...

Le logiciel a fait de nombreux adeptes mais il ne faut pas le cacher, il fait aussi des déçus car il comporte plusieurs lacunes importantes.

- Le principal reproche qu'on peut lui faire, c'est qu'il réduit assez nettement le débit de connexion. Evidemment, c'est lent derrière un proxy, mais ce n'est pas anormal car chaque paquet envoyé fait deux tours du monde en



GONFLER SON RATIO TORRENT A TOUT PRIX



Pour télécharger rapidement sur les trackers P2P, il faut bien sur une bonne connexion internet mais il faut aussi avoir un bon ratio entre ses uploads et ses downloads. Pour augmenter sa vitesse de téléchargement, il n'a pas d'alternative, il faut "gonfler" ce ratio.

SUR LE MÊME CRÉDO

GreedyTorrent :
www.greedytorrent.com
Ratiomaster.nrpg :
<http://ratiomaster.nrpg.info>

A SAVOIR

Pour calculer son ratio, il faut diviser la quantité totale de données envoyée aux autres pairs par la quantité totale de données reçue d'eux. $RATIO = \text{UPLOAD} / \text{DOWNLOAD}$. Pour augmenter la vitesse d'upload, il faut augmenter la vitesse d'upload et/ou réduire la vitesse de download.

Ratio > 1 : Vous êtes très généreux et vous en êtes largement récompensé

Ratio entre 0,5 et 1 : Ça passe mais en l'améliorant votre vitesse de téléchargement augmentera

Ratio < 0,5 : Commencez à vous chercher un autre toit car ça sent le bannissement

Pour bien faire il faudrait donner autant que l'on reçoit, pour s'assurer un ratio à peu près équivalent à 1. Surtout sur les trackers privés, particulièrement exigeants en matière de partage. Presque tous tiennent des statistiques sur leurs clients pour déterminer les bon partageurs des mauvais, les forçant ainsi à maintenir un bon ratio.

Ne pas réussir à maintenir un bon ratio sur un tracker privé, c'est le bannissement assuré. Certains trackers obligent même leurs utilisateurs en péril à effectuer des dons pour se racheter un ratio digne de ce nom. On sait pourtant que même la meilleure volonté du monde ne suffit pas toujours et qu'il est mathématiquement impossible pour tous les utilisateurs d'un tracker d'avoir au même moment un bon ratio, supérieur à 1. Sans compter que certaines connexions internet favorisent fortement le download par rapport à l'upload qui est en général quatre à cinq fois moins rapide et parfois jusqu'à dix fois moins rapide.

Quelques conseils destinés aux gros leechers

Avant d'envisager des solutions plus radicales, petit rappel des quelques règles de base à observer pour conserver un ratio "honnête". Déjà, c'est quand vous êtes nouveau sur le tracker qu'il faut particulièrement le soigner car tant que peu de données ont été échangées, il sera très sensible à chaque nouveau transfert. Une fois que vous vous êtes assuré un ratio confortable sur le

tracker, vous pouvez vous laisser aller, une fois de temps en temps, à mettre la main sur des fichiers que vous ne repartagerez pas. Comment s'assurer un bon ratio d'entrée de jeu ou comment se refaire une santé ? En téléchargeant en priorité les nouveautés, les fichiers populaires que tout le monde s'arrache plutôt qu'une vieillerie qui n'intéresse que vous et que personne d'autre ne téléchargera à son tour. Une fois téléchargés, laissez-les à disposition des leechers quelques jours au moins avant de les effacer. Il reste enfin la possibilité de brider sa vitesse de téléchargement, pour envoyer à la même vitesse que l'on reçoit. Evidemment, ça prendra un peu plus de temps pour recevoir ses précieux fichiers...

Si cela ne suffit pas...

Malgré nos conseils précédents vous avez été banni de votre tracker ou votre ratio reste désespérément bas ? Alors abandonnez-le et recommencez d'un bon pied sur un autre... qui ne prends pas en compte le ratio. Ou alors, il existe un dernier recours, une solution pour sauver les meubles...Rendez-vous à la page suivante.



HACKER SON RATIO

La technologie P2P s'appuie sur le principe de partage et de réciprocité : Je prends, je donne. Certains "P2Pistes", à la recherche de plus grandes vitesses de téléchargement, ne s'emcombrent pas de ces considérations et se tournent vers des applications de "ratio hacking" comme le logiciel RatioMaster.

RatioMaster pirate les données de transfert qui sont renvoyées au tracker à berner et qui permettent d'établir le ratio download /upload. Il se connecte au tracker et se fait passer pour un client BitTorrent normal alors qu'en fait il ne fait que simuler les uploads

et downloads pour donner l'impression au tracker que l'utilisateur upload plus qu'il ne le fait réellement. Vous pouvez télécharger ce logiciel librement et gratuitement à l'adresse suivante : www.moofdev.net/ratiomaster/downloads

- 1 Localisez un fichier torrent sur le tracker que vous voulez berner
- 2 Téléchargez le fichier torrent avec votre client bittorrent habituel
- 3 Refermez votre client bittorrent et lancez **RatioMaster**
- 4 Chargez ce fichier dans **RatioMaster** par glisser-déposer dans "chemin d'accès"

- 5 Paramétrez les vitesses d'upload et de download (la vitesse d'upload est réglée par défaut 5 fois plus rapide que le download)

Fichier du torrent
Chemin d'accès: C:\Users\Zaoh\Downloads\Richard_Wagner_-_Testen_und_Jeide_-_Bayreuth_191

Informations sur le Torrent
Tracker: http://tracker.thepiratebay.org/announce
SHA Hash: 2ADBDC43129C91838AFBE19CA4A28C80BA06E8AC Taille: 250,91 MB

Options
Vitesse d'Upload (Ko/s): 50 Fini (%) 0
Vitesse de Download (Ko/s): 10
Arret après: Ne jamais arrêter

Ratio Master 1.8.3

Langue: French

General Avancé Réseau Log Mise à jour À propos de

Fichier du torrent
Chemin d'accès: C:\Users\Zaoh\Downloads\Richard_Wagner_-_Testen_und_Jeide_-_Bayreuth_191

Informations sur le Torrent
Tracker: http://tracker.thepiratebay.org/announce
SHA Hash: 2ADBDC43129C91838AFBE19CA4A28C80BA06E8AC Taille: 250,91 MB

Options
Vitesse d'Upload (Ko/s): 50 Fini (%) 0
Vitesse de Download (Ko/s): 10
Arret après: Ne jamais arrêter

Stats
Partagé: Téléchargé: Temps Total:
Mise à jour dans: 0 Mise à jour Manuelle Seeders: Leechers:

Demarrer Stop Fermer

- 6 Dans l'onglet "Avancé", sélectionnez la version du client bittorrent utilisé que le logiciel doit imiter (Si RatioMaster ne l'a pas déjà identifié)

- 7 Faites "Démarrer" et observez votre ratio prendre de la hauteur

Options
Vitesse d'Upload (Ko/s): 50 Fini (%) 0,08
Vitesse de Download (Ko/s): 10
Arret après: Ne jamais arrêter

Stats
Partagé: 1,03 MB Téléchargé: 203,77 KB Temps Total: 00:22
Mise à jour dans: 31:31 Mise à jour Manuelle Seeders: 13 Leechers: 3



Attention ! le subterfuge ne marche pas à tous les coups ! Certains trackers privés bien avertis, Oink notamment, peuvent détecter l'entourloupe et vous bannir sans autre forme de procès!

Les trackers vont devoir apprendre à se prémunir contre ces nouvelles méthodes car *RatioMaster* n'est pas le seul sur ce crédo. Espérons quand même que ce type de logiciels ne seront pas exploités à tort et à travers, car c'est la volonté de partager qui a fait l'immense succès de la technologie P2P.



P2P: DÉTENDEZ-VOUS, BTACCEL S'OCCUPE DE TOUT

Chaque fois qu'elle est menacée et qu'on la donne pour moribonde, la technologie P2P s'adapte, se réinvente et nous surprend. Pour preuve, l'arrivée de BTAccel, le service P2P qui télécharge à votre place ! Le site est encore en version Alpha (pré-BETA), donc disponible seulement sur invitation. Tentez votre chance !



VOUS AVEZ DIT «DIRECT DOWNLOAD» ?

Le fichier est d'abord téléchargé en P2P à grande vitesse sur les serveurs de BTAccel. Ensuite, vous devez le télécharger selon le protocole HTTP en direct download, c'est-à-dire en téléchargement direct sur le serveur de BTAccel, selon le modèle client-serveur, par opposition au P2P.

Délégué le boulot à ce service de torrent hébergé. Il va télécharger pour vous vers ses propres serveurs, des fichiers depuis n'importe quels sites de torrent, puis les mettre à disposition en direct download pour que vous les rapatriés sur votre PC. L'interface d'abord. Pas grand chose à dire d'elle si ce n'est qu'elle est épurée au maximum et d'une simplicité enfantine. Un service simple et rapide à prendre en main, on en demandait pas plus.. quoique l'interface, trop impersonnelle, risque d'être peu fédératrice. Le service est gratuit mais

envisage dans un avenir proche de mettre en place un service premium payant (de 10\$ à 25\$ mensuels).

Essayons la bête

Une fois le fichier que vous voulez téléchargé localisé, vous donnez le lien à BTAccel et il s'occupe de tout ! Ensuite ? Ce sont leurs propres serveurs qui vont télécharger le torrent à votre place. Donc vous ne perdez pas de temps avec les basses besognes du téléchargement, vous n'encombrent pas votre bande passante et surtout surtout : vous restez blanc comme

neige ! Rapport à Hadopi, bien entendu. Et oui, ce n'est pas votre ordinateur qui télécharge, vous restez donc anonyme.

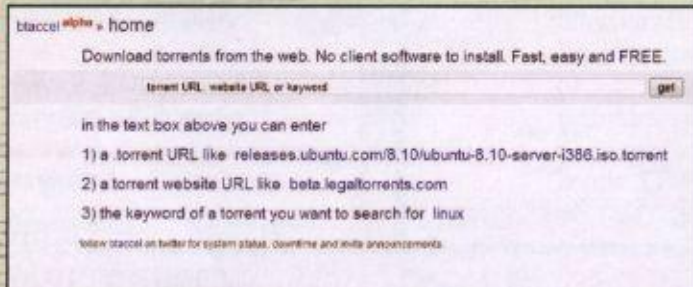
Le temps d'attente avant que le téléchargement ne démarre dépend à la fois de votre statut d'utilisateur,

A DESTINATION DE CEUX QUI DORMAIENT PENDANT LES COURS D'ANGLAIS...

Queuing : le torrent est dans la file d'attente pour le téléchargement

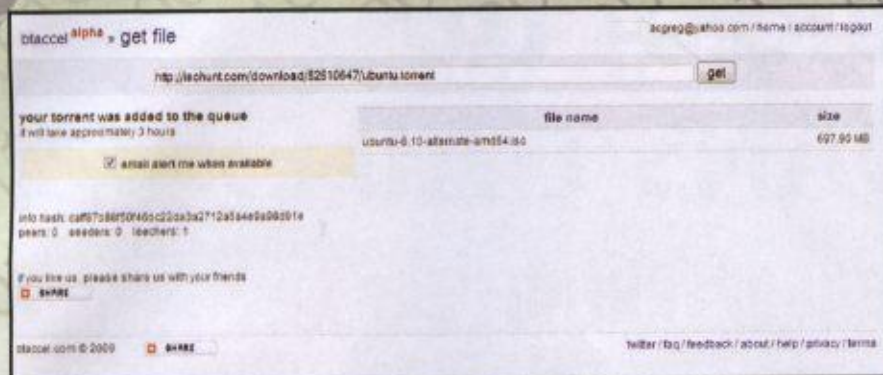
Available : le torrent a été téléchargé par les serveurs de BTAccel et est disponible en direct download

Deleted : pas de chance, le torrent a été supprimé



BTACCEL





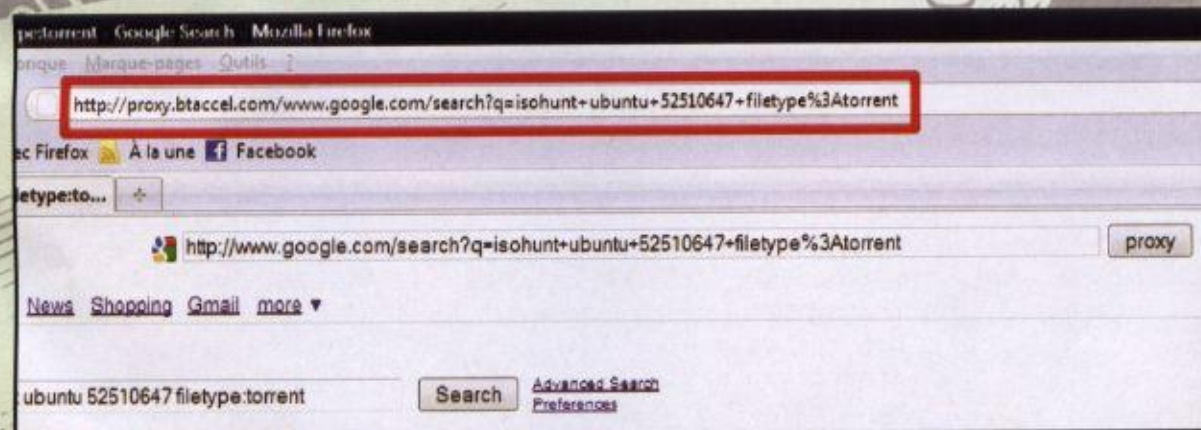
enregistré ou non-enregistré (les deux sont gratuits), et de la charge du serveur. Généralement, les téléchargements commencent après quelques minutes même si vous ne vous êtes pas enregistrés. Il arrive cependant que plusieurs heures ne s'écoulent avant le début du téléchargement, voir qu'il ne débute jamais... Par contre, si vous avez de la chance et que le torrent que vous voulez a déjà été téléchargé sur BtAccel, il peut être disponible en quelques secondes sur le serveur via un système de cache. Les torrent populaires peuvent être téléchargés à des vitesses supérieures à 5000 Kb/s ! Juste le temps d'aller aux toilettes et c'est prêt.

Si vous avez choisi cette option, un email d'alerte vous prévient quand le fichier torrent a été téléchargé. Il vous reste à le rapatrier, sous forme d'un fichier ZIP sur votre ordinateur, en direct download depuis le serveur BTAccel. Aucune installation de logiciel n'est nécessaire, tout ce dont vous avez besoin, et vous l'avez déjà, c'est d'un navigateur ! BTAccel le conservera les fichiers téléchargés deux semaines sur ses serveurs. Pendant cette durée, vous pouvez partager le lien avec vos amis qui pourront le récupérer sur leur PC sans avoir à le télécharger une nouvelle fois.

Un proxy anonyme à votre disposition

BTAccel met aussi à votre disposition la possibilité d'utiliser un proxy anonyme de type "http://proxy.btaccel.com/XXXXXXXX" avec lequel vous pourrez naviguer en toute quiétude dans les eaux dangereuses des sites de torrent. Vous avez donc le choix de localiser vous-même le fichier et de saisir son adresse URL vous-même dans BTAccel, ou alors de profiter de ce proxy anonyme. Dans ce cas, vous pouvez vous contenter de saisir les mots clés qui vous permettront de trouver le torrent et BTAccel vous emmène sous couvert de son proxy sur les portails torrent.

Le concept n'est pas révolutionnaire en soi. Les "seedboxes" offrent globalement le même type de services moyennant quelques dollars par mois (voir notre article suivant pages XX). Combien de temps le service va-t-il tenir le coup ? Bien malin qui pourrait le dire, mais ce qu'on peut affirmer en revanche, c'est que Hadopi et ses sbires n'ont pas tué le P2P, ils l'ont juste poussé à évoluer.



C'EST BIEN



- Ne nécessite qu'un simple navigateur, aucune installation requise
- Plus simple que les clients torrent classiques (Vuze, uTorrent, ...)
- Anonymat

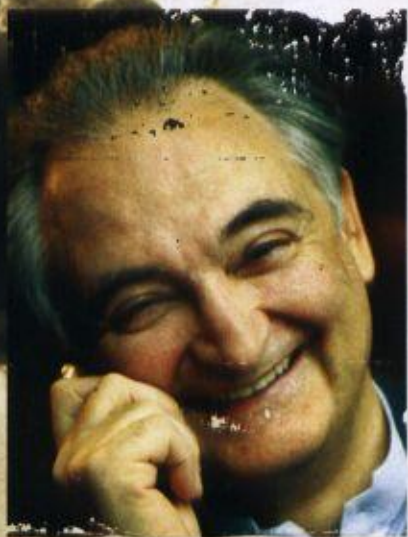
C'EST MOINS BIEN



- Pas toujours très fiable
- Nom pas très « sexy » et interface très impersonnelle



LA CENSURE A DU PLOMB DANS L'AILE !



La "loi favorisant la diffusion et la protection de la création sur Internet", plus tristement connue sous le nom "Hadopi". C'est ce qui nous scandalise depuis plusieurs mois déjà, depuis 2006 et la loi DADVSI plus précisément. "Nous", c'est-à-dire les geeks, les P2Pistes, les internautes, les amateurs de nouvelles technologies, les consommateurs de culture, de musique et de cinéma, les gens qui réfléchissent à l'avenir, ceux qui imaginent autre chose que ce qui existe déjà, hommes ou femmes, jeunes ou moins jeunes. Ca fait beaucoup de monde à être scandalisé donc. Presque tout le monde en fait.

A un mois du vote solennel du texte à l'Assemblée nationale, quand on se bat contre une loi d'un gouvernement tout puissant, les soutiens sont toujours les bienvenus et les bonnes nouvelles sont toujours bonnes à prendre. La dernière petite réjouissance en date ? La nouvelle attaque de Jacques Attali contre la loi Hadopi. Jacques Attali, c'est l'un des personnages éminents de

HADOPI PREND L'EAU AVANT MÊME SON ENTRÉE EN APPLICATION

la vie politique française, sa voix a du poids. Donc c'est toujours bon à prendre. Dans une interview donnée à Libération le 18 août dernier, il a donné une véritable gifle dans la figure d'Hadopi. Ou plutôt non : un bon coup de poing en plein dans sa gueule ! Mais quand-est-ce qu'elle va finir par cre*** cette sal*** de loi ?! Ouhhh, Ca fait du bien...

Jacques a dit ...

Laissons-le parler, après tout c'est lui l'intello. "[Le gouvernement] semble avoir choisi le camp des majors et de quelques artistes liés aux majors. [...] Il défend quelques vedettes politiquement très visibles, mais qui ne représentent rien[...], sont surévaluées au regard de leur utilité artistique, pour ne pas parler de leur utilité sociale." Il y est allé gaiement, on n'en pense pas moins. "Ce sera encore une loi, plus ou moins avortée, qui ne servira à rien", a-t-il ajouté. A rien ? Pas tout à fait, en vérité, Jacques. Hadopi a plusieurs mérites : D'abord elle a permis à une masse d'internautes anonymes, Nous, de se mobiliser et de jeter les bases de vraies organisations pour défendre nos intérêts (Le réseau des pirates, par exemple). Bref, pour la première fois, on a gueulé et ça s'est (un peu) entendu. Un autre bienfait de cette loi, et qui ne fait pas mais alors pas du tout plaisir à ses concepteurs, c'est qu'elle a donné un coup de fouet aux innovations techniques qui permettent de la contourner et à favoriser leur propagation à

Monsieur tout le monde (VPN, cryptage GPG, seedboxes, etc). Et oui, on leur avait pourtant dit qu'ils se fatiguaient pour rien.

En mars dernier déjà il s'était légèrement agacé dans les colonnes de l'Express, Attali. Tout le monde en avait pris pour son grade. La loi Hadopi ? "Indigne, absurde et scandaleuse" et qui "ouvre la voie à une surveillance générale de tous les faits et gestes des internautes", selon lui. Les hommes politiques ? En "connivence entre eux" et "soucieux de s'attirer la bienveillance d' "artistes vieillissants". Le gouvernement ? "[Il] préfère engraisser les majors de la musique et du cinéma, devenues aujourd'hui cyniquement, consciemment, les premiers parasites de la culture". Les élites ? "[Elles] ne comprennent plus rien ni à la jeunesse, ni à la technologie, ni à la culture". Ca c'est envoyé!

Attali est-il sincère ou non ? Est-ce qu'il fait ça par intérêt personnel (pour remonter sa cote auprès des jeunes) ou parce qu'il y croit vraiment ? Pas besoin de se crêper le chignon pendant 107 ans pour le savoir, la réponse c'est qu'"on s'en fout !!". Le plus important c'est qu'il se bat contre Hadopi. Et force est de constater qu'il se bat plutôt pas mal, pour le coup. Ca ne suffira pas à remporter la bataille Hadopi, mais la guerre pour un Internet libre ne fait que commencer.



Ce qui suit a été écrit peu après mon arrestation..

La conscience d'un hacker

Un autre a été pris aujourd'hui, c'est dans tous les journaux. « Un adolescent arrêté dans un scandale de crime informatique. » « Arrestation d'un Hacker après des tripatouillages bancaires. »

Saleté de gosses. Tous pareils.

Mais vous, dans votre psychologie trois-pièces et dans votre technocerveau des années 50, avez-vous jamais regardé derrière les yeux du hacker ? Est-ce que vous vous êtes jamais demandé ce qui le déclenche, quelles forces lui ont donné forme, qu'est-ce qui a bien pu le modeler ?

Je suis un hacker, entrez dans mon monde...

Mon monde est un monde qui commence avec l'école... Je suis plus intelligent que la plupart des autres gosses, ces conneries qu'ils nous apprennent m'ennuient...

Ces fichus élèves en situation d'échec. Ils sont tous pareils.

Je suis dans un collège ou un lycée. J'ai écouté les profs expliquer pour la quinzième fois comment réduire une fraction. Je le comprends. " Non, Mme Smith, je n'ai pas montré mon travail. Je l'ai fait dans ma tête..."

Fichu gosse. Il l'a probablement copié. Tous pareils.

J'ai fait une découverte aujourd'hui. J'ai découvert un ordinateur. Eh attendez, c'est cool. Il fait ce que je veux qu'il fasse. S'il fait une erreur, c'est parce que j'ai merdé. Pas parce qu'il ne m'aime pas...

Ou qu'il se sent menacé par moi...

Ou qu'il pense que je suis un petit malin...

Ou qu'il n'aime pas enseigner et ne devrait pas être là...

Fichu gosse. Tout ce qu'il fait, c'est jouer à des jeux. Tous pareils.

Et ensuite, c'est arrivé... une porte s'est ouverte sur un monde... on envoie une pulsation électronique, qui fonce le long des lignes téléphoniques comme l'héroïne dans les veines d'un drogué, on recherche un refuge contre les incompétences quotidiennes... on trouve une planche de salut...

« C'est ça... c'est là qu'est mon appartenance... »

Je connais tout le monde ici... même si je ne les ai jamais rencontrés, je ne leur ai jamais parlé, n'entendrai peut-être jamais plus parler d'eux... je vous connais tous...

Tu peux parier, y'a pas à tortiller, qu'on est tous pareils... à l'école, on nous nourrissait à la petite cuillère de blédine pour bébé alors que nous avions faim de steak... les bouts de viande que vous nous refiez étaient prémâchés et sans goût. Nous avons été dominés pas des sadiques, ou ignorés par des apathiques. Les quelques-uns qui avaient quelque chose à nous apprendre trouvaient en nous des élèves pleins de bonne volonté, mais ce petit-nombre là, c'était comme des gouttes d'eau dans le désert.

Voici notre monde maintenant... le monde de l'électron et de l'interrupteur, la beauté du bit. Nous utilisons un service déjà existant sans payer pour ce qui pourrait valoir des clopinettes si ce n'était pas administré par des gloutons profiteurs, et vous nous traitez de criminels. Nous explorons... et vous nous traitez de criminels. Nous cherchons le savoir... et vous nous traitez de criminels. Nous existons sans couleur de la peau, sans nationalité, sans parti pris religieux... et vous nous traitez de criminels. Vous construisez des bombes atomiques, vous faites la guerre, vous tuez, vous trompez et vous nous mentez et vous tentez de nous faire croire que c'est pour notre bien, mais c'est nous les criminels.

Oui, je suis un criminel. Mon crime est celui de la curiosité. Mon crime est de juger les gens pour ce qu'ils disent et pensent, pas pour ce qu'ils ont l'air. Mon crime est d'être plus fort que vous, ce que vous ne me pardonneriez jamais.

Je suis un hacker, et ceci est mon manifeste. Vous arrêterez peut-être cet individu-ci, mais vous ne pouvez nous arrêter tous... après tous, nous sommes tous pareils.

8 janvier 1986

CRAQUER UN ACCÈS WIFI



notre pas à pas pratique

TRACKERS PRIVÉS

apprenez comment gonfler
votre ratio pour télécharger
à fond les manettes

Cartes bancaires,
paiements en ligne



ATTENTION DANGER !

GUIDE PRATIQUE VPN

l'anonymat à porté de main

CHIFFRER SES EMAILS

rien de
plus facile

PIRATES INFORMATIQUES

Qui sont ils vraiment ?



MUSIQUE, VIDÉOS,

Profitez
c'est gratuit