

CR-ROM OFFERT !

Avril / Juin 2010

PEER 2 PEER

CLICK P2P LOAD P2P

N°6

3,90 €

GUIDE P2P & TÉLÉCHARGEMENTS

L'ANONYMAT

LES VRAIES SOLUTIONS

VOTRE PROFIL

FAIBLE, MODÉRÉE OU ÉLEVÉE :
DE QUELLE PROTECTION
AVEZ-VOUS BESOIN ?

PRATIQUE

SERVICES ET
LOGICIELS : NOUS
AVONS TOUT TESTÉ

Nos fiches
pratiques :

TOUTES
NOS ASTUCES

- eMule, BitTorrent et Limewire protégés
- Utiliser un proxy ■ Passer par un VPN
- Les réseaux 100% cryptés ■ Etc!

À SAVOIR

QUI SURVEILLE
LES RÉSEAUX ?

+ LEURS TECHNIQUES



SOMMAIRE

- 4 **NOTRE CD GRATUIT :**
Découvrez son contenu !
- 6 **Repères :**
Qui vous surveille ?
- 11 **Qu'est-ce-qu'une adresse IP ?**

SPÉCIAL

Ebooks-land.net

Protection FAIBLE

p.18

- 19 **IPFilter X :** il boute les IP louches hors de votre PC !
- 22 **Le brouillage de protocole :** une arme légitime.
- 24 **Les solutions pour partager tranquille :** le DHT et Torrage

Protection MODÉRÉE

p.26

- 27 **Nos amis les proxy :** ils téléchargent à votre place !
- 33 **Le point sur le P2P privé et le F2F**
- 38 **La nouvelle méthode pour les gros téléchargeurs :** les seedbox
- 44 **RapidShare et MegaUpload :** peut-on se passer du P2P ?

ANONYMAT

Protection ÉLEVÉE

p.46

- 47 **Les VPN :** un réseau privé virtuel pour se mettre à l'abri des petits curieux !
- 50 **Les réseaux cryptés :** I2P, iMule et StealthNet
- 56 **Le côté obscur d'Internet :** les Darknet
- 60 **Usenet et le SSL :** Un protocole plus vieux qu'Internet devient l'ami des téléchargeurs



NOTRE BOÎTE À OUTILS

Depuis le temps que nous en parlons, la loi HADOPI est enfin rentrée en vigueur. Même si à l'heure où nous bouclons ce magazine, nous n'avons pas encore pu trouver de lecteurs ayant reçu les fameuses lettres d'avertissements, personne n'est à l'abri. Une étude de l'Université de Rennes a récemment montré que le nombre d'internautes utilisant des moyens illégaux pour s'approvisionner en contenus multimédia a même augmenté de 3 %, ces trois derniers mois. En effet, le développement de solutions en dehors du périmètre de la loi comme le streaming, RapidShare ou Usenet est en pleine expansion. Si l'on ajoute les réseaux cryptés, les VPN et les différents autres procédés permettant l'anonymat, ce sont 3 millions d'internautes qui échapperaient aux mailles d'HADOPI. Pour protéger votre vie privée, le numéro que vous tenez dans les mains est un concentré des techniques vous permettant d'être plus ou moins invisible sur la Toile. En fonction de votre profil, nous avons séparé ce magazine en trois parties, du plus bas niveau d'anonymat au plus haut. Rappelons enfin que même si le téléchargement d'œuvres protégées est illégal, la moitié des internautes achetant sur les plates-formes légales sont aussi des «pirates».

Bonne lecture !

La Rédaction.

NOTRE CD

50 LOGICIELS OFFERTS !



P2P, INTERNET



MULTIMÉDIA



RÉSEAUX CRYPTÉS



HACKING



P2P PRIVÉ



JEUX VIDÉO

NOTA BENE

Ce CD est garanti sans virus connu. Néanmoins, il arrive que la sensibilité de certains antivirus détecte des faux positifs.



> NOTRE SÉLECTION DE JEUX



* TREMOULOUS
* GLEST
* SIMUTRANS



* RROOTAGE
* FRETS ON FIRE



+ NOS RUBRIQUES BONUS

> A COLLECTIONNER:

> 5 Services Vidéos Inédits

- Sécurité Tube
- Stupéfix TV
- Revoir la télé
- TV Direct
- MagMa enregistrer le stream

4 fonds d'écran militants !

ACCESS DENIED



ACCESS DENIED

Gros plan sur 5 LOGICIELS

- > BitBlinder
- > TOR
- > OneSwarm

- > Free Studio
- > AirSnare

Fs



BIG BROTHER :

QUI SURVEILLE ET COMMENT ?

L'exemplaire du magazine que vous tenez dans les mains n'aurait pas lieu d'exister sans la multiplication des organismes de surveillance qui sévissent sur Internet. Alors qu'on ne parle plus que de HADOPI en France, on oublie un peu vite les sociétés qui sont payées par les ayants droit pour faire la chasse aux «pirates» (certains continuent de les appeler «clients»). Qui surveille et comment font-ils nous traquer ?

Sur Internet, tout peut devenir une source de revenu. Depuis longtemps des sociétés encaissent de grosses quantités d'argent en traquant les P2Pistes. C'est en effet devenu un business. Les majors, qui perdent des milliards (selon Pascal Nègre, le pro du MP3 japonais) continuent bizarrement de payer grassement ces sociétés. Advestigo, Ipoque, Qosmos, Trident Media Guard, Detica ou CoPeerRight Agency se portent très bien et certaines de ces sociétés ont même engagé des poursuites contre les autres pour des raisons de...copyright. Un comble.

À l'insu de votre plein gré

Le fournisseur d'accès Internet (FAI) anglais Virgin Media a dernièrement commencé à mettre en place un système de surveillance des données transitant sur les réseaux. L'objectif de la société est de mesurer le nombre de contenus pirates circulant sur Internet via P2P. 40% des clients du FAI ont donc été choisis aléatoirement (et sans leur consentement bien sûr !) pour être les cobayes. Même si le but officiel de Virgin est de jauger le nombre de fichiers pirates et d'en calculer le coût, on ne peut que se poser des questions quant au bien fondé de cette démarche. En effet, Virgin est aussi un des plus grands vendeurs de disque au monde. Qui nous dit que ces données ne seront pas utilisées pour des poursuites, même indirectement ?



Comment font-ils ?

Pour attraper les internautes, ces sociétés n'y vont pas par quatre chemins, ils font exactement comme les gens qu'ils sont censés attraper : ils allument eMule ou BitTorrent et téléchargent ou proposent des films en téléchargement (la plupart étant des «fake» avec des noms bien racoleur). Il s'agit donc d'une technique «man in the middle» où ces sociétés se mettent en place sur le réseau dans le but de collecter des adresses IP. Lorsque le délit est constaté, les sociétés de surveillance informent les ayants droit et c'est ensuite eux qui passent à l'attaque... Avec une IP,

il n'est pas très difficile d'obtenir l'identité d'une personne auprès de son FAI. Heureusement, il existe des techniques pour bannir les IP «louches» grâce à des logiciels comme PeerGuardian ou IPFilterX (voir page 15).

Et avec HADOPI ?

En ce qui concerne HADOPI, c'est la société Trident Media Guard (TMG) qui a été retenue en tant que prestataire technique en charge de la surveillance des échanges illégaux sur les réseaux P2P. Choisie depuis 2002 par plusieurs professionnels de la musique et du cinéma, la mission de



IPFilterX banni de votre réseau les IP qui vous espionnent

cette entreprise sera donc de surveiller les échanges P2P parmi une sélection de près de 10 000 œuvres identifiées. Sans plus de précision, TMG s'attaquera à la surveillance des 4 réseaux P2P les plus actifs. Rien que pour le secteur musical, la société prévoit de relever 25 000 infractions par jour. Les données recueillies seront ensuite données à la SSCP (Société civile des producteurs de phonogramme) qui les transférera enfin à la HADOPI. Ce sera à la Haute Autorité de voir avec les FAI pour mettre un nom sur les IP et de suspendre l'abonnement le

Avec 10 000 avertissements par jour, les facteurs ne vont pas chômer...

cas échéant. Chaque jour, ce sont 10 000 avertissements qui devraient être envoyés. Avec la multiplication des méthodes «anti-HADOPI», la Haute Autorité s'intéresse de plus en plus au streaming, à RapidShare et MegaUpload ainsi qu'à Usenet.

Les deux sortes de techniques de surveillance

Nous l'avons vu, la technique la plus populaire consiste à se fondre dans le réseau pour mieux débusquer les contrevenants mais il existe aussi des solutions dites «d'observation» dont le principe est d'analyser la nature des flux de données transitant par un point de passage. Plus ce point de passage est grand plus le recueil de données est efficace. Il est donc primordial de bien choisir ce point. Par exemple sur les infrastructures d'un fournisseur d'accès par lesquelles transitent les connexions de milliers d'abonnés. Attention, ces systèmes peuvent aussi être utilisés pour filtrer les flux. Même si officiellement, aucun FAI français n'utilise de telle méthode (très à la mode au Canada et aux États-Unis), il apparaît que plusieurs fournisseurs d'accès ont déjà recours à ce système pour dissuader les P2Pistes de télécharger. Pour savoir comment contrer ce filtrage, dirigez-vous vers la page 18 de ce magazine...

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

Spécial dédicace à tous mes amis leechers, pour leur manque de valeurs déjà, le non-respect du travail des teams, pour se foutre de la gueule des internautes en ne mettant à disposition les fichiers que sur des hébergeurs pour se faire de l'argent, sans parler du peu d'originalité dont ils font preuves donc sans donner de noms

merci à dans l'ordre ou le désordre ça dépend de quel coté de l'écran on se trouve

- *Dayznoob
 - *Movizpd
 - *Kakacity
 - *Alexandra42 (43 ou 44 c comme elle veut !)
 - *Seals / Barmby
 - *Banana11
 - *Biggola
- et désolé pour tous ceux que j' ai oublié...**

**amicalement,
71cucaracha**

P.S : au lieu de leecher, ne serait il pas mieux que chacun scanne des magazines différents pour avoir plus de choix ???

LIBRE ET ENGAGÉ

N°9 Mars/Avril 2010

CLICK LOAD
TÉLÉCHARGEMENT & STREAMING

DOWN LOAD
CHANGE DE NOM!

SEULEMENT **2€**50

RÉVOLUTION STREAMING

FILMS ET SÉRIES À LA CARTE : Les sites qui font polémique

STREAMING ET BITTORRENT : Swarmplay et innoxi

LA TÉLÉ EN DIRECT SUR PC : toutes les chaînes en accès illimité

GUIDE ANONYMAT DOSSIER

RÉSEAUX CRYPTÉS : ILS ÉCHAPPENT À TOUT CONTRÔLE

TESTÉS : Les moteurs de recherche 100% MUSIQUE

100% PRATIQUE

Téléchargez des jeux GRATUITS SUR VOTRE MOBILE!

BitTorrent | DVD Decrypter | CAMStudio
Geatalk | Bit-Che trouve tous les Torrents
Mixez avec Fruity Loops | Best of Jeux gratuits

2€50
PRIX CACHÉ

VOTRE MAGAZINE
Nouvelle Génération

Qu'est-ce que l'IP ?

On parle souvent d'adresse IP sans vraiment savoir de quoi il retourne. Cet identifiant unique est un numéro qui identifie chaque appareil connecté à Internet (ordinateur, serveur, tracker, téléphone, etc.) Utilisé pour communiquer avec le monde entier, ce numéro est aussi le seul moyen de vous retrouver sur la Toile. Voyons comment fonctionne ce système et quels sont ses points faibles...

Une adresse IP (pour «Internet Protocol») est un numéro qui, dans sa version 4, est écrit avec quatre nombres compris entre 0 et 254 et séparés par des points

(212.86.121.102, par exemple). Chaque appareil ou ordinateur connecté à Internet dispose de sa propre IP. Cette adresse est souvent attribuée aléatoirement



à chaque connexion. Parfois, elle change arbitrairement et d'autres fois, elle reste la même tout le temps (IP statique ou fixe). Même dans le cas d'une IP dynamique, votre FAI garde une trace des distributions d'IP. À telle heure, tel jour, Free, Orange et les autres savent qui vous êtes. Une injonction du tribunal les obligera alors à vous «balancer» si vous enfreznez la loi... L'IP est donc le seul moyen de mettre la main sur des terroristes, des pédophiles mais aussi de simples Internauts qui téléchargent.

Un système infallible ?

Mais attention, ce système de détection connaît pourtant des ratés. On se souvient de Gill et Ken Murdoch, respectivement 54 et 66 ans, qui ont reçu une lettre de l'avocat d'Atari pour leur indiquer que leur adresse IP avait été identifiée pour le téléchargement illégal d'un jeu vidéo. Bien sûr, Gill et Ken n'ont jamais utilisé une console de leur vie. Il y a différentes raisons



Connaissez votre IP !

Si vous êtes curieux de connaître votre propre IP, connectez-vous à www.mon-ip.com !



pour expliquer ces erreurs. La première concerne les petits malins qui usurpent l'IP d'une autre personne (masquer son identité sur Internet est légal, c'est l'usurpation d'IP qui est punie). Dernièrement, The Pirate Bay a lancé une opération consistant à inonder leur tracker avec de fausses IP. Ils espéraient alors casser le système en faisant accuser des innocents (la lutte aurait été alors vaine pour HADOPI et compagnie). Il y a aussi les personnes qui piratent le Wi-Fi du voisin...

Bientôt une imprimante française accusée de télécharger de Céline Dion ?



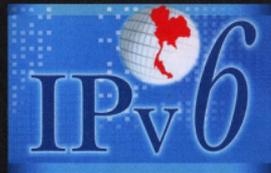
Tout le monde peut se faire accuser

Si votre réseau sans fil est mal configuré, vous pouvez vous retrouver accusé de télécharger illégalement alors qu'il n'en est rien. Il y a aussi les erreurs humaines et les erreurs des «robots», ces ordinateurs chargés de surveiller automatiquement des milliers d'IP. Un américain a même été accusé d'avoir téléchargé le film *Cadillac Records* via BitTorrent. Après plusieurs vérifications, il s'est avéré que c'est le nouveau propriétaire de son ancien routeur qui a commis l'infraction. L'histoire de ces professeurs de l'université de Washington est aussi édifiante. Ils ont réussi à faire accuser une imprimante de téléchargement illégal ! En voulant tester comment les sociétés de surveillance identifiaient ces Internauts pirates, ils se sont rendus compte que ces dernières se limitaient à une «détection indirecte» (une simple collecte d'IP sans vérification ou recoupage d'informations)... Pas étonnant de voir des retraités risquer la prison.



IP v6

Une adresse IP (pour «Internet Protocol») est un numéro qui, dans sa version 4, est écrit avec quatre nombres compris entre 0 et 254 et séparés par des points (212.86.121.102, par exemple). Chaque appareil ou ordinateur connecté à Internet dispose de sa propre IP. Cette adresse est souvent attribuée aléatoirement à chaque connexion. Parfois, elle change arbitrairement et d'autres fois, elle reste la même tout le temps (IP statique ou fixe). Même dans le cas d'une IP dynamique, votre FAI garde une trace des distributions d'IP. À telle heure, tel jour, Free, Orange et les autres savent



qui vous êtes. Une injonction du tribunal les obligera alors à vous «balancer» si vous enfreznez la loi... L'IP est donc le seul moyen de mettre la main sur des terroristes, des pédophiles mais aussi de simples Internauts qui téléchargent.

Selon les études les plus récentes, près de 90 % des informations disponibles sur le web ne sont pas indexées par les moteurs de recherches et sont donc inaccessibles. Bien sûr, « impossible » n'est pas un mot que connaît la rédaction, voici donc quelques outils qui vous permettront d'explorer un vaste réseau, riche en données souvent précieuses.

Le Web invisible n'a rien de mystique. Il ne s'agit pas d'un endroit où traquent les hackers, se cachant avant de passer à l'attaque. Le Web invisible, aussi connu sous le nom de Deep Web ou Web profond en français, se caractérise par son immensité. Sur la masse phénoménale des informations générées chaque jour sur l'Internet, seul un dixième est accessible à l'internaute lambda. La faute aux moteurs de recherches, aux robots d'indexation et à l'architecture même de l'Internet qui ne permet pas de traiter tous les contenus de manière égale. L'exemple le plus frappant reste les fichiers Flash et PDF qui,

il y a encore quelques années n'étaient pas référencés. Aujourd'hui il reste encore de nombreux fichiers qui ne sont pas pris en compte par les outils classiques de recherche. Les vidéos, les images en premier lieu ou les fichiers volumineux en font partie.

Il existe quatre types de contenus qui composent le Web invisible. De ces catégories, le Web opaque est celui qui se rapproche le plus du Web visible. Il concentre les pages peu ou mal référencées ainsi que les fichiers les plus conséquents puisque sur le Web, les pages de plus de 100 Ko sont peu utilisées. Le Web privé

représente quant à lui les pages qui sont volontairement cryptées par leurs auteurs. Les webmasters qui ne souhaitent pas que leurs pages soient aspirées, peuvent placer des scripts de protection dans des fichiers type robot.txt. De telles pratiques privent les sites de référencement et plongent inéluctablement le contenu dans les profondeurs du web. Le Web propriétaire est une autre catégorie qui regroupe les sites protégés par mot de passe, ou sécurisés. Enfin, il existe le Web dit « véritablement invisible ». Il s'agit des contenus dont le format ne permet pas l'indexation. Les pages web dynamiques dont l'URL n'est pas fixe ou encore les bases de données des bibliothèques ou des grands sites marchands.

DÉCOUVREZ

le WEB INVISIBLE!

Le web invisible représente environ 90 % du web !

À quoi ça sert le web invisible ?

S'il est difficile d'estimer la valeur du web invisible, qui par définition n'est pas visible. Les chercheurs et spécialistes considèrent que le Web profond regorge de ressources de première main. Les entreprises devraient y trouver un grand intérêt

puisque de nombreuses informations sur les concurrents circulent, de même que des informations sur les échanges B-to-B. Le niveau qualitatif des données serait même supérieur à celui du web visible, trop vulnérable à la falsification des données. Lors de recherches spécialisées sur un sujet donné, le web invisible peut apporter de nombreux

Les outils indispensables

De nombreux outils permettent très facilement de scruter la Toile cachée afin de découvrir ces informations rares et précieuses. Nous les avons classés en cinq catégories. Nous tenons cependant à vous prévenir que certaines recherches peuvent s'avérer fastidieuses, aux vues de l'immensité du domaine à découvrir.

> Les serveurs de banques de données

Qu'est-ce que c'est ? Il s'agit en réalité de gigantesques portails à la présentation souvent rétro, genre web 1.0, qui regroupent de nombreuses bases de données classées par thèmes.

Où les trouver ?

ABYZNewsLinks et Documentarium.info, pour les professionnels de l'information.
www.abyznewslinks.com



Amf scrute les sociétés cotées au microscope.
www.amf-france.org

Agrionline donne accès à l'ensemble des titres du Groupe France Agricole
www.agrionline.com

> Les moteurs spécialisés et métamoteurs

Qu'est-ce que c'est ? Ce sont des moteurs de recherches spécialisés dans un champ particulier, comme la science ou les sites commerciaux. Les métamoteurs sont de puissants sites qui utilisent plusieurs autres moteurs de recherches.

Où les trouver ?

Turbo10 est certainement le plus connu, il cherche parmi plus de 800 moteurs de recherches profonds.
www.turbo10.com



Direct Search ouvre le web invisible et rapatrie des résultats parmi les publications ou les sites gouvernementaux.
www.freepint.com/gary/direct.htm

Surf Wax est sans doute le plus web 2.0 puisqu'il permet de chercher au sein des feeds ou des blogs.
www.surfwax.com

éléments introuvables ailleurs. Une multitude d'articles scientifiques, de publications universitaires, de livres blancs du marketing hantent les tréfonds de notre Web. Les entreprises sont les principales gagnantes, même si peu d'entre elles sont conscientes de l'existence d'un tel vivier. Il devient très facile d'affiner sa stratégie grâce aux

nombreux outils disponibles, veille concurrentielle ou collection d'information. Mais le citoyen lambda aussi y trouvera son compte, en plus d'une information de première qualité, il y trouvera des données que les gouvernements ont souhaité laisser filtrer. De là à tomber sur un dossier classé top secret du Pentagone... on ne sait jamais.

> Les répertoires spécialisés

Qu'est-ce que c'est ? Ces répertoires sont en réalité des catalogues regroupant des informations sur des sujets précis. Si vous n'avez jamais réussi à trouver une information en particulier, c'est ici.

Où les trouver ?

US Copyright Catalog donne un accès à toutes les informations sur tout ce qui a été « copyrighté » aux États-Unis.
www.copyright.gov/records/

National Gallery of Art vous propose d'accéder à de nombreuses œuvres numérisées.
www.nga.gov/collection/index.shtml

Galaxy of Knowledge, comme son nom l'indique, vous y trouverez de nombreuses informations. Les recherches se font dans les ressources des Smithsonian Institution Libraries.
www.sil.si.edu



> Les bases de données

Qu'est-ce que c'est ? Vous pourrez accéder à l'information brute, ce sont de gigantesques piles d'informations regroupant des données gouvernementales, commerciales ou démographiques.

Où les trouver ?

Musée du Louvre regroupe les travaux du Louvre et un inventaire précis de toutes les œuvres.
www.louvre.fr/liv/oeuvres/bdd_oeuvre.jsp?bmLocale=en

Databases A-Z est une métabase qui vous permettra de chercher dans de multiples autres bases.
www.myunion.edu/library/dbtitle.asp

LexisNexis est la référence en matière d'information. Des enregistrements aussi bien publics que privés sont disponibles.
www.lexisnexis.com



PROTECTION FAIBLE

Résistez sans forcer !

Sans être un véritable forcené des réseaux P2P, vous voulez que votre vie privée soit respectée. Dans cette partie, vous trouverez des solutions simples à mettre en place pour un anonymat standard. Brouillez les pistes, bannissez les IP des majors et partagez sans peur...



- 19 **IPFilter X** : il bannit les IP qui vous scrutent !
- 22 **Le brouillage de protocole** : contre les FAI qui filtrent le P2P
- 24 **Partagez sans crainte** : le P2P décentralisé et le service Torrage

Protection Faible
FILTRAGE D'IP



Barrez les intrus

avec

IPFilterX !

En lieu et place du traditionnel PeerGuardian, nous vous proposons l'expérience IPFilterX qui s'intègre tout aussi bien à eMule. Celui-ci vous garantit davantage de sécurité, consomme moins de ressources systèmes et contient moins de faux positifs.

Les utilisateurs avisés utilisent avec eMule, le filtre d'IP, "IPFilter", pour davantage de confidentialité. Pour mémoire, il s'agit d'un fichier nommé "ipfilter.dat" qui contient une liste noire d'adresses IP jugées néfastes, insidieuses ou espionnes et qui seront systématiquement bloquées par eMule, sitôt qu'elles tenteront d'établir une liaison avec votre client. Le but de ce fichier est d'empêcher ces IP de visualiser vos fichiers, scanner vos ports, etc. Généralement, derrière ces adresses IP se cachent les agences gouvernementales, la RIAA, certains FAI et de façon globale la caste «anti-P2P».

IPFilterX
Gratuit

On aime

> Une liste d'IP «vérifiée»

On n'aime pas

> Un anonymat relatif

➔ <http://nexus23.org>

Le fichier IPfilter que l'on peut trouver sur les sites et forums spécialisés (Emule Pawcio homepage, Bluetack Internet Security Solution, Emule ZenZone, Emule Inside, Emule Project...) est très souvent maintenu à jour mais présente au moins deux défauts majeurs. Il contient un trop grand nombre d'adresses IP et parmi celles-ci bon nombre ne sont pas mises à jour et sont donc obsolètes. Les avantages d'IPfilterX sont nombreux. Celui-ci bloque les mêmes types d'IP suspects mais elles ne sont pas ajoutées sans avoir été au préalable vérifiées. Du coup, vous vous retrouvez face à un IPfilter.dat optimisé et plus efficace.



Récupérez la dernière liste d'IP suspectes sur le site officiel du logiciel...

Un filtrage intelligent

Le dernier IPfilter en date pèse presque 20 Mo et ne charge pas moins de 268 401 filtres IP ! À titre de comparaison, la version la plus récente d'filterX pèse quant à elle 371 Ko et comporte 6 500 filtres IP triés sur le volet... N'importe qui peut ajouter des adresses IP dans l'IPfilter traditionnel. L'inconvénient, c'est qu'il n'est pas rare de trouver alors des "ipfilter.dat" excédant le million d'adresses ! Un IPfilter qui intègre

trop d'adresses IP puise dans les ressources de la machine en ralentissant le système. Et, comme nous l'avons déjà précisé dans le trop grand nombre d'adresses IP incriminés beaucoup d'innocents sont bannis. Autrement dit, le P2Piste trop paranoïaque se prive en fin de compte de sources de téléchargements légitimes. Au final, avec IPfilterX vous êtes autant à l'abri qu'avec IPfilter et sans pénaliser votre machine et votre client de "peers" éventuels

Avec BitTorrent aussi !

Il existe deux autres versions d'IPfilter X toujours mis à jour par Nexus 23 Corp. et comportant la même liste noire d'IP que pour eMule. La première s'adresse à torrent et se nomme ipfilterX. La seconde est plus générique, il s'agit de PeerGuardX et elle fonctionne de concert avec PeerGuardian. Vous trouverez toutes les versions en partant du site <http://nexus23.org/warfare/content/view/17/34>.



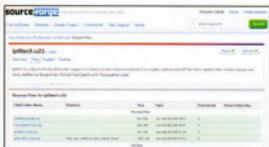
Ebooks-land.net

Utiliser IPfilterX avec eMule



1# TÉLÉCHARGEZ L'EXÉCUTABLE

Rendez-vous sur SourceForge, plutôt que sur un site lambda, ceci afin d'être sûr de télécharger une version fiable et mise à jour d'IPfilterX. Sur la page, récupérez l'archive compressée intitulée **ipfilterXB14-Cuse.zip**. Notez au passage que l'IPfilter fonctionne non



seulement avec eMule mais également sur plateformes Linux et Mac avec le client aMule.

2# INSTALLATION

Rendez-vous à l'aide de votre Explorateur Windows dans le dossier d'eMule. Maintenant, il ne reste plus qu'à extraire de l'archive le fichier **ipfilter.dat** puis, à le copier-coller dans le dossier **C:\eMule0.49c\config** ou **C:\Program Files\eMule0.49c\config** selon votre installation.



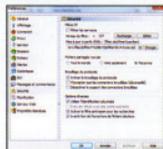
3# CHARGEZ LES FILTRES

Lancez le client eMule. Allez dans l'onglet **Serveurs**, puis dans le **Journal**. Si tout s'est bien déroulé, vous devriez pouvoir lire l'événement "6 500 filtres chargés". Votre IPfilterX est actif.



4# RÉGLEZ LES PRÉFÉRENCES

Afin d'éviter de recopier manuellement le fichier **IPfilter.dat** vous pouvez, tout comme avec IPfilter classique configurer en mode automatique. Pour cela, rendez-vous dans les **Préférences, Sécurité**. Dans le champ **Mise à jour** (http://sourceforge.net/projects/ed2k-ipfilterx/files/ipfilterX%20B14/ipfilterXB14-Cuse.zip). Vous devrez mettre le tout à jour régulièrement, tous les mois, par exemple, en cliquant sur le bouton **Charger**.





Le brouillage de protocole : UNE ARME LEGITIME

Certains FAI (Fournisseurs d'Accès à Internet) n'aiment pas vraiment eMule ou BitTorrent. Gourmands en bande passante, ces logiciels sont accusés de monopoliser une grande partie du réseau disponible. Nos chers prestataires ont alors commencé à filtrer volontairement leurs connexions. Grâce à des serveurs spéciaux, ils traquent les protocoles P2P pour limiter l'accès. Heureusement, il existe des solutions...

Dès 2005, certains internautes américains ont détecté des curieuses activités sur leur réseau. Après différents tests, ils se sont rendus compte que les protocoles P2P qui passaient par leur machine fonctionnaient moins bien que le protocole HTTP. En clair, ils surfaient sur le Net à la vitesse de l'éclair mais eMule ne fonctionnait presque plus. Grâce à certains serveurs

spéciaux intégrés dans leurs réseaux, les FAI américains, suivi de prêt par les FAI français, ont commencé à filtrer les flux P2P. Club Internet et Free ont été les premiers en France à se lancer dans une telle entreprise. Les utilisateurs d'eMule ou de BitTorrent victimes du bridage ne pouvaient quasiment pas se connecter, n'émettaient que très peu et ne téléchargeaient quasiment rien. Une honte

qu'on sait le prix que coûte un abonnement haut débit et que rien ne stipule sur votre contrat que les protocoles P2P sont bannis. C'est comme si Monsieur Peugeot accrochait un boulet derrière votre voiture sans rien vous signaler !

La solution !

Heureusement, il existe des solutions intégrées à nos chers logiciels : le Protocole Obfuscation pour eMule et le Protocol

Encryption pour BitTorrent. Ces fonctions de brouillage vont retirer l'étiquette «P2P» de vos échanges et vont rendre le filtrage des FAI inopérant. Attention ce brouillage de protocole ne vous rend en rien invisible sur la Toile. Il s'agit juste de masquer la vraie nature de vos téléchargements aux FAI. Reste à savoir si les organismes de surveillance comme HADOPI seront dupes ou pas. Pour un véritable anonymat, il faudra choisir une solution plus «costaude».

Le coût du filtrage

Ces serveurs si spéciaux ont coûté des fortunes aux FAI qui voulaient les acheter. Bien sûr, l'opération semblait rentable pour ces entreprises qui payent des sommes astronomiques en bande passante. Malheureusement, avec la multiplication des systèmes «anti-bridage» sur les logiciels P2P, ce filtrage est presque mort. Même la société Ipoque qui commercialisait ces appareils s'est résignée. En France, même si officiellement aucun FAI français ne bride plus les protocoles P2P, certains utilisateurs sont tout de même encore concernés par de tels ralentissements...

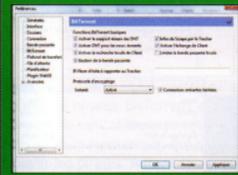
> AVEC EMULE

Lorsque vous paramétrez eMule pour la première fois, le logiciel vous demandera si vous voulez activer le brouillage de protocole. Cochez la case. Si votre eMule est déjà installé, allez dans **Préférences > Sécurité** et cliquez sur **Activez le brouillage de protocole**. Voilà, votre eMule est débloquée !



> AVEC µTORRENT

Dans µTorrent, il suffit d'aller dans **Options > Préférences > BitTorrent** puis de choisir **Activé dans Protocole d'encryptage**. Si vous ne constatez pas de différence, choisissez **Forcé** sans oublier de cocher la petite case à côté. Validez avant de sortir des options.





Retour aux sources!



Torrage
Gratuit

On aime

- > La décentralisation des échanges
- > Pas vu, pas pris

On n'aime pas

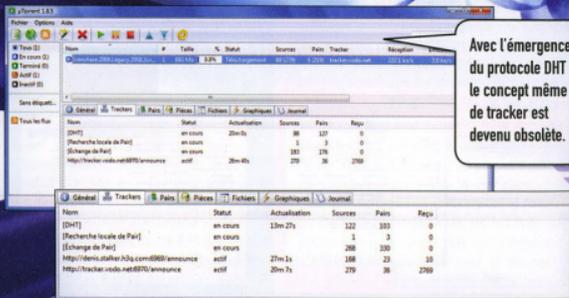
- > Le réseau torrent se complique

→ <http://torrage.com/>

Si les utilisateurs lambda du réseau BitTorrent souhaitent logiquement protéger leur anonymat des espions en tout genre, les seeders sont en réalité les plus exposés. Il existe cependant des techniques pour mieux les dissimuler et ainsi, pérenniser le réseau. Le site Torrage et le protocole DHT en font partie.

Plus de quartiers pour les sources ! C'était écrit, le point faible du réseau Bittorrent réside dans ses sources. Si elles venaient à disparaître, le réseau tout entier serait en péril. Les espions et les esprits malveillants l'ont bien

Avec l'émergence du protocole DHT le concept même de tracker est devenu obsolète.



compris puisqu'ils s'attaquent en priorité aux trackers et aux gros seeders (les utilisateurs qui partagent les fichiers source). La contre-attaque ne s'est pas fait attendre. Les développeurs des différents clients Torrent ont intégré des protocoles permettant de décentraliser les échanges et donc d'éviter l'utilisation des trackers. C'est le cas du DHT (Distributed Hash Table ou table de hachage distribuée) par exemple. Ce protocole est utilisé pour retrouver des informations (adresses IP, nombre de seeders/leechers) sur un réseau pair-à-pair. Avec cette technologie il est possible de se passer des trackers traditionnels et de mettre directement en contact les utilisateurs partageant le même fichier. Les clients µTorrent, BitTorrent, Vuze, Transmission ou encore BitComet intègrent tous cette fonctionnalité de manière transparente pour l'utilisateur.

Torrage, la botte de foin!

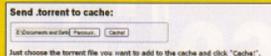
Ce protocole sert d'avantage à désengorger les trackers qu'à réellement protéger les seeders. Une autre solution est apparue récemment, le site Torrage. Grâce à ce site, il est désormais possible de stocker des fichiers torrents anonymement. Torrage n'est donc pas un tracker. En revanche, il peut aider ces derniers à se débouaner en cas de poursuites judiciaires. EZTV et Spnrova l'ont très bien compris puisque ces deux trackers utilisent déjà l'API de Torrage. Potentiellement, chaque internaute peut y stocker un torrent, récupérer son adresse puis la tracker. En effet Torrage est simplement un site de stockage et ne permet pas de lister les fichiers, ni de connaître le contenu vers lequel ils renvoient. Le site n'enregistre pas non plus les adresses IP de ses utilisateurs. Il

Utiliser Torrage



1# ENVOYER LE FICHIER

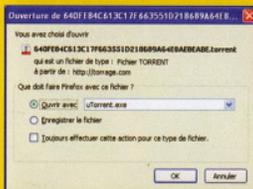
Sur la page d'accueil du site



Torrage, www.torrage.com, cliquez sur **Parcourir** pour sélectionner le fichier torrent que vous souhaitez stocker puis cliquez sur le bouton **Cache**.

2# RÉCUPÉRER ET DISTRIBUER

Le site vous donne ensuite une adresse ressemblant à [http://torrage.com/torrent/\(infohash_du_fichier_en_hexadecimal\).torrent](http://torrage.com/torrent/(infohash_du_fichier_en_hexadecimal).torrent), copiez cette adresse et collez-la sur votre blog



ou votre site. Le fichier Torrent sera directement accessible.

permet en somme une décentralisation extrême du réseau BitTorrent et devient synonyme de véritable casse-tête pour les ayants droit, par exemple, qui souhaitent retrouver les pirates. Autant chercher une aiguille dans une botte de foin!

Un anonymat solide

Pas besoin d'avoir fait Bac +23 pour rester anonyme sur Internet. Ce chapitre regroupe les principaux moyens permettant un anonymat efficace à 90% : P2P privé, proxy étranger, Seedbox, etc. Qui a dit qu'HADOPI était déjà dépassée ?

- 27 **Les proxy sont vos amis !**
- 33 **Le P2P privé :** entre amis ou gens de confiance uniquement...
- 38 **Louez une seedbox !** Elles téléchargent pour vous !
- 44 **La solution de facilité :** les téléchargements directs...



Les proxy : ils se connectent à votre place !

Si vous lisez nos publications, vous avez sans doute déjà entendu parler des proxy. Ces serveurs mandataires ont pour fonction de relayer des requêtes entre un poste client et, dans le cas qui nous intéresse, Internet. Dans la partie de cache-cache qui se joue actuellement avec l'État, ils sont de précieux alliés...



Lorsque l'on navigue sur Internet ou que l'on télécharge, notre ordinateur ainsi que tous les autres PC connectés à Internet utilisent une adresse unique, appelée adresse IP. Cette dernière



permet à tous les intervenants de communiquer avec les serveurs Web (qui eux aussi possèdent une IP). L'adresse est attribuée par le fournisseur d'accès Internet et change ou non à chaque nouvelle connexion. Lorsque vous vous connectez sur un site ou un serveur P2P distant, ce dernier conserve des journaux de connexion associant votre adresse IP aux pages consultées...ou aux fichiers téléchargés. Impossible à falsifier, cette adresse est unique et c'est aussi le seul moyen d'accuser un téléchargeur...

Le dernier maillon de la chaîne

Une façon de masquer son IP consiste à passer par un serveur intermédiaire qui se connectera à votre place aux sites Web ou aux serveurs. C'est le serveur mandataire qui laissera son IP. Bien sûr, un proxy garde aussi des traces de connexions pour sa propre maintenance et aussi pour des raisons légales. C'est là que réside l'astuce :

Masquer son protocole

La plupart des clients P2P proposent aussi une fonction qui a pour but le brouillage de protocole (protocol obfuscation). Cette solution est destinée à contrer le bridage de certains fournisseurs d'accès à Internet. Pour l'activer, allez dans **Préférences > Sécurité > Activer le brouillage du protocole**. Pour plus de détail, voir notre article page 18.

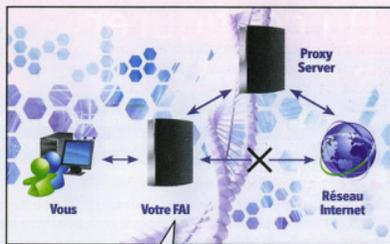
si votre IP passe par un proxy allemand (et même si en Allemagne, le piratage est tout aussi condamné), les robots d'HADOPI verront en vous un citoyen allemand et vous laisseront tranquille. Et si vous avez peur que votre dossier passe entre les mains de la police allemande, vous pouvez toujours trouver un proxy dans un pays qui



est un peu moins regardant en ce qui concerne le téléchargement. Mieux, il existe des proxy qui surfent sur cette nouvelle vague liberticide qui sévit en Europe pour proposer des connexions à des proxy «anonymes». Non seulement ils promettent de ne pas vous «donner» mais ils ne gardent pas de traces : les journaux de connexions sont gardés selon la loi en vigueur dans le pays mais parfois, il n'y a aucune loi ! Vous ne laissez donc aucune trace de votre passage et vous devenez invisible aux yeux des organismes de surveillances. Attention, plus le proxy que vous utilisez est loin et plus les temps de latence seront nombreux. En effet, les paquets doivent circuler de votre ordinateur au proxy, puis du proxy au site Web, puis la même chose en retour, sans compter le temps de traitement par le serveur proxy lui-même ! À vous de trouver le bon équilibre.

Le bon proxy

Trouver un proxy sécurisé, à l'étranger, rapide et autorisant des débits permet-



Quoiqu'il arrive, vous n'êtes jamais connectés directement au réseau

tant le téléchargement n'est pas aisé. Avec la nouvelle mode des VPN, la plupart des proxy se contentent de proposer un surf anonyme à leurs utilisateurs. Nous avons tout de même trouvé le site <http://proxy-list.org> qui dresse une liste de proxy en fonction de plusieurs critères : pays, niveau d'anonymat, cryptage SSL ou non, etc. Choisissez vos critères en faisant bien attention de prendre un proxy anonyme puis choisissez-en un dans la liste. Il est bien sûr primordial d'en prendre un à l'étranger mais pas trop loin non plus !

Vérifiez que votre proxy est actif !

Pour vérifier que votre proxy est bien actif et qu'il vous met bien à l'abri des petits curieux, il existe plusieurs adresses. Par exemple sur www.hostip.com, il est possible de voir votre IP et votre localisation sur une carte. Si ce service vous localise en France c'est que votre proxy ne marche pas ou qu'il est périmé...





Où configurer son proxy ?



Pour utiliser votre proxy, il va falloir rentrer certaines données dans votre logiciel fétiche : client Kademia ou Torrent, navigateur, etc. Voici comment procéder avec 3 principaux logiciels...

1# LES DONNÉES INDISPENSABLES

Pour la plupart des clients, il faut notifier le type de serveur (Socket 4, 4a, 5, HTTP 1.0, 1.1, HTTPS, etc.), l'adresse IP du proxy, le port, puis votre identifiant et mot de passe.

2# POUR EMULE ET µTORRENT

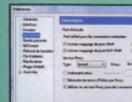
Avec eMule

Pour installer un proxy sous eMule, allez dans l'onglet **Préférences** > **Proxy** et cliquez sur la case **Activer Proxy**. Sélectionnez **HTTP 1.1** dans **Type de Proxy**. Pour le faire connecter au logiciel, il suffit d'indiquer l'adresse du proxy et son port. Généralement, les proxies utilisent les ports 80 (serveur http), 8080 (port de navigation http) ou 3128 (Active API Server Port), mais dans la pratique, n'importe quel port peut être exploité.



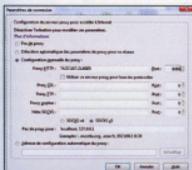
Avec µTorrent

Pour µTorrent, c'est pratiquement la même chose ! Allez dans **Options** > **Préférences** > **Connexion**. Si vos téléchargements ne décollent pas c'est que votre proxy ne fonctionne plus ou qu'il n'est malheureusement est pas compatible avec le débit des téléchargements. Essayez un autre proxy jusqu'à trouver votre bonheur. Il ne nous a fallu que 3 tentatives pour trouver un proxy adéquat !



3# LES AUTRES LOGICIELS

Pour n'importe quel autre logiciel, vous trouverez l'emplacement sans trop de difficulté (dans Options ou Préférences). Si vous désirez juste surfer anonymement, ouvrez Firefox puis allez dans **Outils** > **Options** > **Avancé** > **Réseau** puis cliquez dans **Paramètres** en face de **Connexion**. Vous trouverez tous les champs nécessaires à la mise en place de votre proxy. Une autre solution consiste aussi à se rendre sur un des nombreux proxy disponibles uniquement pour le surf : <http://www.free-proxy.fr>.



NOUVEAU !



L'avenir du numérique chez votre marchand de journaux

POUR TOUS VOS BESOINS,
TOUTES VOS ENVIES

LE NOUVEAU FORMULE!
LE MEILLEUR DE L'INFORMATIQUE FACILE ET PRATIQUE 2,70 €
N°4 PC ET INTERNET!
webpocket
TOUS LES OUTILS <> TOUTES LES ASTUCES
MARS - MAI 2010

2€
70

DOSSIER Découvrez la face cachée du Web

L'Internet SECRET

RÉSEAUX ALTERNATIFS

Si Internet ou nos libertés étaient menacés : ils sont prêts à prendre la relève !

WEB INVISIBLE

90% du Net est masqué. Comment y accéder ?

P2P & MAFIAS

Qui alimente les réseaux ? Qui en profite vraiment ?

COMPARATIF

Les nouvelles offres ADSL et fibre optique au crible

BON PLAN

Le troc pour tous !

WEBORAMA

Les meilleurs sites et services du WEB

INTERNET
MULTIMÉDIA
VIE PRATIQUE
LOISIRS

30 MICRO FICHES
L'informatique facile pour tous !

100% PRATIQUE



LE MEILLEUR DU WEB !

Protection Modérée
LE P2P PRIVÉ



Petits téléchargements

ENTRE AMIS!



OneSwarm
Gratuit

On aime

- > Ergonomie et esthétique
- > Intégration à Google
- > Anonymat

On n'aime pas

- > Difficile à utiliser à une grande échelle
- > Compliqué de trouver des sources

 <http://oneswarm.cs.washington.edu>

Rapides et sécurisés, les réseaux de P2P entre amis, aussi appelés F2F (Friend-to-Friend) ont le vent en poupe. Protégés des espions en tout genre et plus pratiques que le téléchargement direct, ces réseaux séduisent et il y a de quoi!

Que ce soit votre dernière vidéo de vacances avec votre tante du Vercors, les photos d'une soirée avec vos amis ou encore un dossier professionnel avec vos collègues, n'hésitez plus, partagez! Ces échanges en cercles

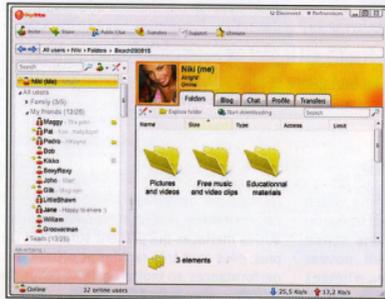
fermés ont l'avantage d'être réellement imperméables aux pirates, espions et autres menaces qui planent sur le P2P. De plus, elles sont très rapides et offrent des performances au moins égales à celles du téléchargement direct.

GigaTribu, LE p2p privé!

GigaTribu est le fer de lance du P2P privé ! Avec cette nouvelle version, encore plus simple d'utilisation, le logiciel souhaite surfer sur la mouvance « d'anonymisation » du P2P. Le principe du P2P privé est de permettre aux petites communautés, amis, familles, de partager des fichiers volumineux en pair à pair. Contrairement au P2P classique, ces fichiers ne seront donc accessibles qu'à un nombre restreint d'utilisateurs, qui devront avoir été invités au préalable. Les échanges sont chiffrés et donc protégés. L'autre avantage de partager ses fichiers de la sorte, en comparaison aux autres services de partage en ligne, c'est que la mise à jour se fait automatiquement. Pas besoin de passer une heure à uploader les images des dernières vacances par exemple.

GigaTribu, le MSN du partage de fichier

Une fois que vous avez invité vos amis, le partage se fait tout à fait naturellement. Dès qu'ils se connectent à GigaTribu, vous



Gigatribu permet de garder contact avec sa tribu numérique et de partager des fichiers volumineux.

les voyez apparaître dans le menu de droite, un peu comme la liste des contacts de MSN. Cliquez sur un des contacts pour avoir accès en temps réel à tous ses dossiers partagés. Vous naviguerez dans ses dossiers, comme si vous étiez sur son ordinateur et pourrez rapatrier facilement n'importe quel document qu'il partage. Seul bémol, parce qu'il y en a toujours un, dans sa version gratuite, GigaTribu ne permet pas le « multicoursing », autrement dit, si vous téléchargez une vidéo qui est aussi partagée par un autre utilisateur, plutôt que de télécharger des petits bouts sur les deux pour aller plus vite, vous ne téléchargerez qu'à partir d'une source. La version « Ultimate » de GigaTribu est donc la seule à permettre les sources multiples, elle possède aussi un algorithme particulier qui permet d'accélérer les téléchargements. En bref, GigaTribu s'impose comme un outil indispensable et sécurisé pour les tribus modernes.

OneSwarm, le P2P intelligent!

L'autre gros bonnet du F2F est plus récent et encore en phase d'expansion. Concocté par l'université de Washington, OneSwarm est sans aucun doute le logiciel d'échange le plus abouti de l'année 2009. Une nuée (swarm en anglais) d'utilisateurs pour se camoufler. C'est en quelques mots, l'idée principale

de OneSwarm. Les utilisateurs du logiciel sont totalement anonymes, protégés par l'architecture du protocole. Bien sûr qui dit principe innovant dit nouveau nom. Le P2P devient ainsi le F2F, comprenez friend-to-friend, soit A2A en français. OneSwarm relie les ordinateurs entre amis, que vous pouvez choisir ou inviter.

Comment ça marche ?

Lorsque vous faites une requête pour télécharger un fichier, le logiciel cherche chez votre voisin direct, si celui-ci ne possède pas le fichier, il lancera une requête chez son voisin direct et ainsi de suite. De sorte que personne ne sait d'où vient la requête sur son voisin direct et ainsi de suite. Les données font le chemin inverse. Les identités du receveur et de l'expéditeur sont ainsi protégées. Celui qui reçoit la requête ne peut, en aucun cas, savoir d'où elle provient. Aucune information sur les utilisateurs, telles que les adresses IP ou identifiants ne sont accessibles entre les utilisateurs du réseau. Ces données sont détenues par le réseau et cryptées dans une table de hachage spécifique.

OneSwarm
Privacy preserving peer-to-peer data sharing

New Fellow: [OneSwarm](#) | [OneSwarm](#) | [OneSwarm](#)

[Overview](#) | [Screenshots](#) | [Downloads](#) | [FAQ](#) | [Help](#) | [Features](#) | [Contact Us](#) | [Feedback](#)

Overview

OneSwarm is a new peer-to-peer tool that provides users with explicit control over their privacy by letting them determine how data is shared. Instead of storing data indiscriminately, data shared with OneSwarm can be made public, it can be shared with friends, shared with some friends but not others, and so forth. We call this friend-to-friend (F2F) data sharing. Check it out!

- Privacy preserving:** OneSwarm uses source address obfuscation to protect user privacy. Instead of user IP addresses, data identity data is used to recover identifiable identifying info. Check out our [Data Storage Usage Internals](#), covering the identity of both sender and receiver. For more info check out the [OneSwarm](#) [FAQ](#) or [Contact Us](#) page.
- User friendly:** OneSwarm is designed to be user friendly. It has a simple interface to search for files and share them.
- Simple:** OneSwarm is simple to use.

Le petit bijou sorti tout droit des cerveaux de Washington allie sécurité, anonymat et vitesse de téléchargement.

Utilisation originale

OneSwarm se différencie également des autres clients P2P de par son utilisation. L'interface est totalement intégrée dans votre navigateur par défaut. Elle est extrêmement simple et intuitive, ce qui ne l'empêche pas de permettre de nombreux réglages de paramètres. Les utilisateurs de Gtalk seront ravis de découvrir que OneSwarm détecte automatiquement vos amis. Il est également possible de scanner un réseau local et de trouver tous les utilisateurs de OneSwarm. Reste maintenant à savoir ce que le service peut donner à grande échelle.

L'autre client de P2P privé

WASTE est l'autre client de P2P privé. Il permet de créer des micros réseaux de 50 personnes maximum, afin de partager des fichiers. Les échanges sont totalement sécurisés et anonymes.

<http://wastegain.sourceforge.net/>



Echanger avec OneSwarm



1# PARTAGEZ

Pour commencer, vous devez définir le dossier de partage, dans lequel vous devrez stocker vos fichiers. Cliquez sur le bouton **Share**. Sous l'onglet **Manuel Sharing**, cliquez sur **Directory** puis **Choose Directory** et sélectionnez votre répertoire dans l'arborescence. Vous avez alors deux options, partager avec vos amis (**Share with friends**) ou rendre votre dossier public. Pour conserver votre anonymat, il est bien entendu conseillé de limiter le partage aux personnes que vous connaissez.



2# RÉGLEZ

Vous pourrez ensuite commencer à mettre les mains dans le moteur et ajuster quelques réglages. Tout d'abord, en cliquant sur le bouton **Settings**, vous pouvez sélectionner les ports d'écoute TCP et UDP de manière totalement aléatoire, grâce au bouton **Randomize**. Ceci évitera de tomber sur les ports écoutés de



manière systématique par ceux qui surveillent les réseaux. Vous pouvez aussi limiter la bande passante utilisée pour l'upload et le téléchargement de données. Notez que si vous sélectionnez 0, il n'y aura aucune limite. Nous vous conseillons de conserver les paramètres par défaut dans **Privacy Settings**. Ceci vous permettra de scanner le réseau local sur lequel vous vous trouvez pour découvrir de nouveaux amis. Enfin dans la partie **Remote access**, vous pouvez définir un nom d'utilisateur et un mot de passe pour vous connecter à votre compte à distance et gérer vos téléchargements.

3# TÉLÉCHARGEZ

Maintenant que toutes ces étapes sont accomplies, vous pouvez commencer à chercher des amis pour partager. Dans la colonne de gauche, cliquez sur **Add Friends**. Vous aurez ici, trois options, importer des contacts depuis **gTalk (Import friends from Gmail/Google Talk)**, trouver des amis sur le réseau local (**Import friends that are connected to my local network**) ou encore ajouter des amis à l'aide d'un cryptage par clé privée/clé publique (**Add friends manually using public keys**). Les deux premières options sont totalement automatisées, vous n'aurez qu'à entrer le nom de votre contact ou préciser son adresse IP. Pour la seconde, vous devrez définir la clé publique manuellement. Pour le reste vous pouvez utiliser OneSwarm comme n'importe quel client P2P et partager librement, sans contrôle.



LE MAGAZINE NOUVELLE GÉNÉRATION

HORS SÉRIE **CLICKLOAD** HORS SÉRIE
N°5 TÉLÉCHÈGEMENT // STREAMING
LE BEST-OF 2010

Numéro exceptionnel !

TOUT : LES MEILLEURS LOGICIELS
LES MEILLEURS SITES ET SERVICES

TÉLÉCHARGER

Films • Séries • Musique • Jeux

LE TOP 50 DE LA RÉDAC

P2P • STREAMING
USENET • MEGAUPLOAD
ANONYMAT • ETC.



100% PRATIQUE + ANONYMAT

Prise en main des meilleurs Softs & Services

Les vraies solutions au crible



EN KIOSQUE

NOUVEAU !



Les Seedbox

téléchargent pour vous !

Alors que de plus en plus de moyens existent pour éviter les fameuses lettres d'HADOPI, BitTorrent nous livre encore une surprise. Pourquoi changer de crémerie quand les bonnes vieilles méthodes se modernisent ? Les Seedbox permettent simplement de rapatrier vos téléchargements BitTorrent via votre navigateur. Il y en aura pour tout le monde...

Seedboxes

On aime

- > Vitesses de téléchargement
- > Fonctionne PC éteint
- > Discrétion
- > Votre bande passante est préservée

On n'aime pas

- > Les prix pas toujours abordables
- > Le manque de disponibilité des serveurs sur les meilleurs sites
- > Une prise en main parfois délicate



Une Seedbox est un serveur dédié qui est utilisé exclusivement pour les téléchargements BitTorrent. Ce dernier se charge de récupérer le ou les fichiers de votre choix pour vous le restituer ensuite en téléchargement direct. La Seedbox s'occupe aussi les "seeder" (d'où son nom de seedbox) vers les trackers. L'intérêt d'utiliser une Seedbox est multiple.

Vous louez un espace de stockage sur Internet qui gère vos downloads BitTorrent à ultra haute vitesse. Un must pour les dingues de téléchargements

CHOISIR SON SERVICE "SEEDBOX"

La location d'un seedbox peut être relativement onéreuse. Pour en choisir une adaptée à ses besoins, plusieurs critères importants entrent en ligne de compte :

> SON PRIX Certes, c'est souvent le critère décisif lors d'un achat ou, dans le cas présent, d'une location. Les tarifs s'échelonnent pour la plupart des offres entre une quinzaine et une centaine d'euros. Souvenez-vous qu'une solution alternative consiste à partager une seedbox entre plusieurs utilisateurs. Notez aussi que ces services étant souvent américains, les prix sont presque toujours annoncés en dollars 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. On trouve beaucoup d'offres proposant des disques durs de tailles avoisinant les 250 Gb, 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 Ce critère doit être considéré avec soin car la bande passante conditionne la vitesse de chargement. Pour faire simple, plus elle est élevée, mieux c'est. Vous trouverez des services offrant une bande passante de 100 Mb/s, 200 Mb/s, 1000 Mb/s, et on vous annoncera souvent une bande passante illimitée.

> LE NOMBRE DE TORRENTS ACTIFS SIMULTANÉMENT Ne négligez pas cet aspect, beaucoup d'offres n'ont aucune restriction de trafic, mais certaines limitent le nombre de torrents actifs simultanément sur votre serveur à moins d'une dizaine, parfois même à seulement deux.



Name	Size	Status	Progress	Download	Seed	Speed	Estimated Time	Actions
.../.../.../...	482.8 MB	Seeding	100%	734.6 KB/s	514.6 KB/s	152+4.997	00:00:29	[Icons]
.../.../.../...	756.7 MB	Seeding	100%	0.0 KB/s	54.4 KB/s	2+1.475	10:25:17	[Icons]
.../.../.../...	4.97 MB	Seeding	100%	20.9 KB/s	0.0 KB/s	0+0:289	04:18:46	[Icons]
.../.../.../...	231.9 MB	Done	100%				Download Successful	[Icons]

Dans un premier temps, les téléchargeurs passent entre les mailles du filet HADOPI puisqu'ils n'utilisent plus le protocole BitTorrent directement : c'est la Seedbox qui le fait.

Vous téléchargez sur un serveur ultra-rapide fourni par votre seedbox. Lorsque vous récupérez votre fichier, la vitesse de téléchargement s'envole en quelques secondes.

Choisir son service "seedbox"

> TorrentFlux

Incontestablement le plus populaire des services de location de serveur de type seedbox. Pour seulement 5, 9 ou 15 \$ mensuels, vous pourrez utiliser respectivement 2, 4 et 7 torrents simultanés. Une aubaine face à d'autres solutions souvent trop onéreuses. Le revers de la médaille, c'est qu'il faudra vous armer de patience pour profiter des services de TorrentFlux. Les inscriptions sont fermées et il faut s'inscrire sur une liste d'attente avant de devenir l'un des heureux élus.

www.torrentflux.com



> Seedbox.fr

Sur ce service français localisé à l'étranger, les forfaits commencent à 3 € pour 10 Gb de stockage avec une bande passante de 100 Mbps. Les forfaits

les plus chers sont à 25 €/mois. Pour ce prix, vous avez 1 To de capacité pour une bande passante atteignant les 1 Gbps... Pour tous les goûts et toutes les bourses...

www.seedbox.fr

Name	Size	Status	Progress	Download	Seed	Speed	Estimated Time	Actions
.../.../.../...	482.8 MB	Seeding	100%	734.6 KB/s	514.6 KB/s	152+4.997	00:00:29	[Icons]
.../.../.../...	756.7 MB	Seeding	100%	0.0 KB/s	54.4 KB/s	2+1.475	10:25:17	[Icons]
.../.../.../...	4.97 MB	Seeding	100%	20.9 KB/s	0.0 KB/s	0+0:289	04:18:46	[Icons]
.../.../.../...	231.9 MB	Done	100%				Download Successful	[Icons]

> Seedbox Hosting

Votre Seedbox va envoyer votre ratio dans la stratosphère, annonce le site. La bande passante et le nombre de fichiers torrents sont illimités. Pour 47 \$ par mois, vous aurez droit à 100 Gb de stockage contre 1 000 Gb si vous vous fendez de 97 \$ mensuels. Votre Seedbox est accessible dès le paiement effectué, contrairement à beaucoup d'autres services ou le délai est souvent de 48h. Par contre, tout le monde n'aura pas la



chance de trouver un serveur encore disponible à la location

<http://seedboxhosting.com>

À part le prix, les seedboxes n'ont que des avantages par rapport à un client Torrent traditionnel

Ensuite, vous devenez le roi de votre tracker ! En effet, avec les débits affichés par certaines Seedbox, votre ratio va décoller !

Enfin, la vitesse est un facteur déterminant. La plupart des Seedbox sont équipés en lignes très haut débit. C'est donc bien plus rapide que nos petits téléchargements "maison".

Une fois que la Seedbox a achevé le téléchargement, vous pourrez vous connecter à ce serveur via un petit logiciel ou une interface Web pour rapatrier votre fichier sur votre disque dur.

Quels avantages ?

Les seedboxes se développent très rapidement aux États-Unis mais restent encore largement méconnues en Europe et en



Non seulement les seedbox téléchargent à votre place mais le rapatriement du fichier en HTTP vous met à l'abri d'HADOPI !

Espagne. Outre la vitesse de téléchargement qu'elles autorisent, elles présentent de nombreux autres avantages :

[1] Ultra-haut débit
Évidemment, l'argument premier est que les serveurs de type seedbox sont équipés d'une connexion haut débit par fibre optique de 100 Mbits/s au minimum. Idéal pour obtenir de grandes quantités d'informations en un minimum de temps.

[2] Idéal pour les trackers privés
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.

[3] Ne vous occupez de rien !
Votre ordinateur n'a pas besoin de rester allumé pendant la durée du téléchargement car les serveurs disposent de leurs propres

disques durs. Vous pouvez donc télécharger 24h/24 et 7j/7 sans craindre d'endommager votre ordinateur ou de mettre le feu à votre maison !

[4] Votre bande passante lui dit merci
Le téléchargement de torrent n'a ainsi aucune incidence sur votre connexion Internet normale, aucune perte de débit ne ralentira votre surf. En revanche, la vitesse de téléchargement direct (FTP ou HTTP) des données présentes sur votre seedbox vers votre ordinateur dépend bien entendu de votre propre bande passante (donc de votre abonnement Internet).

[5] Confidentialité
Surtout, s'il pénètre à votre fournisseur d'accès à Internet la vilaine idée de brider votre connexion ou de limiter la quantité d'informations téléchargées par P2P (et ces vilaines idées gagnent du terrain...), cela n'affectera absolument en rien votre seedbox étant donné que la location du serveur inclut aussi la location de la connexion par fibre optique, nullement liée à votre FAI. Cela implique donc une plus grande sécurité vis-à-vis des espions.

Astuce : Louer une Seedbox à plusieurs

Pour réduire les coûts de location d'une Seedbox, une solution intéressante revient à partager une Seedbox et donc les frais de location entre plusieurs personnes. Il suffit de partager les logins et mots de passe entre les différents utilisateurs qui peuvent utiliser le serveur à leur convenance.

Télécharger un fichier avec BtAccel

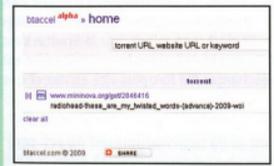


BtAccel se comporte comme une sorte de Seedbox. Ici les serveurs sont moins rapides mais le procédé est gratuit et la finalité est la même : faire télécharger un fichier via BitTorrent et le récupérer via http.

1# DÉMARREZ
Dans sa version de test, BtAccel permet aux utilisateurs «gratuits» jusqu'à 100 Go de téléchargement. Vous devrez simplement créer un compte après avoir demandé une invitation. Une fois que tout ceci est réglé, allez sur votre page d'accueil, Home. Entrez l'adresse du site sur lequel vous souhaitez récupérer le fichier torrent, et cliquez sur Get. Vous serez alors redirigés vers ce site via un proxy (par ex. <http://proxy.btaccel.com/www.mininova.org>). Faites votre sélection et téléchargez le .torrent. Ici, le dernier morceau de Radiohead, distribué gratuitement sur Mininova par le groupe.



2# TÉLÉCHARGEZ
Votre téléchargement démarre alors automatiquement sur BtAccel. Comme avec tous les clients BitTorrent, vous pourrez voir l'évolution du téléchargement et la vitesse de progression. Une dernière mise à jour du service permet également de suspendre et reprendre le téléchargement.



3# RAPATRIEZ
Une fois votre document téléchargé, cliquez sur le lien pour aller vers la page affichant les détails du fichier. Si plusieurs fichiers étaient inclus dans le .torrent, vous les verrez listés ici. Pour télécharger, cliquez simplement sur la partie qui vous intéresse, le reste se déroule comme un téléchargement direct en HTML.



TÉLÉCHARGEMENT DIRECT

L'alter-P2P!



MEGAUPLOAD

Le téléchargement direct, principalement représenté par Rapid Share, MegaUpload et Usenet (dont nous parlons un peu plus loin dans le magazine), s'impose petit à petit comme l'alternative idéale au P2P. Les échanges de fichiers volumineux sont simples et relativement sécurisés. Éclairage.

La plupart des services d'hébergement et de téléchargement direct sont basés dans des paradis du hacking

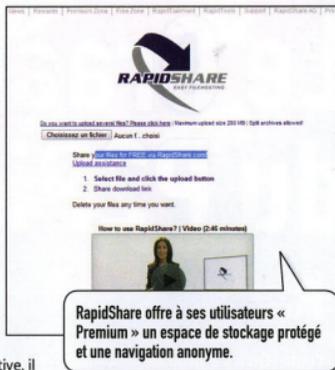
Échanger et partager sans P2P c'est possible! L'idée peut paraître saugrenue (surtout à la rédaction de Click and Load P2P) mais elle a fait son chemin. Le responsable n'est autre que le téléchargement direct. Les sites tels que RapidShare et MegaUpload sont légions. Il suffit à l'utilisateur de charger un fichier sur les serveurs de ces sites puis de récupérer l'adresse donnant accès au fichier distant. N'importe quelle personne en possession de ce lien peut ensuite télécharger le contenu. L'avantage majeur de cette technique sur le P2P est la vitesse. Si la qualité des échanges en P2P dépend du nombre de sources, le téléchargement direct s'effectue en HTTP et ne dépend donc que des capacités de votre ligne. Et c'est tant mieux, car la France s'est dotée des meilleures installations haut débit et il n'est pas rare de télécharger dix fois plus vite en direct que par le P2P.

Que vaut le cryptage Premium?

L'autre caractéristique appréciable du téléchargement direct réside dans l'anonymat qu'il procure. L'architecture de ce système fait qu'il est extrêmement difficile de se mettre entre le fichier et le téléchargeur et par conséquent de savoir qui télécharge quoi. De plus, RapidShare et MegaUpload proposent un service en HTTP sécurisé grâce au SSL (Secure Sockets Layer). Cette fonctionnalité réservée aux utilisateurs Premium (payants) rajoute une couche de données chiffrées à vos échanges. Pour savoir si cette protection est active, il faut se tourner vers votre barre d'adresse. Le site de RapidShare apparaît donc sous cette forme : <https://ssl.rapidshare.com>. Ceci garantit une plus grande sécurité dans les échanges de données entre votre ordinateur et les serveurs de RapidShare.

Est-ce vraiment anonyme?

Les téléchargements sont donc anonymes et protégés, en principe. En principe seulement car lorsque vous vous connectez à un serveur, celui en garde une trace. Or, si pour une raison ou pour une autre, les serveurs venaient à tomber entre les mains d'un tiers, vos logs de connexion seraient alors exposés. C'est la seule solution aujourd'hui qui est offerte aux ayants droit pour lutter contre le piratage des œuvres protégées. Or, la plupart des services d'hébergement et de téléchargement direct sont basés dans des paradis du hacking, où les autorités locales sont plutôt complaisantes. C'est le cas par exemple de MegaUpload dont le siège et les serveurs sont localisés à Hong-Kong.



La justice s'en mêle

les serveurs de RapidShare sont en revanche plus exposés puisqu'ils se situent en Allemagne. La justice allemande a d'ailleurs souvent eu maille à partir avec le site d'hébergement, condamnant RapidShare à de multiples reprises. Il y a six mois, RapidShare s'est vu condamné par une cour allemande à filtrer activement ses contenus. Une action qui, malgré toute la bonne volonté du monde, est difficilement réalisable, surtout quand on sait que les contenus des serveurs de RapidShare sont estimés à plusieurs dizaines de pétaoctets, soit plusieurs milliards de films (au hasard). L'autre menace est représentée par les ayants droit. Ceux-ci font régulièrement pression sur les sites d'hébergement et ont récemment réussi à obtenir l'adresse IP d'un utilisateur de RapidShare qui avait uploadé le dernier album de Metallica avant sa sortie. Attention donc, car l'anonymat de ces plateformes est à géométrie variable.

PROTECTION ELEVEE

Le Graal du P2Piste

Reservees aux plus forcenés des P2Pistes, ces solutions sont pour l'élite. Qu'il s'agisse de passer par un prestataire spécial (Usenet ou VPN) ou par des réglages plutôt alambiqués, c'est le chapitre de toutes les tentations.

- 47 Des réseaux privés virtuels : la face cachée de la Lune !
- 50 Le P2P crypté : quand "P2P" rime avec "caché"
- 56 Le côté obscur de la Toile : les Darknet...
- 60 Usenet, le protocole qui ne sert pas qu'à discuter...



Protection Elevée

LES RESEAUX PRIVES VIRTUELS



VPN : l'anonymat garanti

Avec la nouvelle loi HADOPI, nombreux sont les internautes qui souhaitent protéger leurs petits échanges de fichiers. Les solutions permettant de devenir anonyme sur la Toile deviennent de plus en plus nombreuses. Parmi ces dernières, on compte les VPN (Virtual Private Network). Voyons ce que propose cette technologie...



LES MEILLEURES DES SOLUTIONS ?

En ce qui concerne l'anonymat, il n'y a pas de meilleure solution. Ce qu'il faut savoir c'est que l'anonymat complet n'existe pas. Il y aura toujours un moyen de remonter jusqu'à vous (ce serait un peu trop facile pour les pédo-nazis d'Al Quaida non ?) La deuxième chose à savoir (et la bonne nouvelle), c'est que les ordinateurs qui traquent les P2Pistes sur le Web iront toujours au plus simple. Vous avez 10 fois plus de chance de vous faire attraper si vous téléchargez les derniers films sortis sur eMule ou BitTorrent que si vous avez ne serait-ce qu'une maigre protection. À vous de voir celle qui sera la moins contraignante et la plus économique...

Avec la quantité de nouveaux moyens mis à disposition des internautes pour se cacher de la méchante HADOPI, on s'y perd un peu. Certaines de ces solutions cumulant plusieurs technologies, la confusion est de mise pour les P2Pistes débutants...

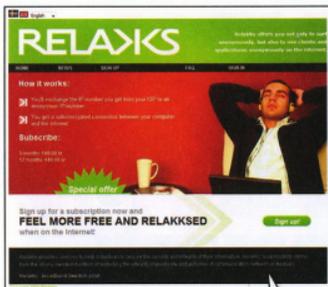


Les VPN

Un VPN (pour Virtual Private Network) permet de recréer en ligne via Internet, le même fonctionnement qu'un réseau local (où au moins deux ordinateurs sont reliés physiquement avec des câbles réseaux).

Pour profiter de cette technologie, il suffit de s'abonner à un service spécial donnant l'accès au réseau (voir notre pas à pas). Une fois que votre connexion à Internet passe par ce VPN, tous vos échanges de données sont cryptés (et pas seulement le protocole HTTP, comme c'est

le cas avec les «sites écrans»). Vous pouvez donc télécharger via BitTorrent ou eMule sans craindre les foudres d'HADOPI puisque personne ne peut savoir ce que vous faites. Pour plus de sécurité, nous vous conseillons de prendre un fournisseur de service qui ne soit pas français. De la sorte, personne ne pourra vous dénoncer, même pas un journal de connexions ! Pour vous faciliter la tâche, voici une petite liste de fournisseur de point d'accès VPN. Certains sont payants, d'autres non. Vous pouvez toujours tenter votre chance ou essayer avec un VPN gratuit mais il faut savoir



Basée en Suède, l'entreprise Relaks propose des solutions d'anonymat très avantageuses.

que les payants offrent une meilleure rapidité et une bande passante illimitée bien sûr...

- www.relaks.com
- www.ultravpn.fr
- <http://cyberghost.natado.fr>
(version gratuite limitée à 10 Go par mois)
- www.anchorfree.com
- <http://itshidden.com>

Devinez, devinez, devinez qui jeeeeee suis

Prendre des précautions sur les réseaux c'est bien mais est-ce que votre petite parade fonctionne ? Après avoir changé votre configuration réseau ou payé un tiers pour qu'il vous assure un anonymat, il faut encore vérifier que ça marche ! Pour cela, il existe un site qui vérifie que votre véritable IP n'est jamais accessible.

Concrètement, le site vous demande de télécharger un fichier torrent pour pouvoir vous certifier que la connexion est sûre et que l'IP est bien masquée. Bien sûr, c'est gratuit...

➤ <http://checkmytorrentip.com>

Configurez et Connectez-vous à votre VPN !



Avant de commencer, il faut savoir que chaque service VPN a sa propre méthode de fonctionnement, certains préférant une configuration automatique via un logiciel maison. Quoiqu'il arrive, faites confiance à la méthode de votre fournisseur. Cette méthode manuelle ne doit servir qu'en dernier recours ou si aucune explication n'est fournie par votre fournisseur VPN...

1# LE CENTRE RÉSEAU ET PARTAGE

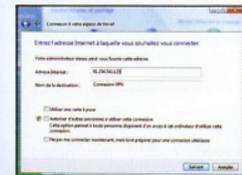
Après vous être abonné à un fournisseur de point d'accès VPN, cliquez sur **Démarrer**



puis allez faire un tour dans le **Panneau de configuration**. Cliquez sur l'icône vous invitant à afficher plus de détails (**Affichage classique**) et allez sur **Centre réseau et partage**.

2# VOTRE NOUVELLE CONNEXION

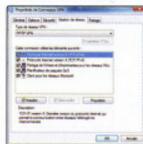
Cliquez ensuite sur **Configurer une nouvelle connexion** ou un **nouveau réseau**. Vous devrez ensuite choisir **Connexion à votre espace de travail** et cliquer sur **Suivant**. Dans cette liste, vous devez opter pour **Utiliser ma connexion Internet VPN**. Renseignez les champs adresse, nom, nom



d'utilisateur et mot de passe (qui vous sont donnés par votre fournisseur). Cliquez enfin sur **Connecter**.

3# LE PROTOCOLE PPTP

Si la connexion est lente, interrompez-la et dans vos paramètres réseau (les deux petits écrans en bas à droite de votre écran, près de l'horloge). Sélectionnez le nom de votre VPN et faites un clic droit pour trouver **Propriétés**. Dans le champ **Type de réseau**, choisissez le protocole **PPTP VPN** et validez. La connexion devrait être plus rapide.



4# HO LA BELLE IP TOUTE NEUVE !

Pour vérifier que votre IP est bien différente, allez sur www.mon-ip.com et regardez votre IP avec et sans la connexion au VPN. Vous êtes masqué sur la Toile ! À vous les téléchargements et bye bye HADOPI !





TOUS ANONYMES avec les réseaux cryptés !

Beaucoup vous le diront, la seule solution pour être totalement anonyme sur Internet est de passer par des réseaux parallèles cryptés. Quasiment indéchiffrables, vos données naviguent en toute sécurité. I2P et StealthNet en sont la parfaite illustration !

I2P

Gratuit

On aime

- > L'anonymat intégral
- > La communauté

On n'aime pas

- > La lenteur des échanges
- > La faiblesse des sources

➔ www.i2p.de

> scanning...

Cryptez vos échanges pour plus de sécurité. I2P est un protocole futuriste qui permet de créer une couche logicielle supplémentaire afin de crypter les échanges de messages sur le Net. Celle-ci est compatible avec de nombreux protocoles comme POP, SMTP, IRC et P2P. Par abus de langage, l'utilisation d'un client P2P avec I2P est appelé P3P, pour P2P de 3ème génération. Vous pouvez télécharger I2P sur le site officiel (www.i2p.de). Le logiciel est régulièrement mis à jour, la dernière version (0.7.3) date en effet du 18 mai 2009.

Comment ça marche ?

Une fois que vous avez téléchargé le logiciel, un simple double-clic suffira à l'installer. Il tournera ensuite en tâche de fond et vous permettra de vous connecter à un réseau anonyme. Plutôt que de vous connecter directement à un poste pair, vous passerez par un tunnel de connexions cryptées, rendant votre identité indécélabale. Pour faire simple, si Bob veut envoyer un message à Tom, il fera passer les données par Steve, Harry et peut-être même par George. Les détracteurs du projet argumenteront que de tels dispositifs ralentissent fortement les échanges de données. S'ils n'ont pas entièrement tort, ils doivent savoir qu'I2P s'efforce de réduire cet inconvénient réel au maximum.

Pas assez populaire

Reste à nos yeux un problème plus sérieux : le manque de sources disponibles sur ces réseaux «anonymisés». Peu d'utilisateurs ont eu vent de cette technologie, ce qui explique ce phénomène. Seule la solution I2P pour eMule rompt avec cette logique puisque les utilisateurs se connectent au réseau Kademia et bénéficient donc de ses millions de sources ! Notez également que I2P propose un client mail anonyme, idéal au moment où les publicitaires envahissent votre courrier.

eMule, BitTorrent et Gnutella

Pour conserver votre anonymat, les applications que vous utiliserez devront être compatibles avec I2P. Pour le P2P, plusieurs clients sont déjà disponibles pour les différents protocoles. Ainsi vous pourrez télécharger des fichiers torrent avec I2PSnark ou un plugin Vuze, utiliser I2PPhex pour le

Les bonnes adresses

> <http://forum.i2p>

Le site incontournable pour avoir réponse à vos questions les plus complexes.

> <http://eepsites.i2p>

Un annuaire de sites très pratique pour trouver des sites spécialisés.

> <http://tracker2.postman.i2p>

Le tracker de fichiers torrent I2P le plus connu.

> <http://crstrack.i2p/tracker/>

un autre tracker très fourni

> <http://planet.i2p>

Un agrégateur de flux RSS spécialisé dans le protocole I2P.

NDLR : Attention ces adresses ne seront accessibles que si vous avez configuré votre navigateur pour passer par le routeur I2P (lire notre pas à pas).

protocole Gnutella ou encore iMule pour Kademia. Si I2PSnark est inclus avec I2P, vous devrez bel et bien télécharger un client complémentaire si vous êtes fan des liens ed2k. Le client iMule est quasiment un clone d'eMule, basé sur le code de aMule, il est donc multplate-forme. Ce dernier nécessite tout de même quelques réglages et n'est pas à la portée des utilisateurs débutants.

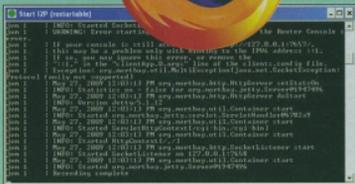
Pour BitTorrent, le Client I2PSnark est la solution idéale pour découvrir le fonctionnement de I2P. Si les téléchargements sont lents et les sources encore peu nombreuses, la communauté est très soudée et permet d'alimenter les quelques trackers spécialisés dans les torrents I2P.

Configurez Firefox avec I2P



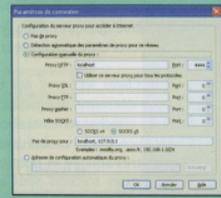
1# L'INSTALLATION

Une fois que vous avez installé I2P, cliquez sur l'icône Start I2P (restartable). Une fenêtre devrait s'ouvrir. Cette console vous indique en temps réel le statut de votre routeur I2P à travers lequel vous devez passer pour accéder au réseau I2P. Pour être sûr que cette couche logicielle est activée, regardez dans la barre d'outils système, vous devriez voir l'icône I2P.



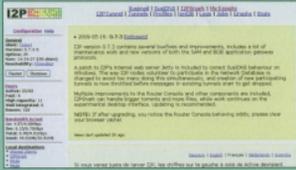
2# LA CONFIGURATION

Lancez ensuite Firefox. Dans le menu Outils, choisissez Options et cliquez sur Avancé. Sur l'onglet Réseau, cliquez sur le bouton Paramètres. Dans la fenêtre suivante, assurez-vous que la configuration manuelle du proxy est sélectionnée. Tapez localhost dans le champ proxy HTTP et choisissez le port 4444. Redémarrez ensuite Firefox pour que les changements soient pris en compte.



3# CONNECTEZ-VOUS!

Relancez I2P ou tapez l'adresse <http://127.0.0.1:7657> dans le navigateur. Vous aurez aussi accès à la configuration du routeur. Dans la colonne de droite, assurez que Uptime fonctionne, cette option montre le temps de connexion. Dans la partie Peers, Active devrait indiquer le nombre de pairs auxquels vous vous connectez, un chiffre supérieur à 100 devrait vous assurer une vitesse de navigation confortable. Notez les liens Configuration que nous utiliserons pour le pas à pas sur iMule et I2PSnark sur lequel vous devez cliquer pour vous connecter au client Torrent.



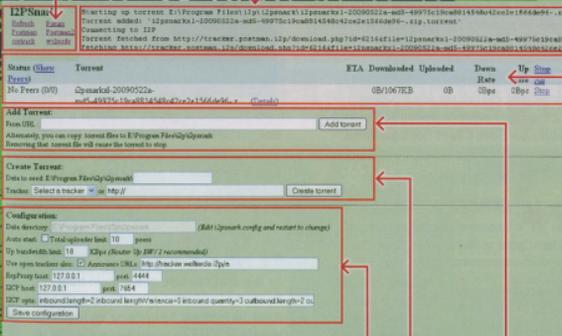
BitTorrent anonyme avec I2PSnark



Les liens utiles. I2PSnark vous fournit ici un lien vers des forums spécialisés ainsi que vers des trackers de Torrent I2P.

Le statut de votre torrent. I2PSnark établira la communication avec le tracker.

Retrouvez les informations traditionnelles sur vos téléchargements. Nom, nombre de pairs, avancement du fichier, taux de téléchargement et d'upload. Vous pourrez aussi interrompre et reprendre le téléchargement.



Vous pouvez ici définir, les limites de téléchargement ou le nombre de pairs autorisés à se connecter chez vous.

Vous pouvez également créer facilement un torrent, afin d'alimenter la communauté. Choisissez un fichier et un tracker.

Pour ajouter un torrent, indiquez le chemin local sur votre ordinateur ou depuis le tracker I2P en copiant l'adresse.

Télécharger avec iMule



Certains passionnés d'I2P n'ont pas hésité à reprendre la base du logiciel aMule pour créer un client compatible I2P et Kademia. Le résultat s'appelle iMule, un client relativement proche d'eMule, et est le seul moyen d'accéder à de nombreuses sources Kademia avec un anonymat garanti.

1# LE ROUTEUR

Avant de vous connecter à iMule, vous devrez cependant configurer vos routeurs. Dans la page Configuration



du routeur I2P (<http://127.0.0.1:7657/config.jsp>), cliquez sur le lien Client. Cochez l'option SAM application bridge, cliquez sur Save Client Configuration, puis sur le bouton Restart, dans le menu de droite.

2# LANCEZ VOTRE CLIENT

Laissez quelques minutes au routeur pour redémarrer et lancez le client iMule. Vous n'aurez pas beaucoup de réglages à faire ici. Le client iMule possède son propre serveur I2P, donc a priori, vous n'avez pas besoin d'installer I2P, nous

les conseillons tout de même pour des raisons de stabilité. Il faut donc désactiver cette option de iMule. Allez dans le menu

Préférences. Dans l'onglet I2P Connection, vérifiez que l'option Enable internal I2P server est bien décochée.

3# LES NOEUDS

Le client iMule se connecte ensuite tout seul aux nœuds Kademia. Une



liste par défaut est téléchargée automatiquement depuis www.imule.i2p/nodes.dat. En fouillant un peu sur les sites I2P (les Eepsites), vous trouverez des listes de nœuds plus fournie.

4# TÉLÉCHARGEZ !

Pour le reste, iMule fonctionne de la même manière que la mule traditionnelle. Le moteur de recherche est tout aussi performant. Le système de crédit est identique. Il est en revanche impossible de transférer ses crédits depuis eMule. L'anonymat à un prix.



StealthNet, l'autre réseau crypté !



Certains passionnés d'I2P n'ont pas hésité à reprendre la base du logiciel aMule pour créer un client compatible I2P et Kademia. Le résultat s'appelle iMule, un client relativement proche d'eMule, et est le seul moyen d'accéder à de nombreuses sources Kademia avec un anonymat garanti.

Entièrement gratuit et open source, StealthNet a été développé à partir du code source du célèbre programme Rshare. Cette plateforme de P2P chiffré (ou crypté) garanti à ses utilisateurs un anonymat complet sur son réseau. Le fonctionnement d'un tel logiciel est plutôt complexe : l'ensemble des informations qui circulent est crypté de tous bords et un système de clés publiques / privées (appelé cryptographie asymétrique) permet d'envoyer un fichier à un destinataire précis, sans qu'un tiers risque d'y avoir accès.

Malheureusement, les échanges sur les réseaux chiffrés sont souvent plus lents que ceux effectués via les logiciels de P2P classiques. Ceci s'explique facilement : les informations circulent dans tous les sens, elles sont cryptées, décryptées, cryptées à nouveau... bref, votre connexion a parfois du mal à suivre. De plus, ces réseaux séduisaient jusqu'ici peu d'utilisateurs et rassemblaient donc peu de sources. Aujourd'hui, les développeurs redoublent d'efforts pour créer des interfaces de plus en plus agréables.

Démarrez avec StealthNet



1# PARAMÈTRES

Rendez-vous dans l'onglet Paramètres, puis Préférences. Le port 6097 est indiqué, par défaut. Pour optimiser le fonctionnement de StealthNet, vous devez ouvrir ce port sur votre box ou votre routeur.

2# PRÉFÉRENCES

Si vous possédez un autre logiciel P2P, le plus simple est de remplacer le chiffre 6097 par celui correspondant au port TCP que vous avez déjà ouvert dans cet autre logiciel. Par exemple, pour eMule, vous trouverez ce numéro dans Préférences puis Connexion.



3# GARE AUX CONFLITS

Attention, pour éviter les conflits, vous ne devez pas utiliser StealthNet et eMule en même temps



Les Darknet, ces réseaux obscurs

La multiplication des lois liberticides stimule le développement de méthodes alternatives de téléchargement. La plus poussée mais aussi la plus controversée de ces méthodes est la connexion via un «darknet». Il s'agit d'une sorte de réseau privé virtuel ultra-sécurisé. Véritables outils de résistance pour les défenseurs du P2P, ces darknet peuvent aussi aider les criminels ou autres réseaux terroristes.

En créant des lois qui réduisent nos libertés et en attaquant systématiquement en justice les P2Pistes, ces derniers vont de plus en plus se tourner vers des solutions complètement clandestines. Nous vous avons déjà parlé des logiciels et solutions permettant de télécharger complètement incognito. Bien sûr les sources sont moins nombreuses mais au fur et à mesure que ces réseaux intéresseront les Internauts,



le choix augmentera exponentiellement. Il s'agit, en fait, de logiciels qui fonctionnent avec des protocoles cryptés (ou plus exactement «chiffrés»). Même si certains clients traditionnels (eMule, LimeWire, etc.) proposent quelques outils permettant de dissimuler la nature de vos échanges, dans les cas qui nous intéressent dans cet article, l'anonymat et la dissimulation sont de mise d'un bout à l'autre de la chaîne. Même votre adresse IP (c'est elle qui permet de vous identifier en cas de plainte) est invisible !

Freenet, le «darknet»

Le plus populaire de ces «réseaux anonymes» est Freenet. Il s'agit, en fait, d'un Web parallèle, où chaque utilisateur fait office de serveur (nœud ou «node» en anglais). Chaque participant stocke une partie du réseau dans son PC et tout est chiffré : c'est le principe du «darknet». Impossible d'obtenir une information sur un tiers ou même de censurer quelque chose. Les détracteurs de Freenet crient au scandale en brandissant l'argument de la cybercriminalité, des réseaux terroristes ou pédophiles alors que ses défenseurs parlent de liberté d'expression pour les dissidents Chinois, Biélorusses ou Birmans. Même si Freenet n'est pas forcément dédié au P2P, il existe des plugins permettant de s'échanger des fichiers. Par exemple, FreeMuleT intègre le réseau eDonkey, tout en assurant la confidentialité de Freenet...

Freenet et eMule, même combat

Dans le cas qui nous intéresse ici, nous allons voir comment il est possible de se servir de Freenet pour télécharger comme



Freenet a fait beaucoup d'effort pour se démocratiser...

sur le réseau Kademia. La seule différence avec votre eMule chérie, c'est bien sûr l'anonymat : ici personne ne vous connaît et tous les échanges sont chiffrés. Les robots informatiques de la future "riposte graduée" seront à des années lumière de se douter de quoi que ce soit. Le point noir, c'est le nombre de sources. Même si les utilisateurs sont de plus en plus nombreux depuis l'intégration d'un openNet (une manière beaucoup plus simple de se connecter et s'identifier), n'espérez pas trouver autant de choix que sur eMule. Le bon côté c'est que les P2Pistes français sont assez nombreux et vous trouverez un bon nombre de sources francophones. En ce qui concerne la rapidité, il vous faudra 2 ou 3 jours pour récupérer un fichier DivX standard de 700 Mo. En effet, le principe de fonctionnement un peu alambiqué et le chiffrage automatique rendent les débits un peu moins véloces qu'avec un client BitTorrent ou un eMule bien configuré...



FreeMULET, comment ça marche ?



Freenet
Gratuit

On aime

> Un réseau complètement sécurisé et anonyme

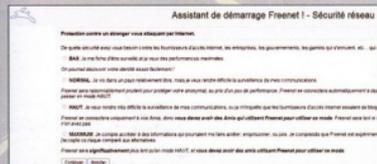
On n'aime pas

> Vous stockez des données (cryptées) qui ne sont pas les vôtres !

➔ <http://freenetproject.org>

1# INSTALLEZ FREENET

FreeMULET fonctionne avec Freenet, ce dernier doit donc être installé et lancé. Allez sur le site des développeurs et cliquez sur **Download** puis sur le lien **freenet.webinstall**. Suivez les instructions pour installer la version 0.75 du darknet. L'assistant de démarrage vous invite à paramétrer la sécurité générale du réseau (choisissez **Haut** si vos amis utilisent Freenet, **Maximum** si vous habitez en Chine ou **Normal** pour une première utilisation), la sécurité physique, la vitesse de votre connexion et la mémoire allouée.



2# L'AJOUT DE FREEMULET

Une fois Freenet lancé et prêt à fonctionner, il faudra aller sur ce lien via votre navigateur :

<http://board.planetpeer.de/index.php/topic,4081.0.html>. Ici vous trouverez le fichier binaire (binary) nécessaire à l'installation de FreeMULET. Cliquez sur le premier lien et une nouvelle page apparaîtra.

Faites ensuite un clic droit dans **Cliquez ici pour ouvrir le fichier** en tant que **application/java-archive** pour enfin faire **Enregistrer** la cible du lien sous... Mettez ce fichier dans votre bureau en attendant.



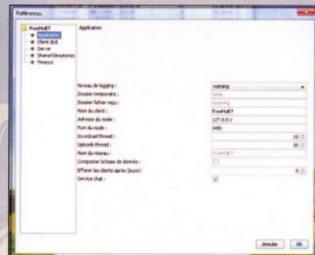
3# LA COMMANDE JAVA

Placez ensuite FreeMULET-0.6.30.jar dans un dossier. Toujours avec Freenet lancé, démarrez FreeMULET avec la commande **java -jar FreeMULET-0.6.30.jar** ou en double cliquant dessus (selon la version de votre JRE).



4# LA CONNEXION

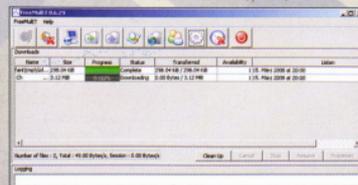
Connectez donc FreeMULET en cliquant sur **Connexion** en haut à gauche (l'icône en forme de prise électrique) et des peers vont apparaître. Le logiciel va alors télécharger l'index de leurs fichiers : soyez patient, toutes ces étapes peuvent prendre



quelques minutes en fonction du degré d'anonymat et de votre connexion. Vous pourrez alors lancer des recherches en vous dirigeant vers l'onglet **idoin** (avec la loupe).

5# C'EST PARTI !

Il suffit de taper votre requête et le tour est joué. Pendant que vous effectuez vos premiers téléchargements, vous pouvez faire un tour dans les autres onglets. Le panneau **Préférence** est disponible en cliquant sur l'engrenage. Vous pouvez ici paramétrer votre identifiant, l'adresse IP de votre «nœud», les dossiers de destination, etc. Les fichiers téléchargés seront placés, par défaut, dans le répertoire **Incoming** du dossier où se trouve FreeMULET. N'oubliez pas aussi de partager votre contenu avec le réseau





USENET l'anonymat absolu

Le vieux protocole Usenet, toujours utilisé de nos jours pour discuter, a dernièrement connu un regain d'intérêt auprès des P2Pistes. Ce système d'échange permet en effet de poster et de récupérer des fichiers. Hébergée sur des serveurs dédiés et protégée par le cryptage SSL, cette méthode de téléchargement fait de plus en plus d'adeptes...

Usenet est un ensemble de protocoles inventé bien avant la démocratisation d'Internet. Ce système sert en premier lieu à discuter de choses et d'autres sur des sortes de forums appelés «newsgroups». Tombé en désuétude mais tout de même utilisé par un noyau dur d'utilisateur, Usenet connaît à présent une seconde jeunesse. Certains utilisateurs ont, en effet, popularisé l'échange de fichier vidéo ou audio sur des groupes spéciaux



portant la mention «binaries». Alors que tous les newsgroups étaient disponibles via votre FAI, la RIAA et les Majors ont fait le ménage pour éviter le piratage massif. Dorénavant, pour accéder à l'ensemble des groupes, il faut s'acquitter d'un abonnement payant auprès d'un prestataire. Pour une somme comprise entre 2 et 20 € par mois, il est donc possible de télécharger à des vitesses pouvant dépasser les 5 Mo/sec ! Mais la cerise sur le gâteau, c'est qu'avec le cryptage SSL, l'accès est 100 % anonyme...

Comment cela fonctionne ?

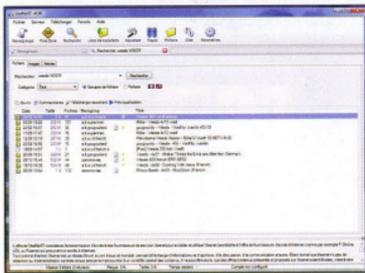
1. S'enregistrer auprès d'un prestataire
2. Télécharger le logiciel fourni par votre prestataire (ou en choisir un autre)
3. Configurer votre logiciel
4. Chercher et trouver des fichiers
5. Démarrer les téléchargements !

Le SSL : la clé de l'anonymat

En premier lieu, il faut souligner que Usenet est un peu en dehors du circuit traditionnel de téléchargement. Avec des serveurs éparpillés et un protocole «à part», les robots d'HADOPI iront plutôt voir ailleurs (utilisateur d'eMule, attention !). Mais si vous êtes d'un naturel parano, le SSL place la barre encore plus haut. Il s'agit d'un protocole de chiffrement qui fonctionne suivant un mode client-serveur. Il authentifie le serveur et garantit la confidentialité des données échangées sans échange de clé



De peur d'être «fliqué» sur la Toile, de nombreux P2Pistes se tournent maintenant vers Usenet



Cerise sur le gâteau, la fonction SSL est intégrée à l'architecture des serveurs Usenet. Ainsi, le cryptage de votre trafic ne ralentit jamais la progression des téléchargements et reste très léger pour votre système.

Les prestataires Usenet

Plusieurs sociétés prestataire d'accès Usenet proposent des services permettant de se connecter à tous les newsgroups, y compris les fameux «binaries».

Parmi les plus connus, on citera UseNeXT, Giganews, Power Usenet ou NewsHosting : chacun dispose de ses forces et de ses faiblesses mais les avantages par rapport à eMule ou BitTorrent sont significatifs :

**Grâce au protocole SSL
256 bits, à vous l'anonymat !
Pas de corps, pas de crime !**

publique (cette partie se fait de manière transparente pour l'utilisateur). La plupart des prestataires Usenet proposent un cryptage SSL 256 bits. Impossible donc pour les «policiers du Net» de remonter jusqu'aux Internauts qui utiliseraient Usenet pour pirater. L'identité, l'IP, le type de données envoyées et son contenu sont donc protégés. De même, les bridages des FAI peu scrupuleux (qui limitent votre bande passante lorsque vous téléchargez via eMule ou BitTorrent) sont inefficaces.

TLS ou SSL ?

Sur certains sites, vous trouverez aussi la trace d'un certain protocole TLS (Transport Layer Security). Il s'agit en fait du successeur du SSL (Secure Sockets Layer). Plus résistant mais aussi plus évolutif, le TLS est maintenant beaucoup plus utilisé que son grand frère. Néanmoins, par abus de langage, on parle plus souvent de SSL pour décrire ces deux protocoles de sécurisation...

un débit défiant toute concurrence et un cryptage des données permettant d'être intraçable sur la Toile. Sachez aussi que la plupart de ces sociétés proposent une période d'essai gratuit permettant de se faire une idée de ce que propose le service.

Avant de choisir votre fournisseur Usenet, il faudra prendre en compte différents paramètres, à commencer par la période de rétention. Il s'agit de «l'espérance de vie» du fichier. Car le fournisseur «nettoie» régulièrement ses bases de données (le stockage lui coûte bien sûr très cher). Plus la période de rétention est longue, plus les téléchargeurs auront accès à une base riche et diversifiée. Pour ceux qui mettent

à disposition leurs propres fichiers, ils savent que les autres Internauts y auront aussi accès plus longtemps. Là où les FAI n'offraient que quelques jours, les prestataires spécialisés peuvent accorder jusqu'à 240 jours !

Un autre critère à surveiller pour bien choisir votre fournisseur : le nombre de connexions simultanées, qui correspond au nombre de téléchargements que vous pouvez lancer en même temps. Plus il y en a, mieux c'est, bien sûr, pour attendre des vitesses vertigineuses ! Enfin, le point le plus important réside dans le coût du service. Ici, il s'agit de bien jauger l'utilisation que l'on va faire de cet abonnement car, souvent, le prix varie en fonction du nombre de gigaoctets téléchargés.



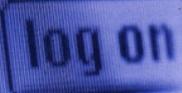
19.95\$ NHXL	14.95\$ NH Unlimited	10.00\$ NH Lite
<ul style="list-style-type: none"> Plus de 100 bases de données 40 connexions simultanées Streaming 240 jours Lightning Accelerator Téléchargement Boost 	<ul style="list-style-type: none"> Plus de 240 jours de rétention 30 connexions simultanées Cryptage SSL 256 bits Téléchargement Boost 	<ul style="list-style-type: none"> Plus de 240 jours de rétention 20 connexions simultanées Streaming 240 jours Lightning Accelerator Crédit de Téléchargement
INSCRIRE VOUS MAINTENANT	INSCRIRE VOUS MAINTENANT	INSCRIRE VOUS MAINTENANT

Comment ça marche ?

1. Le client se connecte au service Usenet sécurisé par SSL et lui demande de s'authentifier.
2. Le serveur envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification.
3. Le client vérifie la validité du certificat (donc l'authenticité du service), puis crée une clé secrète aléatoire puis chiffre cette clé à l'aide de la clé publique du serveur. Enfin, le client lui envoie le résultat (la clé de session).
4. Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. L'échange totalement sécurisé peut alors commencer...



LES OUTILS ESSENTIELS !



Dans ce numéro, nous vous avons présenté les meilleures techniques et méthodes pour passer inaperçu sur la Toile. Voici quelques outils complémentaires qui vous aideront dans votre course à l'anonymat. Attention, ils deviendront vite indispensables.

QuickPar > Recolle les morceaux

Nous l'avons déjà abordé, sur Usenet, les fichiers multimédias sont découpés en plusieurs petits fichiers de petite taille. Dans la plupart des logiciels que nous vous présentons, il n'est pas nécessaire de recombinaison les fichiers mais si vous optez pour un autre prestataire ou si vous utilisez Free, il faudra vous y coller. QuickPar est un logiciel qui permet justement de vous faciliter la vie de ce côté. Il suffit de l'installer et de cliquer sur Add Files. Choisissez votre groupe de fichiers en prenant bien soin de ne pas en oublier un. Cliquez ensuite sur Open. Si QuickPar vous semble un peu trop confus, vous pouvez toujours tenter de recombinaison vos fichiers avec WinZip, WinRAR ou bien le très bon (et gratuit) 7Zip. Il suffit pour cela de cliquer sur un des morceaux de fichiers pour que le logiciel restitue votre fichier final.

➔ www.quickpar.org.uk



HotSpot Shield > Le VPN

Les hotspots sont très pratiques, surtout si vous voulez consulter vos mails en mangeant un hamburger, malheureusement ils sont souvent infestés de connexions pirates. Attention donc à bien vous protéger, nombreux sont les pirates à attendre le faux pas. Lorsque vous vous connectez à un spot Wi-Fi, Hotspot Shield crée un réseau privé virtuel



(VPN) entre votre ordinateur et la passerelle Internet d'Anchor Free. Vous vous connectez au Web en mode 100% sécurisé.

➔ <http://hotspotshield.com/?lg=fr>

BitBlinder > Tracker privé

BitBlinder est un tracker privé qui permet l'échange de torrents

tout en restant anonyme et sans perte de vitesse. On peut aussi l'utiliser pour la navigation sur des sites web sur lesquels on veut rester discret, moyennant une petite perte de vitesse. Il s'agit sans doute du meilleur moyen aujourd'hui de naviguer de façon anonyme sans en payer la contrepartie.



➔ www.bitblinder.com

TOR > Web crypté

TOR est l'outil indispensable de cette sélection. Le logiciel s'est fait un nom depuis quelques années auprès des internautes qui recherchaient un peu d'anonymat. Il s'est depuis démocratisé et offre un service de qualité. TOR, le "roulage en onion", est un réseau mondial décentralisé de routeurs qui permet de rendre anonyme tout échange Internet basé sur le protocole TCP. C'est un logiciel libre distribué sous licence BSD révisée.

➔ www.torproject.org

NOTMYIP > Gratuit et efficace

Ce petit logiciel a créé le buzz à sa sortie. De nombreux utilisateurs ont fait le rapprochement avec la fameuse loi Hadopi qui utilise l'adresse IP des internautes comme preuve pour prononcer une éventuelle coupure d'accès. Or le



logiciel ne propose d'échanger son IP contre une IP étrangère... NotMyIP est une version dérivée gratuite du service Anonymity Gateway qui s'inscrit dans la liste des fameux "anonymiseurs". Il vous permet de vous affecter trois adresses IP différentes des Etats-Unis.

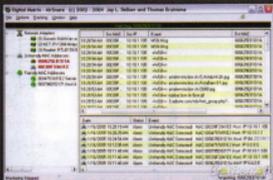
➔ www.privacy-gateway.com/notmyip.html





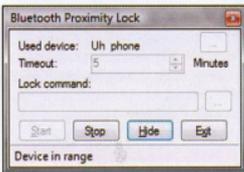
AirSnare > Espionner les espions
AirSnare vous permet de savoir si quelqu'un squatte votre réseau Wi-Fi. C'est un outil gratuit permettant de détecter les ordinateurs non autorisés sur votre connexion et permet de récupérer de nombreuses informations. Ce logiciel est reconnaissable à l'heure où la Haute autorité récemment mise en place (Hadopi) exige que vous protégiez votre connexion. Comme personne ne sait exactement comment faire, nous vous donnons une piste, utilisez Airsnare.

➔ <http://home.comcast.net/~jay.deboer/airsnare/index.html>



BTPprox > Verrouillage

Très ingénieux, BtProx propose une solution originale pour éviter que des petits curieux ne



feuilleter dans votre PC en votre absence. Il vous suffit d'un simple appareil Bluetooth (téléphone, iPod, etc.). Une fois configuré, le logiciel fermera votre session dès que votre appareil ne sera plus dans la portée du champ Bluetooth de votre ordinateur.

➔ <http://btprox.sourceforge.net/>

HAMACHI > VPN crypté

Au pays de Golderak, on ne fait pas tout comme tout le monde. Hamachi est un réseau privé... virtuel. C'est-à-dire que ses utilisateurs sont connectés entre-eux par VPN. À réserver aux grands paranoïaques... mais aussi aux amateurs de jeux en réseau puisque c'est à l'origine sa raison d'être principale !

➔ <https://secure.logmein.com/products/hamachi2>



ThreatFire >

Protection résidente
ThreatFire propose de protéger votre système des processus dont l'activité est nocive pour la stabilité de votre système. Il agit, en fait, comme un antivirus résident. Fonctionnant sans base de signatures, ce logiciel permet donc de se prémunir des attaques encore inconnues.

➔ <http://www.threatfire.com>



**UN MAGAZINE
LIBRE & ENGAGÉ**

PEER 2 PEER

CLICK & LOAD P2P

**Culture libre pour
tous, Technologie et
Respect des artistes!**



AVERTISSEMENT

Click & Load P2P est un magazine d'information, de débats et de sensibilisation technique aux nouveaux usages multimédia. Téléchargements, échanges de fichiers, diffusions d'œuvres numériques, droit d'auteur, innovations technologiques, communautés, nouveaux services en ligne : Down Load P2P traite de toute cette actualité culturelle, numérique et socio-économique qui intéresse plusieurs dizaines de millions d'internautes Français.

Nous rappelons à nos lecteurs que toutes les informations, logiciels, services et conseils présentés dans Click & Load P2P ne doivent en aucun cas servir à enfreindre le cadre législatif en vigueur, notamment celui lié à la protection du droit d'auteur. Vérifiez toujours que ces outils et actualités ne soient utilisés que pour favoriser un usage légal et responsable :

- 1) Téléchargement, copie et échange d'œuvres, programmes ou services libres de droit ;
- 2) Téléchargement, copie et échange d'œuvres, programmes ou services sous licence autorisant la copie ou l'usage privé et/ou non commercial ;
- 3) Téléchargement, copie et échange d'œuvres, programmes ou services dont vous avez acquis les droits exclusifs auprès d'une société ou de tout autre ayant droit, que ce soit à titre gratuit ou payant.

ID Presse et ses salariés se dégagent de toute responsabilité quant à l'usage délictueux ou infractuel que vous pourriez faire des informations, logiciels, services et conseils présentés dans Click & Load P2P. Vous devez vous conformer aux lois en vigueur en France ainsi que dans votre pays d'origine.

CLICK & LOAD P2P
N°6 – Avr. 2009 / Juin 2010
Une publication du groupe ID PRESSE
27, bd Charles Moretti – 13014 Marseille

E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme

RÉDACTION

Rédacteur en chef :
David Côme

Rédacteur en chef adjoint :
Benoit Bailleur

Dnt collaboré à ce numéro :
Michael Couvert, Virginie Ratto

Secrétaire :
Karima Allali

Directeur artistique :
Sergei Afanasiuk

Maquettiste :
Stéphanie Compin

Imprimé en France / Printed in France :
Léonce Deprez
Zi Le Moulin 62620 Ruitz

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : En cours

«Click & Load P2P» est édité par ID Presse, 27 bd Charles Moretti, 13014 Marseille. RCS - Marseille 491 497 665.

Parution : 4 numéros par an.
La reproduction, même partielle, des articles et illustrations parues dans «Maximum Down Load» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.



**GUIDE
PRATIQUE**

**UN ANONYMAT
GARANTI**

**Numéro
spécial**



PROTECTION ÉLEVÉE

PROTECTION MODÉRÉE

PROTECTION FAIBLE

71cucaracha, BuzyFun, eBooks-PARADIZE
pour

Ebooks-land.net

**VOTRE MAGAZINE + CD-ROM OFFERT
NOS GUIDES
DE RÉFÉRENCE**

L11970-6-F-3,90 €-RD

