

← CD OFFERT !

Août/Oct. 2011

PEER 2 PEER

CLICK P2P LOAD P2P

N°11

3,90 €

PIRATAGE, WAREZ, HACKING,
ANONYMAT, MENACES...

LE GUIDE

DU WEB INTERDIT

ENQUÊTE SUR :

**LES MAFIAS
DU WEB**

WAREZ, DROGUES,
TRAFIC DE DONNÉES,...



MENACES DU WEB

Les **TECHNIQUES DES
PIRATES** pour prendre
le contrôle de votre PC

CYBER ATTAQUES

Tout savoir sur les
nouveaux **HACKTIVISTES**

LES RÉSEAUX ANTI-CENSURE

Internet filtré... ou coupé ? Les
SOLUTIONS ALTERNATIVES existent !

**+
30** LOGICIELS
ET SERVICES
100% Web Interdit !

Les Menaces du Web

4

Les techniques et les nouvelles menaces

- 4 ▶ PHISHING : De plus en plus sophistiqué
- 8 ▶ Tout savoir sur les VIRUS, SPYWARES, ROGUES, VERS, ETC.
- 12 ▶ UN PC BLINDÉ : Les solutions en pratique
- 18 ▶ L'USURPATION D'IDENTITÉ
- 22 ▶ PIRATAGE DE BASES DE DONNÉES
- 26 ▶ WI-FI : Les menaces et les protections
- 30 ▶ DROGUES :
Le Web stupéfiant à haut risque



HACKTIVISTES

35

Une nouvelle génération de hackers « Robins des bois »

- 36 ▶ WIKILEAKS casse le Secret Défense
- 38 ▶ ANONYMOUS : Les vengeurs masqués
- 40 ▶ LULZ SECURITY : 50 jours de folie !
- 42 ▶ La galaxie des NOUVEAUX HACKERS

WAREZ, CULTURE & MAFIAS

45

L'univers Warez prône la liberté. Même celle de faire du business illégal ?

- 45 ▶ LEXIQUE : 40 termes pour s'y retrouver dans l'univers Warez
- 50 ▶ DÉCOUVREZ LA SCENE, l'antichambre secrète du P2P et du téléchargement direct
- 54 ▶ INTERVIEW : Les coulisses de la Scene



RÉSEAUX ANTI-CENSURE

58

Internet filtré ou coupé ? Découvrez les alternatives pour échapper au flicage tout en surfant incognito



LE MANIFESTE DU HACKER

62

Un texte de 1986 qui définit toujours la culture hacking pour des milliers de pirates



TOP 30 des Logiciels et Services 100% WEB INTERDIT

64



PROTÉGEZ-VOUS DU PHISHING !



Malgré les moyens mis en oeuvre par les géants du Web, malgré les listes noires de sites vérolés, le phishing touche de plus en plus de gens. Ces arnaques s'adaptent parfaitement aux nouvelles technologies et évoluent sans arrêt.

Attention aux escrocs pirates ! Ce n'est pas nouveau, le Net est un faisceau de propagation incomparable pour les arnaques en tout genre. Il y a un peu plus de 6 ans, avec l'émergence des achats en ligne, on voyait arriver le phishing, aussi connu sous le nom d'hameçonnage. Cette technique, très simple, consiste à faire croire à un internaute qu'il se trouve sur un site qu'il connaît bien (messenger, banque, etc.) afin de récupérer ses identifiants. Le pirate peut ensuite se connecter tranquillement avec les identifiants et essayer de chercher plus d'informations, comme un code de carte bleue ou des identifiants pour un compte PayPal.

COMMENT ÇA MARCHE ?

C'est sans surprise que les sites les plus visés par ces pratiques sont des sites marchands ou des banques. Il est fréquent de recevoir des mails provenant d'un faux site PayPal, par exemple, vous demandant de renseigner vos identifiants. En 2010, les cas de phishing à grande échelle se sont succédé. La Caf (Caisses d'allocations familiales) avait d'ailleurs dû mettre un message à destination de ses utilisateurs afin de les prévenir. Les escrocs envoyaient des messages affirmant que la Caf vous devait de l'argent, ils vous demandaient ensuite vos coordonnées personnelles afin de réaliser le virement. Avec ses coordonnées, ils ont ainsi pu détourner plusieurs milliers d'euros. Ce sont ensuite les banques de La Poste, de la Caisse d'Épargne ainsi que le fournisseur d'accès Orange, qui ont connu des imitations de leurs mails. Le dernier acte de phishing en date concerne une enseigne un peu différente, puisqu'il s'agit de Mc Donald's. Ici, le leurre est un repas

gratuit (les hackers ont vraiment beaucoup d'imagination). Pour obtenir ce repas, vous devez télécharger un formulaire, qui est en fait un trojan.

LES PIRATES FONT LEUR BEURRE

Si ces techniques peuvent s'apparenter à des feintes de Sioux, cela n'empêche pas de nombreux internautes de tomber dans le panneau. En France, l'institut Ponemon estime à 2,2 millions d'euros l'argent récolté illégalement auprès des entreprises. Et selon Edward Amoroso, responsable des systèmes d'information chez AT&T, ce montant serait en fait bien plus important et s'élèverait même à 1000 milliards de dollars par an à l'échelle mondiale (entreprises et particuliers réunis). Si ces méthodes sont aussi performantes, c'est parce qu'elles s'adaptent parfaitement aux nouvelles technologies.

Objet: CAF - Nous vous devons 161,82 euro



Vous avons étudié vos droits à partir du 01.01.2010
Il apparaît après calcul que pour mois 01.11.09 - 01.12.09
vous n'avez rien reçu alors que vous aviez droit à 161,82 euro.
NOUS VOUS DEVONS 161,82 euro.
Votre Caisse d'Allocations familiales.

[cliquez ici pour entrer](#)

Les pirates n'hésitent pas à s'attaquer à des sites tels que la Caf. Si vous recevez un mail suspicieux de ce type, ne suivez pas le lien et surtout, ne communiquez pas vos données personnelles (téléphone, numéros de compte, etc.)

LES NOUVELLES MÉTHODES

Ainsi, en 2010, nous avons vu émerger deux nouvelles techniques. Le TabNabbing et les « attachements » HTML 5. La première consiste à transformer un site lorsque vous ouvrez un nouvel onglet. Quand vous revenez au premier site, celui-ci ressemble à une page de connexion, sauf qu'elle est factice. Si vous entrez vos identifiants, ils seront enregistrés dans une base de donnée pirate. Ici, les pirates jouent sur les dernières évolutions de vos navigateurs et exploitent les moindres failles. La méthode des

Selon un spécialiste des systèmes d'information chez AT&T, le montant détourné par le phishing dépasserait les 1000 milliards de dollars à l'échelle mondiale pour l'année 2010 !

attachements HTML utilise quant à elle la technologie HTML5. Grâce à HTML5 vous pouvez afficher une page hors connexion. Les liens que vous recevez dans les mails pointent donc désormais vers ces fausses pages qui, elles-mêmes vous redirigeront vers des sites inconnus des filtres anti-phishing. Les pirates démontrent ici, si besoin en était, qu'ils ont toujours un temps d'avance lorsqu'il s'agit d'exploiter au maximum les capacités des nouvelles technologies.

5 ASTUCES POUR LUTTER CONTRE LE PHISHING

Il existe tout de même des méthodes simples pour éviter de tomber dans le piège du phishing.

- 1. Bien étudier le contenu de votre email.** S'il provient de votre banque ou d'un site marchand, il ne doit pas être bourré des fautes d'orthographe. Or, les pirates sont souvent étrangers ou mauvais en orthographe, résultat, il est très facile de déjouer leur piège. Envoyez le mail à la poubelle.
- 2. Ne jamais donner vos informations personnelles.** Votre banque ou les sites marchands ne vous demanderont jamais des informations bancaires ou vos identifiants. Si une telle demande vous est faite, alors le message est suspicieux.
- 3. Ne pas cliquer sur les liens.** Évitez à tout prix de cliquer sur les liens contenus dans les mails. Il est encore préférable de les retaper à la main dans votre navigateur. Les adresses de phishing ressemblent très fortement aux vraies adresses, observez les bien. Parfois, seule une lettre sera différente.
- 4. Vérifier la connexion sécurisée.** Quasiment tous les sites de confiance utilisent désormais des connexions sécurisées. Pour vérifier que c'est bien le cas, regardez la barre d'adresse, vous devriez y trouver la mention HTTPS ou un logo représentant un cadenas.
- 5. Vérifier les certificats.** Si enfin, vous avez encore un doute, vous pouvez aller dans les paramètres de sécurité de votre navigateur afin de vérifier les certificats du site.

Les outils pour lutter CONTRE LE PHISHING

CHROME

❖ Navigation sécurisée

Le navigateur « made in » Google a toujours été à la pointe de la navigation sécurisée. Vous ne laisserez aucune trace sur le web pouvant être utilisée par les pirates. Chrome met également en évidence la partie principale de l'adresse pour faciliter les vérifications.



🌐 www.google.com/chrome

OPERA

❖ Filtre

Opera a été le premier des navigateurs à intégrer un filtre antiphishing. Dans sa version actuelle, le navigateur établit un état de la réputation du site sur lequel vous vous trouvez. Pour cela, il vous suffit de passer la souris sur la zone à gauche de la barre d'adresse.



🌐 www.opera.com

BITDEFENDER ANTI-PHISHING FREE EDITION

❖ Anti-virus

BitDefender est une solution généraliste pour lutter contre tous les types de Malwares. Ce module gratuit filtre pour vous les liens et adresses suspectes dans vos mails, conversations instantanées ou lors de votre navigation sur le web.

🌐 www.bitdefender.fr



LONG URL PLEASE

❖ Démasqué

Pour tromper les internautes avec de fausses adresses, les pirates n'hésitent pas à utiliser les raccourcisseurs d'adresse. Long URL Please est un plugin Firefox qui retrouve pour vous l'adresse originale dans sa version longue.



🌐 www.longurlplease.com

PANDA CLOUD ANTI-VIRUS

❖ Le Cloud

Panda est une application antivirus en ligne. Autrement dit, vous n'aurez pas besoin d'installer quoi que ce soit. Panda Cloud fait une veille permanente pour mettre à jour la liste des sites bloqués et faire de la protection en temps réel.

🌐 www.cloudantivirus.com





MALWARES :

CONNAÎTRE TOUTES LES MENACES

Internet, c'est merveilleux ! Une telle source de culture et d'information serait presque parfaite si l'on n'était pas confronté aux mauvaises surprises que sont les virus, les spywares et autres malwares. [Click & Load P2P](#) vous explique les différences et vous donne toutes les pistes pour naviguer sur une mer d'huile...

Lorsque l'on parle de virus informatique, on fait allusion à un petit programme qui s'installe sur votre PC et le rend plus ou moins inopérant. Or, ce terme est un peu usurpé : en effet, on devrait plutôt parler de «malware». Voyons les différences entre ces bêtes et comment s'en protéger...

Les virus

Le virus est un morceau de programme s'intégrant dans un autre logiciel. Chaque fois que l'utilisateur exécute ce programme «infecté», il active ainsi le virus qui ira se fondre dans d'autres programmes. À la longue, cela peut rendre inutilisable l'ordinateur et cela peut signifier la perte de toutes vos données.



NOTRE ASTUCE

Installez un antivirus avec une protection résidente et mettez-le à jour le plus souvent possible. Évitez aussi les pièces jointes ou les fichiers EXE qu'un «ami» vous aura envoyés...



NOTRE ASTUCE

Ici aussi un l'antivirus est votre partenaire idéal. Comme certains vers s'activent à une date précise, un scan de temps en temps ne fait pas de mal non plus. Attention aux sites à problèmes : porno, warez ainsi que les liens vers des pages inconnues...

Les vers

Le ver est un malware qui se propage sur des ordinateurs grâce à Internet. Contrairement au virus, le ver n'a pas besoin d'un programme hôte pour se reproduire. Il exploite des failles dans des programmes (messagerie instantanée, client mail, etc.) afin d'assurer sa propagation et corrompre votre système.

Les chevaux de Troie ou «trojans»

Quant au cheval de Troie, il s'agit d'un logiciel qui a l'apparence d'un programme «propre», mais qui est conçu pour exécuter des actions nuisibles dans le dos de l'utilisateur. Vous pouvez donc sans le savoir servir d'hôte pour un pirate qui «volera» votre IP pour accomplir ses méfaits.



NOTRE ASTUCE

Comme les vers ou les virus, les trojans n'aiment pas les antivirus bien configurés. Pour certains cas particuliers, vous pouvez aussi utiliser le logiciel gratuit HijackThis qui permet de contrôler les programmes lancés au démarrage ou les composants «louches»...

Les spywares

Le spyware est un logiciel que vous pouvez contracter de la même manière qu'un malware, au fil de vos surfs. Il peut aussi être intégré dans un programme «normal» et s'installer en même temps que celui-ci. Le but des spywares est d'épier vos surfs, vos horaires de connexion, vos adresses e-mail, etc. Ils peuvent aussi mémoriser vos données privées (genre, âge, situation de famille), tout ce qui pourrait aider des tiers à dresser une fiche sur vous ou votre famille.



NOTRE ASTUCE

Attention, les antivirus sont souvent inefficaces contre les spywares. Pour éviter ces indésirables, il suffit de bien configurer votre firewall et de surtout faire attention lors de l'installation de programmes inconnus ! Ils cachent parfois des spywares très pénibles à éradiquer.

Les adwares

Pour les adwares, le principe est un peu différent. Ces petits programmes n'ont pas pour vocation de vous espionner directement, mais d'afficher sur votre écran diverses publicités. Bien sûr, pour pouvoir cibler ces «pop-up», ces derniers peuvent s'octroyer le droit de fouiner un peu dans votre PC, à la recherche de mots-clés ou de noms de fichiers évocateurs. Certains sont à la fois spyware et adware...



NOTRE ASTUCE

Outre les logiciels spécialisés dans la suppression des adwares (Ad-Aware, etc.), il convient de faire attention lors de l'installation de plugin ou de programmes que vous ne connaissez pas. Généralement, c'est vous qui êtes responsable de leur installation sur votre PC en cliquant trop rapidement sur «Suivant» !

Les rogues

Les rogues sont de faux antivirus créés par des petits filous pour faire de l'argent sur la crédulité des internautes. Tout commence par une infection bénigne, le rogue s'installe sur votre ordinateur, mais ne détruit rien du tout. Au bout de quelques minutes, vous verrez une fenêtre, un pop-up ou un avertissement Windows qui vous indique qu'une menace est détectée sur votre ordinateur. Bien sûr cette menace est imaginaire et pour supprimer ces infections, vous devez passer à la caisse ! Si vous ne cédez pas, le rogue va alors tout mettre en œuvre pour vous faire craquer : affichage de plusieurs fenêtres, modification du fond d'écran (pour faire croire à quelque chose de sérieux, etc.)



NOTRE ASTUCE

Les rogues s'attrapent comme des vers, mais ne sont pas tout le temps détectés comme des menaces. Évitez à tout prix de cliquer sur un bouton provenant d'un antivirus que vous n'avez pas installé. Refusez bien sûr de payer quoique soit et tentez une décontamination avec Malwarebytes Anti-Malware...

LES PRÉCAUTIONS

Il existe des astuces très simples pour éviter de formater son disque dur et réinstaller ce bon vieux Windows. Une des premières mesures est d'éviter à tout prix les sites «à risque» : pornographie, piratage, sites vous proposant monts et merveilles (gagnez de l'argent facile, des cadeaux, etc.) Il est aussi indispensable de réfléchir à deux fois avant d'ouvrir une pièce jointe envoyée par e-mail. Si vous connaissez l'expéditeur, il y a peu de chance que vous vous retrouviez infecté (quoique certains malwares peuvent usurper l'identité d'un de vos contacts). Par contre, attention à toute pièce jointe expédiée par un tiers inconnu : vous pourriez vous en mordre les doigts ! Malgré toutes ces précautions, votre PC ne deviendra jamais une forteresse imprenable, sans l'aide de logiciels dédiés à la sécurité (voir pages suivantes).

SURF SUR INTERNET :

UN PC BLINDÉ !

Comme nous l'avons vu dans les pages précédentes, il existe moult embûches lorsque l'on souhaite surfer sur Internet. Voyons comment éviter les problèmes avec les trois logiciels que nous vous proposons. Un pour chaque type de problème !

AVIS DE LA RÉDACTION

On aime :

- La gratuité
- Une bonne solution «tout en un»

On n'aime pas :

- La voix de la femme qui annonce les mises à jour !

www.avast.com

GRATUIT

AVAST! NOTRE ANTIVIRUS STAR

L'antivirus préféré de la rédaction est l'arme idéale contre les virus, les vers et autres trojans. En plus des mises à jour quotidiennes et de sa protection résidente, ce nouvel opus d'Avast! propose deux fonctionnalités qui n'étaient présentes que sur les versions payantes...

VIRUS, VERS ET TROJANS

Avast! est un terme nautique anglais qui signifie «stop». Non seulement Avast! permet de réaliser des scans très poussés (rapide, minutieux, sélectif ou sur des supports amovibles), mais il dispose d'une protection résidente très efficace. À la moindre alerte, Avast! prévient l'utilisateur et lui laisse le choix dans la marche à suivre. Ce logiciel permet l'analyse en temps réel des documents ouverts, des programmes exécutés, des e-mails entrants et sortants, des logiciels PE, des messageries instantanées, etc. Les mises à jour sont automatiques et quotidiennes, le logiciel ne demandant rien qu'un enregistrement gratuit par an pour fonctionner. Les utilisateurs avancés peuvent aussi compter sur les réglages «Experts» et prédéterminer des actions à effectuer en cas d'alerte...

LA VERSION 6

Cette version comprend tout de même son lot de nouveauté. Elle intègre, en effet, deux nouvelles fonctionnalités qui étaient autrefois payantes : la Sandbox et WebRep. La première permet de créer une machine virtuelle qui va agir comme une «zone tampon». Si un programme suspect est sur le point de se lancer, cet ordinateur virtuel s'éteindra en laissant le véritable système sain et sauf. WebRep permet, quant à lui, d'informer les internautes sur le véritable contenu d'un site grâce à un système de vote. À l'installation, WebRep va se positionner sur votre navigateur. Ici, vous pourrez donner une note au site de votre choix et avertir les autres utilisateurs sur son contenu (pornographie, warez ou blog et site marchand).

The screenshot shows the Avast! Antivirus interface with several callouts pointing to specific features:

- Top Left:** C'est la section qui permet de lancer un scan, d'examiner les rapports ou de paramétrer un scan au démarrage
- Top Middle:** Pour lancer un scan rapide en cas de suspicion de contamination
- Top Right:** Scan minutieux pour des résultats plus probants
- Far Right:** Permet de scanner les CD, DVD, clé USB ou tout autre support amovible
- Left Side:** Les réglages liés à la protection résidente
- Maintenance:** Maintenance : pour les mises à jours, la zone de quarantaine, etc.
- Bottom Left:** Scan sélectif : c'est vous qui choisissez les dossiers à examiner...

4 Étapes > Premiers pas avec Avast!

Étape 1 > L'interface

L'interface graphique est extrêmement simple. Vous devez avoir une icône Avast! sur le bureau ou une icône orange ronde dans le systray pour ouvrir le logiciel. Des rubriques avec des sous-menus sont disponibles à gauche et sur la droite, vous retrouvez les informations ou actions possibles.



Étape 2 > Mise à jour

La mise à jour est accessible par la rubrique **Maintenance**. Pour lancer la mise à jour, cliquez en haut sur le bouton **Mettre à jour le programme**.

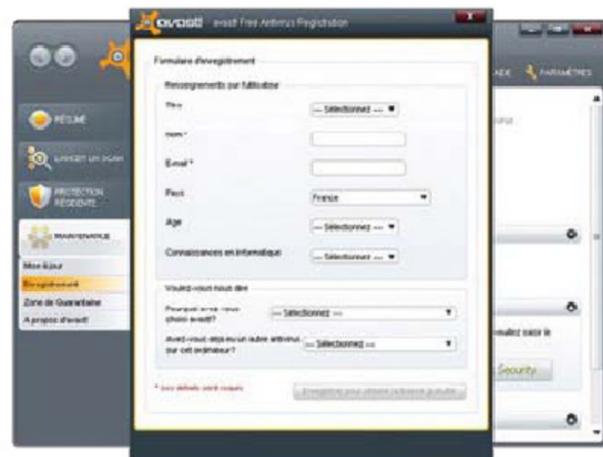


Ce ne sera nécessaire que lors de l'installation. Lorsqu'une menace est détectée, le logiciel affichera une fenêtre.



Étape 3 > L'enregistrement

Afin de pouvoir utiliser la version gratuite pendant un an, vous devez enregistrer Avast! auprès de l'éditeur. Toujours dans la rubrique **Maintenance**, faites **Enregistrement** puis **Enregistrez-vous maintenant**. Il vous suffira de remplir le formulaire et de l'envoyer pour obtenir une licence.



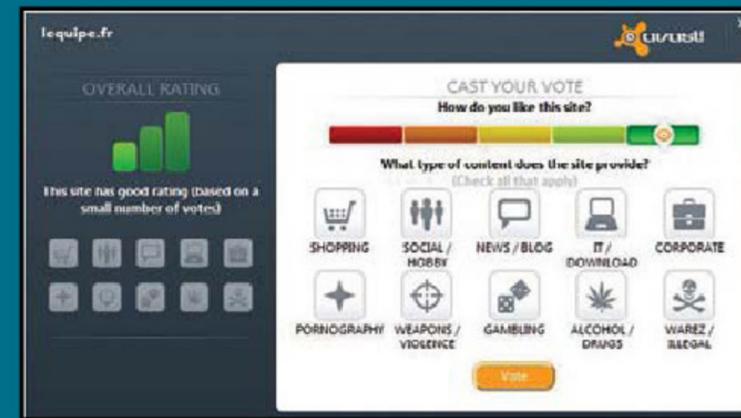
Étape 4 > Alerte !

Si une activité suspecte est détectée, vous pouvez alors choisir d'**Ignorer** ou de **Mettre en quarantaine**. Vous avez toujours le choix puisque certains faux positifs (des alertes qui ne sont pas dangereuses) sont toujours possibles. Les sites frauduleux seront bannis.

3 Étapes > Les nouvelles fonctions d'Avast! 6

Étape 1 > Web Réputation

Le programme va alors vous demander si vous souhaitez installer **WebReputation**. Validez pour que cette fonction s'installe aussi dans votre navigateur. La nouvelle icône doit être visible dans la barre d'outil de votre **Firefox** ou de votre **Internet Explorer**.



Étape 2 > Note et description

Lorsque vous êtes sur un site, cliquez sur cette icône et même si celui-ci a déjà une note, donnez votre avis ! Il est aussi possible de préciser le contenu du site. Dans **Google**, les sites avec une note **WebReputation** apparaissent avec une icône spéciale sur la page de recherche.

Étape 3 > Auto Sandbox

La fonction **AutoSandbox** permet de lancer un programme suspect dans une machine virtuelle pour vérifier son intégrité. Vous n'avez absolument rien à faire à part donner votre accord pour lancer la **Sandbox** le cas échéant.



SPYBOT – S&D, LE MODE D'EMPLOI

SPYBOT > LAVIS DE LA RÉDACTION

On aime :
- Léger et puissant
- La «vaccination»

On n'aime pas :
- L'interface moche qui n'a pas changé depuis 5 ans

www.safer-networking.org

GRATUIT



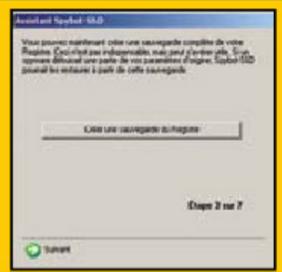
Impitoyable avec les espionciels ou spywares, Spybot requiert quand même quelques connaissances de base pour une utilisation efficace....

SPYWARES ET ADWARES

Comme un antivirus, Spybot fonctionne avec un système de signatures pour reconnaître les espionciels qu'il doit éliminer. Il faut donc faire une mise à jour avant chaque scan de votre système. En ce qui concerne la fréquence des analyses, vous pouvez vous en tenir à trois par mois ou après l'installation de logiciels que vous ne connaissez pas.

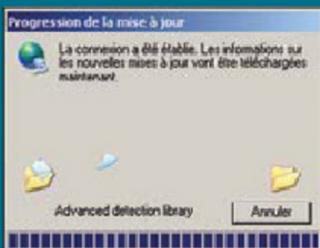
Étape 1 > Sauvegarde du registre

Pendant l'installation, le logiciel vous demande si vous voulez faire une sauvegarde de la base de registre. Il est conseillé de le faire, au cas où le logiciel ferait une mauvaise manœuvre pendant la désinstallation d'un spyware. Vous pourrez revenir à votre point de sauvegarde si l'ordinateur ne veut rien savoir (dans la partie Sauvegarde).



Étape 2 > La mise à jour

Spybot recherchera ensuite les mises à jour de la base de signatures et vous demandera si vous voulez les télécharger. Il est évidemment conseillé de le faire, pour être le plus exhaustif possible dans vos analyses.



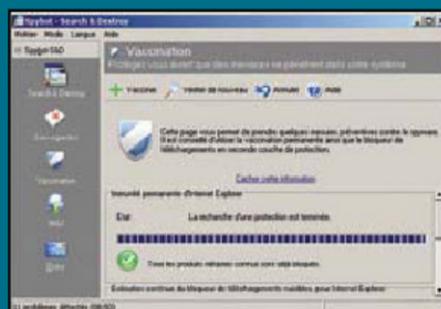
Étape 3 > Le scan

Passez ensuite à l'analyse en elle-même. Cliquez sur **Search & Destroy** et sur **Vérifier tout**. La recherche devrait prendre quelques minutes. Si vous êtes infecté par des spywares, les différents éléments seront visibles dans la fenêtre. Il vous suffira ensuite de faire un clic sur **Corriger les problèmes** pour que les espions soient neutralisés.



Étape 4 > La vaccination

Enfin, vaccinez votre ordinateur ! Cette mesure permettra de parer toute éventualité d'infection ultérieure. Allez dans la section adéquate et attendez que la recherche s'achève. Cliquez ensuite sur **Vacciner**, en haut. Pour plus de protection, vous pouvez aussi activer le bloqueur de téléchargements nuisibles, dans la même fenêtre...



MALWAREBYTES ANTI-MALWARE FAIT LE MÉNAGE

ROGUES ET ROOTKITS



Malwarebytes Anti-Malware (MAM) est le compagnon idéal si l'on est victime d'un rogue, ces faux-antivirus qui vous font croire à une contamination pour vous soutirer de l'argent...

On aime :
- Spécialisé dans l'élimination des rogues
On n'aime pas :
- Pas de protection résidente dans la version gratuite depuis 5 ans

www.malwarebytes.org

GRATUIT

MAM est un antimalware très puissant. Même si vous êtes déjà équipé d'Avast, il s'agit d'un très bon complément puisqu'il est spécialisé dans l'élimination des rogues et des rootkits. Ce logiciel est gratuit, mais malheureusement la protection résidente n'est disponible que dans la version payante (20 €). Qu'à cela ne tienne, vous pourrez vous débarrasser des rogues ou autres malwares en faisant un scan dès que vous aurez des signes de contamination.

Étape 1 > L'installation

Allez sur le site Web et cliquez sur **Download Free Version** puis sur **Download Location**. Installez le soft et cochez les cases de mise à jour et de lancement automatique.

Étape 2 > La recherche

Dans l'onglet principal **Recherche**, vous aurez le choix entre un examen rapide et un examen complet (la troisième option n'est disponible que dans la version payante). Si vous êtes sûr d'être contaminé par un rogue, optez pour le complet, faites **Recherchez** et choisissez les disques durs que vous voulez scanner. Selon la quantité de données que vous avez sur votre ordinateur, le scan peut s'avérer très long.

Étape 3 > Les résultats

À la fin du scan, cliquez sur **Afficher les résultats** si le logiciel a découvert quelque chose puis sur **Supprimer la sélection** pour corriger les problèmes. Un journal devrait s'ouvrir avec le détail des actions effectuées. La plupart du temps, le programme effacera les traces des malwares, mais il arrive cependant qu'il ne puisse les mettre qu'en quarantaine (voir l'onglet idoine).



Étape 4 > Les onglets

Si un fichier ne peut être effacé, soit parce qu'il est verrouillé ou utilisé en ce moment par le système, il faudra utiliser le module **File Assassin** (dans l'onglet **Autres outils**). En ce qui concerne les autres onglets, pas de surprise majeure. Allez dans **Mise à jour** pour updatier votre logiciel avant chaque utilisation, et faites un tour dans **Exclusion** en cas de faux négatif pour ne pas réexaminer un fichier inoffensif qui aurait été détecté comme une menace.



USURPATION

QUAND LES
VICTIMES
DEVIENNENT
COUPABLES

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

D'IDENTITÉ :

Un internaute français sur dix est victime d'usurpation d'identité

D'après une étude de YouGov commandé par Verisign (un spécialiste d'infrastructure réseau), 10 % des internautes français ont été victimes d'usurpation d'identité au cours des 12 derniers mois (1). Ce chiffre qui paraît énorme comprend en fait toutes les formes d'usurpation d'identité, y compris la fraude à la carte bancaire. Subtiliser l'identité d'une personne n'est pas si difficile que cela.

Il suffit de connaître un nom, une date de naissance, une adresse et le nom des parents de la victime. Grâce à ces premiers éléments et avec un peu d'habileté on peut retrouver d'autres informations comme le numéro de sécurité sociale. Les fraudeurs ne se privent pas pour fouiller vos poubelles ou voler dans votre boîte aux lettres à la recherche de RIB ou de toutes autres informations bancaires.

**ALLO ?
C'EST POUR UN SONDAGE**

Le faux sondage téléphonique est aussi un classique. Au début les questions sont d'ordre général puis plus les minutes passent et moins le «sondé» se méfie sur la nature personnelle des questions. Le but est parfois de se faire une «vraie fausse» carte d'identité et de collecter assez d'information pour obtenir un prêt bancaire, des prestations sociales ou pour éviter de payer des amendes. Avec Internet, c'est encore plus facile. C'est incroyable le nombre d'informations qu'il est possible d'obtenir grâce à un réseau social ou un blog. En plus de ces techniques, il faut ajouter le phishing (ou hameçonnage) qui consiste à faire croire à un email émanant de votre FAI ou d'une société que vous connaissez (banque, boutique en ligne, eBay, etc.) pour vous soutirer des



Chaque année, on recense en France 213 000 cas d'usurpation d'identité

renseignements. Chaque année, en France, on recense 213 000 cas d'usurpation d'identité, un chiffre énorme au regard du nombre de cambriolages (150 000) ou de vols d'automobile (130 000). En moyenne, la somme dérobée s'élève à 1 300 € et 25 % des victimes se plaignent de ne pas avoir été remboursées. Outre les trous dans le budget ou le traumatisme psychologique (le fait de devoir prouver «être soi-même» y est pour quelque chose !), les conséquences pour les victimes peuvent prendre des proportions désastreuses puisque 15 % d'entre elles ont été frappées d'interdiction bancaire et 13 % ont été assignées devant un tribunal.

QUID DE LA LOI ?

D'après l'article 434-23 du code pénal, le fait de prendre le nom d'un tiers, dans des circonstances frauduleuses et sans

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

Que faire en cas d'usurpation d'identité ?

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



Des pirates informatiques iraniens ont inventé un logiciel qui ne laisse aucune chance aux serveurs Internet. En quelques clics de souris, nous avons pu nous rendre compte que les données privées et sensibles sauvegardées sur les serveurs d'entreprises Françaises et étrangères étaient accessibles aux flibustiers du Web. Enquête !

PIRATAGE DE BASES DE DONNÉES :

Les nouvelles armes des hackers

Tout débute à la fin du mois de mai dernier. Un hacker français contacte la rédaction pour nous expliquer que certaines données de notre serveur Internet pouvaient être lues et copiées très simplement. «*Il me suffit de quelques clics de souris pour accéder à l'ensemble des adresses électroniques de la rédaction*» soulignait-il alors. Et effectivement, en quelques secondes, une base de données s'ouvrait à nos regards étonnés. Un tour de passe-passe digne d'un David Copperfield de l'informatique. Inquiétant ! Si notre hacker s'est donné pour mission de nous aider, nous allons découvrir que le business des bases de données sur Internet est devenu un gagne-pain fructueux pour des centaines de pirates informatiques. Des e-voleurs équipés de logiciels étonnants. De véritables passe-

partout électroniques à l'image du logiciel X'j3v (Le nom a été modifié pour ne pas permettre aux scripts kiddies de s'en donner à cœur joie, NDLR), un programme créé par des bidouilleurs iraniens.

PETIT OUTIL, GRANDS SECRETS

X'j3v ne paie pas de mine. Quelques boutons en anglais ; deux/trois onglets ; aucun mode d'emploi. Pourtant, derrière ces quelques bits, une arme redoutable qui devrait permettre aux responsables informatiques de réfléchir à deux fois sur la sécurité de leurs serveurs. Dans le cas de cet «outil», il en existerait plusieurs dizaines du même type sur la toile, il suffit de rentrer une adresse Internet trouvée via le moteur de recherche Google. «*Le plus terrible*, souligne François (un pseudonyme), un pirate informatique,

Il suffit de quelques mots clés dans Google pour établir le lien qui ouvrira les portes du site que je cible». Bilan de cette opération banale, le logiciel informatique se charge de trouver le point d'entrée à la base de données de n'importe quel site Internet. Opération que ce software effectue en moins de trois secondes. Vous avez bien lu, n'importe quel site Internet équipé d'une base de données est en danger. Lors de notre rencontre avec François, aux hasards de nos questions, l'intrus a été capable de nous présenter des serveurs faillibles appartenant à Orange, Paris Match, M6, mais aussi des sites gouvernementaux, des boutiques, des hôtels, ... «J'aurai pu effectuer une razzia sur leurs informations, en quelques minutes» s'amusait alors notre interlocuteur. Dans sa démonstration particulièrement inquiétante, des données bancaires se sont affichées dans certains cas ; des identifiants de connexion ; les messages internes. Bref, l'ensemble des petits et grands secrets inscrits et sauvegardés dans la moindre base de données. À noter que François nous a fourni les liens et les accès fautifs afin que les sites découverts lors de notre entretien soient alertés et corrigés. Du remords le jeune homme ? Peut-être ! En attendant, lors de sa démonstration, nous avons pu voir défiler devant nos yeux écarquillés des dizaines de mots de passe, non chiffrés ; des données bancaires sauvegardées dans des bases de données de boutiques en ligne.

UNE DEMANDE TRÈS FORTE POUR CE TYPE DE DONNÉES

Vicieux, l'outil décortique une par une les tables d'enregistrements sauvegardées dans les bases de données. En quelques secondes, selon les configurations des sites et serveurs Web, les identités, les adresses physiques, les courriels, les adresses IP, les

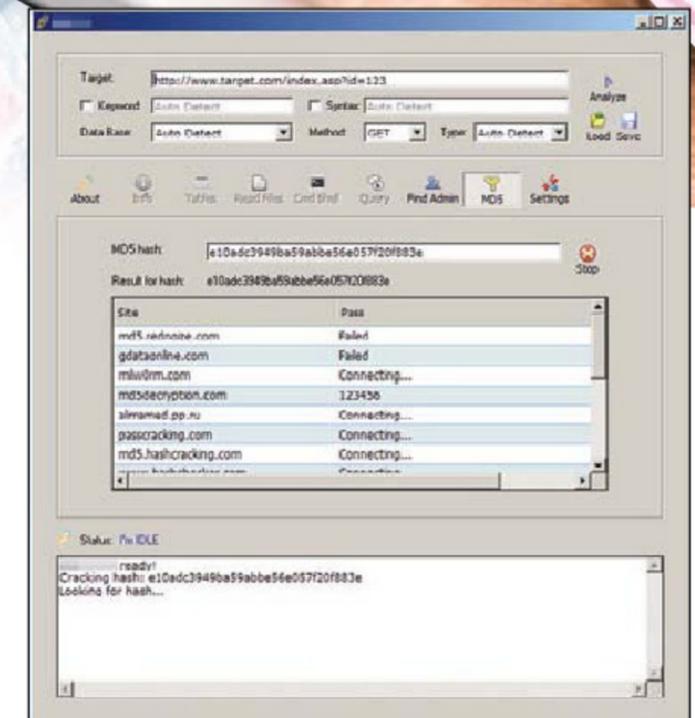
messages laissés par les employés et les visiteurs des sites concernés apparaissent. Dans le pire des cas, les commandes et les données bancaires sont consultables à souhait. «Aujourd'hui, souligne François, une base de données peut se revendre très chère. Si je mets la main sur des adresses électroniques, je les revends à des spammeurs. Si j'accède à des données bancaires. Il existe sur la Toile des espaces privés où il est possible de revendre, échanger, acheter ce type de prestations. Il m'est arrivé de toucher plus de 4 000 € par mois en revendant mes découvertes.»

UN MARCHÉ NOIR EN PLEINE EXPANSION

Les tarifs varient selon les «produits». Nous avons pu constater sur deux forums basés en Russie que les informations d'une carte bancaire (Les 16 chiffres, la date de validité et le CVV, le cryptogramme inscrit à l'arrière de la CB) pouvaient se revendre entre 5 et 30 euros pièce. «Le problème, souligne le pirate informatique, est qu'il y a de plus en plus de monde pour la revente de données piratées. Cela fait baisser les prix.» Comme le souligne Jérôme Granger, responsable de la communication de l'éditeur de solutions de sécurité informatique G DATA «Cette économie souterraine qui prend de l'ampleur. Le développement de l'économie souterraine au cours des dernières années s'illustre par le biais d'un exemple : Là où les pirates informatiques se vantaient autrefois d'arriver à obtenir via des données volées un accès gratuit à d'innombrables offres de pornographie sur Internet, ils se targuent aujourd'hui du nombre de cartes de crédit qu'ils ont déjà réussi à dérober. Fait remarquable : ces données se transforment à présent en espèces sonnantes et trébuchantes. Une tendance qui a fait naître une économie souterraine.



Aujourd'hui, tout ce qui existe déjà dans un vrai environnement économique légal : fabricants, commerçants, prestataires de services et clients se trouve dans l'économie des cyberdélinquants». Bref, le «black market» informatique a encore de beaux jours devant lui ! Pour rappel, tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physique (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de cinq ans d'emprisonnement et de 300 000 € d'amende (art. 226-17 du code pénal).



En quelques clics et avec un peu de chance, n'importe qui peut trouver quantité de données sensibles



WI-FI :

Les menaces et les protections

On vous le répète depuis longtemps : les connexions Wi-Fi sont de plus en plus fragiles et donc piratées. Même en rase campagne des intrus peuvent utiliser votre réseau et faire ce que bon leur semble. Au mieux, vous constatez un ralentissement de votre débit et au pire, HADOPI vous tombe dessus ! Voyons comment faire en sorte de se protéger un peu mieux...

Pirater un réseau Wi-Fi est un sport devenu à la portée de tous. Pour s'en convaincre, il suffit de faire une recherche sur Google. Entre les logiciels sous Windows et les Live CD embarquant des distributions Linux ciblées pour pirater spécifiquement ce type de réseau, il y a de quoi faire. BackTrack, par exemple, est une distribution Linux qui a pour objectif de fournir l'ensemble des outils nécessaires aux tests de sécurité d'un réseau. Le logiciel SpoonWep2, contenu dans les versions de BackTrack, permet de capter les flux Wi-Fi et de cracker «à la volée» la clé d'accès au réseau. Encore réservé aux hackers aguerris il y a quelque temps, ce savoir est en passe de rentrer chez «Monsieur tout le monde». Pour moins de 50 €, il existe des kits comme le WiFi-Box qui permet de «voler» la bande passante de n'importe qui ! On peut faire encore moins cher puisque n'importe quelle clé Wi-Fi compatible avec les modes injection de paquet (packet injection) et monitoring peut faire l'affaire. La Alfa AWUS036H permet de la faire pour environ 30 € ! Quand on sait que BackTrack est gratuit... Vous trouverez ici une liste de matériels compatibles : www.backtrack-linux.org/wiki/index.php/Wireless_Drivers



Traquer les méchants avec AirSnare et Wireshark

Pour ceux qui souhaiteraient s'amuser, nous vous invitons à installer les logiciels AirSnare pour détecter la présence d'intrus sur votre réseau et «sniffer» différentes informations sur eux avec Wireshark. Ce logiciel analyse les paquets d'informations circulant sur le réseau et en affiche les détails...



LE WEP PAR DÉFAUT, MAIS DÉPASSÉ !
Le problème vient de la fragilité des clés WEP (Wired Equivalent Privacy), censées fournir une sécurité équivalente aux câbles, malheureusement dépassées et pourtant encore utilisées sur de nombreux produits. Alors que de plus en plus de pirates amateurs s'essayaient avec succès au décryptage de clés

WEP, les fournisseurs d'accès comme les professionnels du secteur recommandent de passer à un cryptage supérieur, le WPA (pour Wi-Fi Protected Access) qui intègre une couche de chiffrement AES très réputé pour sa fiabilité. Attention, même avec une clé WPA, votre réseau Wi-Fi n'est pas à l'abri d'un hacker résolu, mais la plupart du temps, les «voleurs» de box iront vers la solution la plus facile. Si des réseaux

alentour sont plus faciles à pirater (et croyez-nous, ce sera le cas), ils préféreront toujours voir ailleurs. D'autant qu'un réseau «blindé» est souvent le fait d'une personne ayant des connaissances techniques et qu'il serait dangereux pour le contrevenant de se mettre à dos un utilisateur chevronné qui remontera jusqu'à lui le cas échéant. Voyons comment sécuriser un peu mieux votre connexion sans fil...

Des chercheurs trouvent la faille

Jusqu'à présent, la méthode utilisée pour casser les clés WPA consistait à tester toutes les combinaisons possibles. Cette technique longue et fastidieuse est aussi connue sous le nom de «force brute». C'est là que Erick et Martin innovent. Ils ont trouvé un moyen de décrypter ce type de clé en seulement 15 minutes. Leur méthode consiste à envoyer un maximum d'information au routeur le forçant à révéler des informations sur la clé de cryptage. Les chercheurs ont récemment présenté leur trouvaille au forum de PacSec au Japon, sous les regards médusés des plus grands spécialistes de la sécurité informatique.

4 Étapes > Blindez votre réseau Wi-Fi !

Attention, nous avons réalisé ce pas à pas avec notre Livebox. Il se peut que le vocabulaire change en fonction de votre FAI ou de votre matériel (routeur ou box), mais vous devriez vous y retrouver...

Étape 1 > Connexion à la box

Pour changer votre configuration, il faudra d'abord vous connecter à votre routeur ou votre box. Il faut pour cela rentrer l'URL suivante dans votre navigateur : http://192.168.1.1 Si cela ne fonctionne pas, renseignez-vous auprès de votre FAI l'adresse de votre box ? Si vous ne vous êtes jamais connecté à celle-ci, l'identifiant et le mot de passe devraient être admin pour les deux.



Étape 2 > Le mode de sécurité

Une fois identifié, repérez la ligne Wi-Fi ou Réseau sans fil puis cliquez dessus. Dans Mode de sécurité (ou équivalent) choisissez le WPA. S'il y a plusieurs choix, essayez le WPA2-PSK (AES). Attention, cette norme n'est pas compatible avec tous les matériels. Dans le doute, choisissez WPA2



(TKIP/AES). Choisissez ensuite votre clé de sécurité. Si vous n'avez jamais touché à cette clé, elle devrait être la même que celle collée au dos de votre box (grave erreur !). Pour être sûr de choisir une clé assez solide, aidez-vous du logiciel décrit dans l'encadré de la page précédente.

Étape 3 > Filtrage MAC et masque SSID

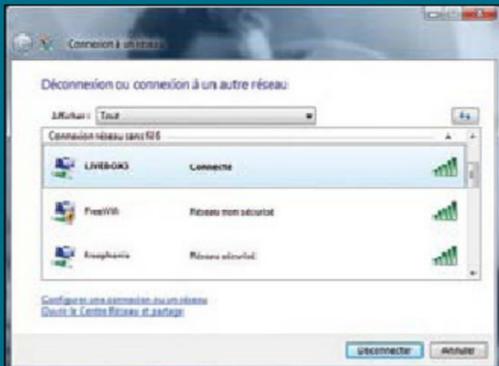
Avant de sortir de la page de configuration, vous pouvez aussi décider d'activer le filtrage des adresses MAC. Cette option consiste à interdire l'accès à des périphériques non autorisés. Cette option se trouve dans la même rubrique ou dans Paramètres avancés. Pour brouiller les pistes, vous pouvez aussi changer le SSID (le nom de votre réseau). De Livebox-65gt, vous pouvez passer à Ma Connexion, par exemple. Il est aussi possible de faire en sorte de ne pas diffuser son SSID. Le pirate débutant qui essaiera de scanner les SSID alentour ne verra rien (mais attention, un pirate équipé du logiciel Kismet sous Linux arrivera à tout voir !)



Configuration du filtrage par adresse MAC : Activer le filtrage par adresse MAC : [checked]. Equipements autorisés table with columns: Nom, Adresse IP, Adresse MAC, Statut, Supprimer.

Étape 4 > Reconnexion

Une fois que vous avez réalisé vos modifications, validez et notez votre nouvelle clé, car il faudra la rentrer dans Windows pour avoir accès à Internet. Faites un clic droit dans les deux petits écrans en bas à droite à côté de l'horloge et cliquez sur Connexion à un réseau. Attendez de voir votre box et rentrez votre clé toute neuve. Vous êtes connectés et bien mieux sécurisés !



Ils fabriquent de la DROGUE !

C'est bien connu, on trouve de tout sur Internet ! Avant que la police du Net apprenne à se servir d'un mulot, on trouvait même des sites qui proposaient toutes sortes de drogues en vente par correspondance. Mais maintenant que le réseau des réseaux est sous étroite surveillance, les cyberdealers sont de plus en plus rares. La nouvelle mode est aux sites de «recettes» : héroïne, Lsd, xodone, H, cocaïne, etc.

Les sites proposant des graines de cannabis et les moyens de cultiver de chez soi ne manquent pas sur la Toile. On en trouve même proposant le matériel adéquat pour commencer ce type de culture dans un simple placard. Évidemment puni par la loi, ce type de pratique n'a cependant jamais tué personne. Par contre, on trouve de plus en plus de sites qui proposent des protocoles très détaillés permettant de faire à la maison des drogues beaucoup plus puissantes. Notre confrère [Zataz.com](#) a dernièrement fait état d'un

site qui proposait des livres entiers sur le sujet pour un abonnement d'une vingtaine d'euros mais avec un peu de persévérance, nous avons trouvé des sites qui proposaient gratuitement de telles informations. Et les réseaux P2P ne sont pas en reste...

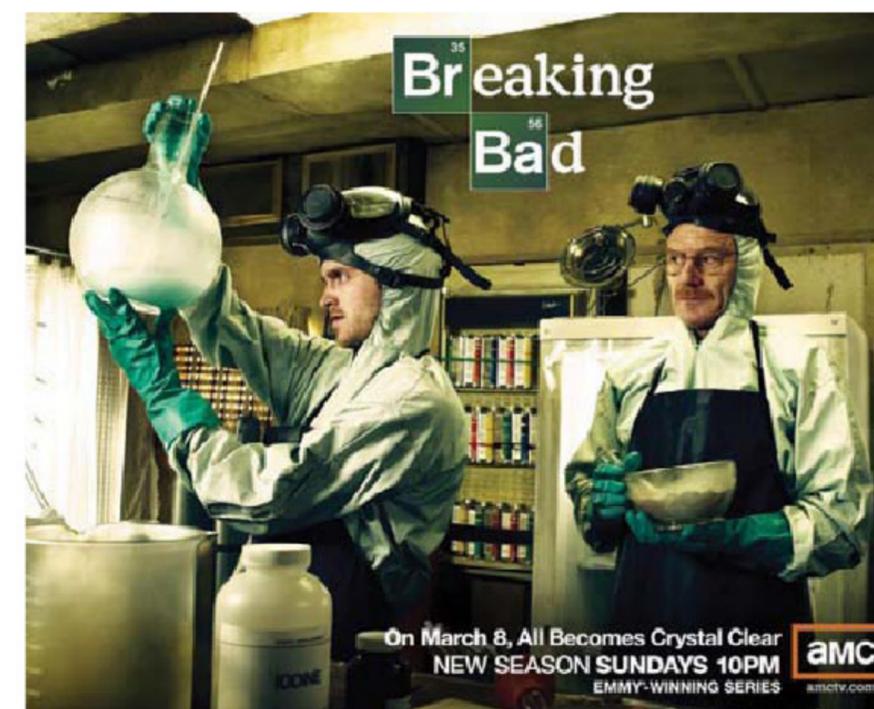
PAPA EST EN HAUT, IL FAIT DE L'HÉRO...

Attention, il n'est pas si facile de réaliser de telles drogues chez soi avec du matériel volé en cours de chimie. Mais comme les sommes en jeu sont considérables, l'investissement est payant. Pourtant, des apprentis chimistes commencent à se faire attraper par la police. L'année dernière, un jeune homme habitant Bourgoin-Jallieu a commandé sur Internet 900 g de feuille de coca et un litre d'huile de sassafras pour faire ses propres comprimés d'ecstasy. Il a expliqué à la police qu'il était simplement entré en contact avec un administrateur de forum qui lui avait expliqué comment réaliser sa «popote» et où trouver les «ingrédients». L'apprenti Escobar ne

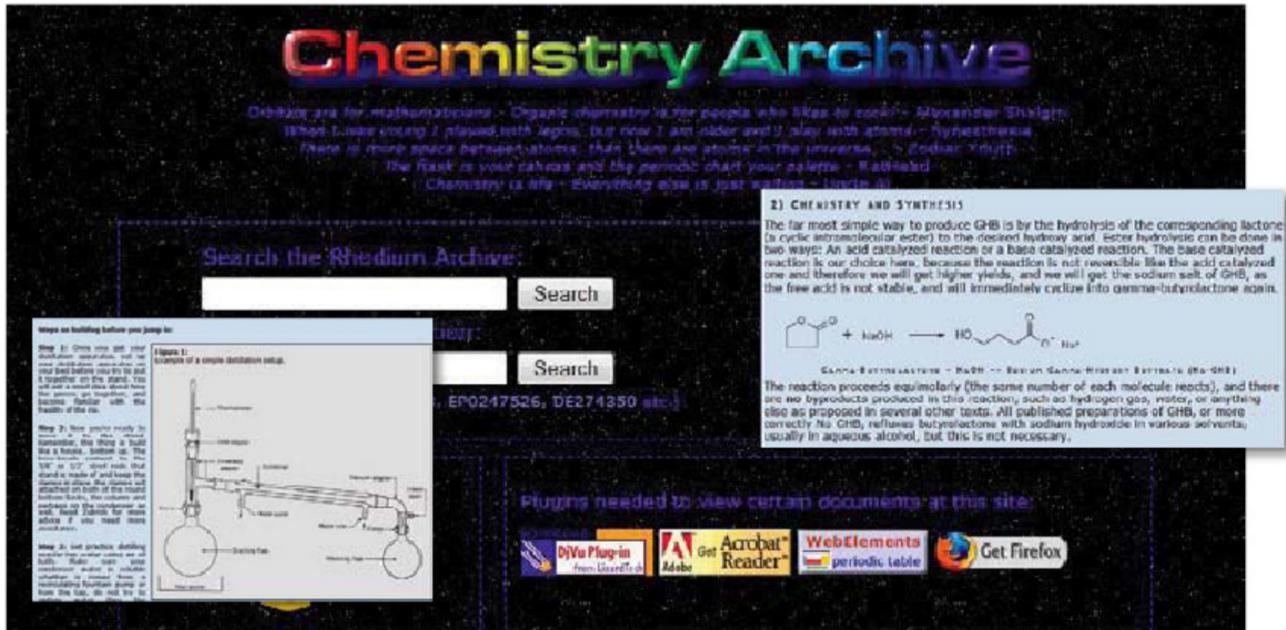
savait pas que l'huile de sassafras, à la fois utilisée dans la parfumerie mais aussi comme médicament est bien connu des services de police pour être un précurseur de l'ecstasy. Cette huile essentielle est d'ailleurs interdite en France depuis 2007 et son importation est étroitement surveillée. Lors de la perquisition les policiers ont découvert un véritable laboratoire... C'est d'ailleurs là tout le problème : l'appât du gain attire de plus en plus de gens vers ce genre dérive. Il faut pourtant savoir que la drogue de synthèse demande beaucoup de rigueur scientifique à produire. Comme

Quid de la loi ?

La production et/ou la fabrication illicites de stupéfiants sont un crime, passible de 20 ans de réclusion criminelle et d'une amende de 7 500 000 €. Cette peine pouvant être portée à 30 ans si les faits sont commis en bande organisée. De quoi refroidir les apprentis botanistes/chimistes.



Le phénomène est tellement «à la mode» qu'une série a vu le jour. Breaking Bad ou l'histoire d'un prof de chimie qui se met à fabriquer de la méthamphétamine pour subvenir aux besoins de sa famille



toute manipulation chimique, le danger est grand et les risques sont multiples : explosion, contamination par des produits volatils, mauvais dosage entraînant un empoisonnement ou la mort.

En cherchant un peu sur Internet ou Usenet, on trouve des ressources très précises sur la manière de fabriquer de la drogue. Ici un site pour «chimiste» qui donne des méthodologies pour réaliser MDMA, Meth, LSD ou GHB, «la drogue du violeur»

Les herbes type «Legal buds» bannies de France

On trouve aussi sur Internet des sites qui vendent des alternatives à la marijuana : les Legal Buds. Présentées comme des herbes à parfumer ou comme de l'encens, elles ont été récemment interdites par le Ministère de la Santé et des Sports français (et ne sont donc plus «Legal»). Sans THC (la substance active du cannabis), ces mélanges d'herbe censés contenir de la queue de lion (un proche parent du cannabis) ou de la salvia divinorum (appelé sauge des druides) contiennent des molécules chimiques comme la CP47 ou la CP497, des cannabinoïdes très puissants réalisés en laboratoire. Il y a encore peu de temps, il suffisait de commander ces «herbes» pour les recevoir chez soi dans des petits paquets flashy avec des noms exotiques : Gorilla, Gold Spirit, Green Viper, etc. Voici un petit reportage très intéressant sur ce sujet diffusé sur TF1 : www.wat.tv/video/droque-sur-internet-1ap6n_2flv7.html



NOUVEAU !

NOUVELLE FORMULE 100 PAGES ET PRIX MINI 3'90€ WINDOWS 7, VISTA ET XP 100% FICHES PRATIQUES

PC TRUCS & ASTUCES

JUILLET / SEPT 2011

WINDOWS INTERNET MULTIMÉDIA BUREAUTIQUE SÉCURITÉ MOBILES

LES MEILLEURS LOGICIELS ET SERVICES GRATUITS

DOPEZ VOTRE PC AVEC 100 FICHES PRATIQUES

+3 DOSSIERS COMPLETS

- GMAIL FACILE ! UTILISER GMAIL COMME UN PRO !
- OUTLOOK LES SECRETS DE LA MESSAGERIE N°1
- TWITTER 1,2,3... TWITTEZ !

✓ SIMPLE ✓ PRATIQUE ✓ EFFICACE

- AVEC UNE SIMPLE CLÉ USB ! INSTALLER WINDOWS 7
- ENVOYEZ DE GROS FICHIERS AVEC DROPBOX
- SÉCURISEZ VOTRE PC, DOSSIERS ET FICHIERS !
- UN VRAI GPS GRATUIT SUR MOBILE
- BEST OF : LES MEILLEURS SITES PRATIQUES !

Sous-titres faciles avec OS PLAYER !

L'avenir du numérique chez votre marchand de journaux

LE 1^{ER} MAGAZINE

100% ANDROID ET 100% PRATIQUE

NOUVEAU
SEULEMENT 2,95 € !

LE 1^{ER} MAG 100% ANDROID
ET 100% PRATIQUE !

E-MAILS
▶ Tout savoir sur Gmail
et la création d'autres
comptes mails

SÉCURITÉ
▶ Vol, Virus, Espions et
Surveillance : Comment
protéger son mobile

MOBILES & TABLETTES
ANDROID

JUN-AOÛT 2011

LE **GUIDE** DE
L'UTILISATEUR
Libérez la puissance
de votre mobile !

+ DE 60 FICHES
PAS À PAS
Vos smartphones et tablettes :
+ clairs, + faciles, + pratiques !

DOSSIER SPÉCIAL
L'INTERNET
FACILE SUR
MOBILE !

TEST COMPARATIF
▶ Mobiles et Tablettes :
LES NOUVEAUTÉS DE L'ÉTÉ

MULTIMÉDIA
▶ MUSIQUE
EN ILLIMITÉ
AVEC SPOTIFY

+ DE
80 APPS
POUR DOPER
SON MOBILE

2'95
€
SEULEMENT !

Chez votre marchand
de journaux

LES HACKTIVISTES

Selon les experts en sécurité, l'année 2010 a connu un nombre record d'attaques informatiques. Les Hacktivistes sortent de leurs terriers numériques et passent à l'action. Wikileaks fait fuiter des informations confidentielles et les Anonymous défendent la veuve et l'orphelin. Ces pirates dotés d'une conscience collective sont de véritables Robins des bois. Découvrez ces groupuscules secrets qui sont en train de changer la face du Web.

LES HACKTIVISTES PASSENT À L'ATTAQUE !

WIKILEAKS N'A PAS FERMÉ LE ROBINET !

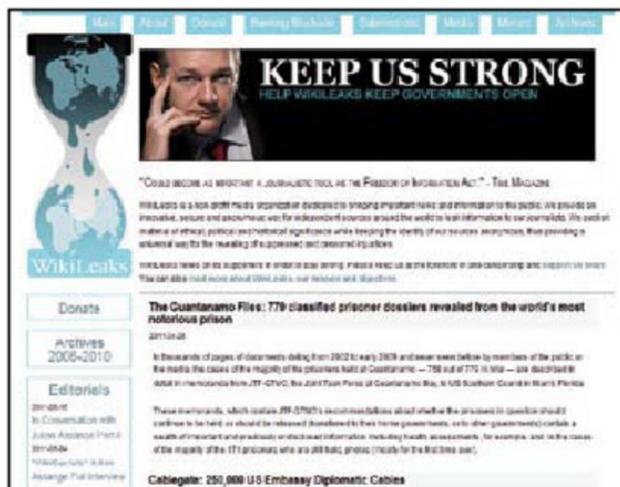
Si Julian Assange est l'homme de l'année 2010, c'est sans aucun doute grâce à Wikileaks, le site dont il est le porte-parole. La diffusion de plus de 250 000 documents secrets de la diplomatie américaine a mis en lumière ce site pourtant créé il y a 5 ans. Entre anonymat, mystère, complot et révélation, découvrez la face cachée de Wikileaks.

Angé ou démon ? Défenseur de la liberté d'expression ou dangereux irresponsable ? Robin des Bois de l'information ou sociopathe narcissique et opportuniste ? Qui est vraiment Julian Assange ? Cette question n'aura peut-être un jour plus de raison d'être tant sa «créature», Wikileaks, dépasse désormais sa simple personne. Même si le sulfureux Australien venait à disparaître, à être court-circuité ou à perdre le contrôle, le site le plus polémique de l'année 2010 lui survivrait. Enfin, «devrait» lui survivre. Car ils sont nombreux à vouloir mettre hors d'état de nuire son médiatique créateur et son outil de diffusion d'informations confidentielles ou secret-défense.

IRRESPONSABLE ?

Wikileaks est accusé de tous les maux et suscite la colère de nombreux gouvernements et organisations concernés par la publication de données confidentielles. Le mot qui revient le plus souvent est «irresponsable». On accuse le site d'être au mieux un outil moralement illégal, au pire un «tout-à-l'égout» sans scrupule qui manipule et opère une propagande principalement anti-américaine, mettant en danger personnes physiques et nombre de relations internationales. L'ambition affichée de Julian Assange est pourtant toute autre : son objectif à long terme serait que Wikileaks devienne «l'organe de renseignements le plus puissant au monde». Et à ce titre, à l'occasion du «Cablegate» qui alimente la chronique depuis l'année dernière, il a eu l'intelligence de très rapidement nouer des partenariats avec les médias occidentaux réputés les plus sérieux : The New York Times (USA), The Guardian (Royaume-Uni), Der Spiegel (Allemagne), El Pais (Espagne) et Le Monde (France). Ces grands journaux

Wikileaks tend à se positionner comme une simple agence de presse spécialisée dans la révélation de documents confidentiels.



WIKILEAKS EN DATES :

4 Octobre 2006 : John Young, co-fondateur de Wikileaks enregistre le nom de domaine Wikileaks.org.

2007 : Le cap du million de documents confidentiels répertoriés par le site est dépassé.

Avril 2009 : Wikileaks publie les détails du procès Dutroux, pourtant protégés par le secret de l'instruction.

Avril 2010 : On peut voir sur le site de Wikileaks une vidéo montrant deux journalistes de l'agence Reuters tués par un hélicoptère américain, c'est le début du succès pour le site.

Novembre 2010 : c'est le «Cablegate». Wikileaks diffuse plus de 250 000 documents de la diplomatie américaine. Le monde entier est dans l'embarras.

Novembre 2010 : dans la foulée, le site subit de nombreuses attaques de DDoS.

Décembre 2010 : Le compte Paypal de Wikileaks est suspendu.

16 Décembre 2010 : Accusé de viol par la justice suédoise, Julian Assange est placé en liberté conditionnelle et doit porter un bracelet électronique.

ont ainsi pu consulter en avant-première les quelque 250 000 télégrammes diplomatiques américains collectés par Wikileaks, c'est-à-dire de la correspondance échangée entre le département d'État à Washington et ses ambassades, pour l'essentiel entre 2004 et 2010.

CAUTION JOURNALISTIQUE

Wikileaks travaille donc désormais en amont avec des journalistes professionnels pour vérifier les sources et la véracité des documents tout en leur laissant le temps de contrôler, de filtrer et de préparer la nécessaire mise en contexte des informations collectées. Une démarche intelligente qui entend positionner Wikileaks comme une «simple» agence de presse spécialisée dans la révélation d'informations confidentielles. Aux journaux ensuite de valoriser ces documents de façon déontologique, responsable et éclairante pour le grand public. C'est le deal qui a été négocié avec les journaux sus cités. Mais il ne faut pas oublier que ce travail n'empêche pas Wikileaks de laisser à la disposition de tous, simples curieux, gouvernements ou personnes malintentionnées, l'ensemble des documents, sans aucun filtre. Pour Julian Assange, il s'agit d'éviter tout type de censure. Pour ses détracteurs, c'est là que réside la faiblesse du système. D'autant qu'il est quasi certain que Wikileaks se fera vraisemblablement intoxiquer et manipuler un jour par de fausses révélations aux conséquences peut-être dramatiques.

LE SAVIEZ-VOUS ?

La chaîne de télévision publique américaine PBS annonçait récemment que Tupac Shakur n'était pas mort. Or, ce rappeur des années 90 est bien mort en 1996. Ce sont les hackers de LulzSec (voir page 40) qui se sont amusés à pirater la chaîne en signe de représailles pour une émission sur Wikileaks qui n'était pas de leur goût.

Anonymous, des «Hacktivistes» anonymes



On entend parler d'Anonymous comme d'un groupe de hackers, mais la réalité est tout autre. Il s'agit en fait de plusieurs groupes d'activistes ne communiquant pas entre eux, mais se rejoignant dans leur volonté de rester anonyme et le combat qu'ils livrent pour préserver la liberté d'expression ou le droit à la vie privée.

Les actions d'Anonymous sont nombreuses et leurs buts très différents. Ce sont dernièrement le gouvernement iranien (pour le deuxième anniversaire de la réélection du président), le FMI (pour ne pas tendre la main à la Grèce), Sony (pour l'ensemble de son œuvre) ou l'ancien dictateur Ben Ali qui ont fait les frais de leurs actions. Le point commun de toutes ces «factions» d'Anonymous c'est leurs moyens de pression : les attaques DDoS.

DDoS ? KEZAKO ?

Un Distributed Denial of Service (ou « déni de service » en français) vise à saturer de requêtes des sites pour qu'ils ne soient plus en mesure de répondre. Le but est bien sûr de paralyser des organismes ou des organes gouvernementaux entiers. Au passage, Anonymous essaie de voler le maximum de documents, e-mail et compte pour les mettre en ligne et mettre dans l'embarras les sociétés ou pays visés. Cela a notamment été le cas pour Sony qui a non seulement vu

LE SAVIEZ-VOUS ?

Lors des manifestations physiques du groupe, les membres d'Anonymous sont masqués comme dans le film *V pour Vendetta*. Ce masque tire son origine du visage présumé du conspirationniste catholique Guy Fowkes. Ce dernier avait essayé de faire exploser le palais de Westminster où se trouvait le roi protestant Jacques Ier en 1605.



son réseau PSN mis sur la touche, mais aussi les mots de passe de ses participants publiés. Le but ici n'était pas de faire subir des préjudices aux joueurs, mais de leur envoyer un message pour faire comprendre à Sony que les «joueurs à travers le monde ont des droits et ne sont pas uniquement une source de revenus».

TOUTE UNE ORGANISATION !

Comment ces personnes s'organisent pour passer à l'action ? Par le biais de différents

LES ANONYMOUS EN DATES :

Novembre 2006 : La communauté Anonymous prend forme sur les forums de 4Chan.

2007 : Anonymous s'attaque à nouveau au site communautaire Habbo. Le Great Habbo Raid of 07 est la première action d'envergure des Anonymous.

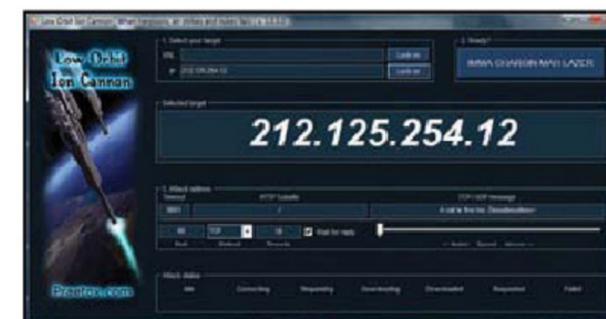
Janvier 2008 : Anonymous s'en prend aux scientologues avec le projet Chano-logy.

Mai 2009 : Le YouTube Porn Day voit de nombreux Anonymous envoyer des vidéos à caractère pornographique sur la plateforme YouTube.

2009 : Avec l'aide de The Pirate Bay et de pirates iraniens, les Anonymous forment un front de défense des libertés en Iran, en marge des élections.

2010 : En soutien à Julian Assange, un groupe se proclamant de la mouvance Anonymous a perpétré plusieurs attaques contre les sites Amazon, PayPal, Visa et Mastercard qui ont coupé les comptes et ressources financières de Wikileaks.

2011 : En donnant des moyens techniques aux contestataires du printemps arabes, les Anonymous ont participé à leur manière à ces premières révolutions 2.0.



LOIC est le logiciel préféré des Anonymous. Il permet de manière très simple de lancer des attaques de DDoS, même pour un débutant.

sites ou réseaux comme 4chan, Rockstararmy ou Usenet. Ce phénomène a connu un énorme succès et les internautes intéressés se passent le mot par le bouche-à-oreille. Car l'originalité de ces attaques DDoS réside dans son système de partage. Au lieu de s'en prendre à un serveur avec une seule machine ou une grosse quantité de PC «zombie», le groupe de hackers a préféré se bâtir une petite communauté de «soldats». Et pour que chacun puisse prendre part à l'attaque, Anonymous met à disposition un programme répondant au doux nom de LOIC (comme le « Low Orbit Ion Cannon » de *L'Empire contre-attaque*). Pour utiliser ce logiciel, pas la peine d'être un pro de la sécurité informatique ou un pirate aguerri, il suffit de rentrer une adresse IP et de cliquer sur un bouton à l'heure du «rendez-vous».

Ce type d'attaques étant difficilement évitables, les sites les subissant ne peuvent qu'attendre que l'orage passe. Il est très fréquent que le site ne soit pas disponible immédiatement après, les effets peuvent se prolonger pendant plusieurs heures. Les hackers en profitent alors pour accéder à des données sensibles qui ne sont plus protégées. C'est aujourd'hui l'arme principale des Anonymous. Ceux-ci veulent s'en servir contre quiconque porterait atteinte à la neutralité du Net. Cela s'appelle Hacktivisme !

LULZ SECURITY : 50 JOURS DE FOLIE !

En seulement 50 jours, entre le mois de mai et de juin 2011, un groupe de pirates a réussi à se faire une renommée mondiale. Lulz Security a attiré les regards du monde entier, décryptage de ce phénomène.

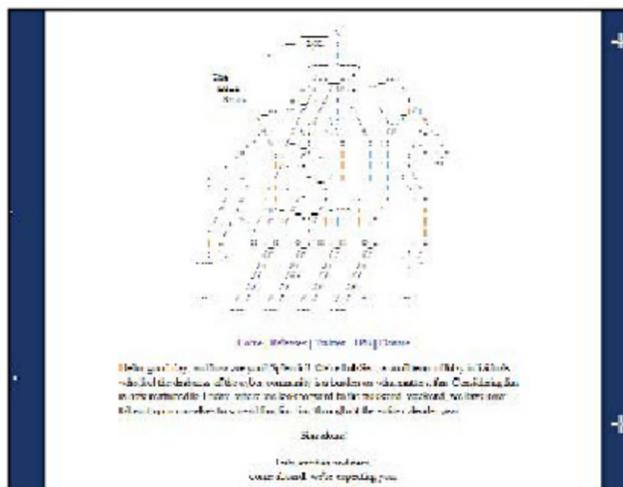
Impressionnant ! Comme le tableau de chasse des pirates du groupe indépendant LulzSec. Entre le 7 mai et le 26 juin, soit cinquante jours, les pirates se revendiquant du groupe Lulz Security ont multiplié les exploits et les attaques contre des cibles très diverses. Parmi les victimes de LulzSec, on compte tout de même Sony, Nintendo, le Sénat américain, la CIA, les gouvernements brésilien et anglais, Electronic Arts ou encore le FBI. Les motivations de ce groupe sont simples. Ils font ça pour le plaisir. « Lulz » en anglais est une déformation de « lol » au pluriel. D'ailleurs sur leur compte Twitter, qui retransmettait leurs aventures en temps réel, on pouvait lire ceci, « Si vous trouvez ça marrant de voir le chaos se développer, nous, on trouve ça marrant de le causer ». On est très loin de la philosophie hacktiviste

des Anonymous. Et pourtant, c'est au sein des Anonymous que LulzSec a vu le jour.

QUI SONT-ILS ? D'OÙ VIENNENT-ILS ?

Plusieurs théories, plus ou moins fumeuses, circulent sur la façon dont s'est formé LulzSec, mais nous ne sommes pas là pour relayer les rumeurs, ce qui est certain, c'est que quatre anciens membres des Anonymous se sont regroupés un jour, guidés par un désir commun d'ennuyer un maximum de personnes. Ces pirates étaient connus depuis longtemps, on ne rentre pas sur la scène pirate par hasard ou sur un exploit unique. Leurs pseudonymes vous diront d'ailleurs peut-être quelque chose, il s'agit de Topiary, le plus loquace, ainsi que de Tflow, Sabu et Kayla. Cette dernière, connue pour avoir 16 ans depuis au moins 6 ans, possède une force de frappe impressionnante avec une véritable armée personnelle de botnet (ordinateurs zombies), qu'elle mettait au service de Lulz. Ces quatre-là constituent le noyau dur de LulzSec.

Le site de Lulz Security est très basique, lorsque vous y pénétrez, la chanson de la série *La croisière s'amuse* se met en route, si vous cliquez sur le bouton pour l'éteindre, le niveau sonore augmente. Une blague de potache dans l'esprit du groupe de pirates.



LULZSEC EN DATES :

7 mai 2011 : LulzSec s'en prend à la base de données de l'émission américaine X-Factor.

23 mai 2011 : Attaque du site Sony Music au Japon

2 juin 2011 : LulzSec affirme avoir piraté 1 million de comptes de Sony Pictures Europe.

13 juin 2011 : Piratage du site du Sénat américain.

15 juin 2011 : Piratage du site de la CIA.

20 juin 2011 : LulzSec attaque et met hors ligne le site de la SOCA (Serious Organised Crime Agency), un site gouvernemental du Royaume-Uni.

22 juin 2011 : LulzSec fait des émules au Brésil, un groupe se revendiquant du mouvement LulzSec fait tomber le site présidentiel.

26 juin 2011 : Piratage de EA, plus de 550 000 comptes (identifiants et mots de passe) des joueurs de *BattleField* heroes sont exposés au public.

26 juin 2011 : LulzSec se retire de la scène et annonce une fusion partielle avec AntiSec.

UNE ASCENSION ÉCLAIR

Un grand débat a secoué la toile pendant les deux mois durant lesquels LulzSec a sévi. Il s'agissait de savoir si leurs membres étaient des génies ou simplement des « scripts kiddies » (des débutants qui ne font que profiter de failles connues et répandues). Quelle que soit la réponse, ils ont passionné la Toile pendant ces 50 jours. Leur compte Twitter a été suivi par plus de 250 000 personnes et leur site (rudimentaire) a connu des millions de connexions du monde entier. Nul doute que les pirates ont gonflé ces chiffres artificiellement à l'aide de botnets, mais leur visibilité a tout de même été exceptionnelle, en si peu de temps. Il y a plusieurs raisons à cela, la première est sans aucun doute la réputation de leurs victimes (dont la CIA, rien que ça). Ensuite, ils se sont appuyés sur une communication bien rodée. Les fuites (liste de données confidentielles, identifiants et mots de passe de compte personnels, etc.) ont toutes été diffusées librement sur la Toile grâce à des fichiers Torrent.

Mais après cinquante jours, au sommet de sa gloire, le groupe LulzSec a décidé de se dissoudre pour des raisons encore inconnues. Selon leur dernier communiqué de presse, certains membres vont rejoindre les Anonymous et notamment les AntiSec, un groupe qui lutte contre le lobby des fabricants de solutions de sécurité.

LE SAVIEZ-VOUS ?

Tout n'est pas toujours blanc ou noir. On connaissait les « white hats » (gentils pirates) et les « black hats » (méchants pirates), voici maintenant les « grey hats ». Ces pirates n'agissent pas pour nuire aux internautes, mais ils sont tout de même amenés à commettre des délits. Les AntiSec rentrent dans cette catégorie, ils prônent d'ailleurs le Full disclosure.

LA GALAXIE DES ANONYMOUS

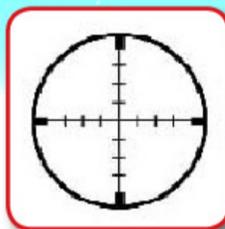
Les Anonymous ne possèdent pas de hiérarchie, leur organisation est plutôt anarchique. Derrière cette étiquette se trouve une multitude de groupuscules indépendants (AnonOps, AntiSec, Projet Chanology, etc.), anonymes ou revendiqués.



AVENGE
Assange



Manifestations

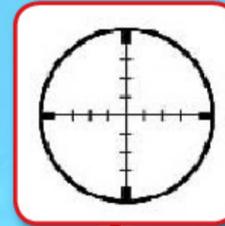


Attaques Ddos
Cibles : les sites de la Scientologie

LulSec



Attaques DDoS
Cibles : RIAA, IFPI, MPA



Attaque Habbo



Attaque Playstation Network



LOIC

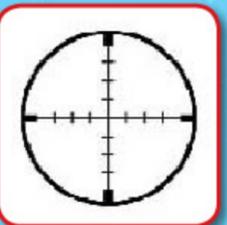
ANONYMOUS : LA "LÉGION"

OPÉRATION PAYBACK

ANONOPS

??

LOIC



Attaques DDoS
Cibles : les sites de Sony

PROJET CHANOLOGY



LOIC

ANONYMOUS IRAN



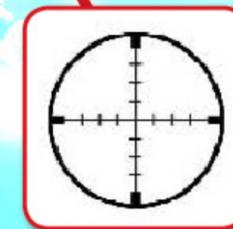
Manifestations

ANTISEC

LOIC



Piratage ImageShack



Opération Tunisie
Attaques DDoS
Cibles : les sites du gouvernement tunisien

LIBRE ET ENGAGÉ



CLICK LOAD
N°17 TÉLÉCHARGEMENT & STREAMING

Juillet/Août 2011
2€
90

THE END
FIASCO
CLAP
POUR HA

2€
90
PRIX CANON

FILMS, SÉRIES, MUSIQUE, JEUX
TÉLÉCHARGER

100% PRATIQUE & GRATUIT!

LES MEILLEURS SERVICES ET LOGICIELS
LES MEILLEURES SOURCES DU WEB

GUIDE MEGAUPLOAD
Mipony, la NOUVELLE BOMBE du Téléchargement Direct

NOUVEAU!
Le test de **GOOGLE MUSIC!**

BEST-OF
Le TOP des SERVICES VIDÉO ET MUSIQUE!

100% PRATIQUE

[Miro Converter] [Torrents & RSS] [Fetch.10]
[Torrent Turbo Search] [Foot gratuit en HD!]
[DropBox] [Grooveshark] [Mugen] [Etc!]

**VOTRE MAGAZINE
Nouvelle Génération**

Repères

WAREZ, CULTURE ET MAFIAS

NOTRE LEXIQUE DU WAREZ



Le Warez a ses codes et surtout, son vocabulaire. Pour mieux comprendre cet univers particulier, voici une liste (non exhaustive) de 40 termes expliqués et décortiqués.

• Oday :

Désigne les releases, cracks, appz ou exploit qui sont totalement nouveaux. Pour un hacker, une faille Oday signifie qu'elle n'a pas eu le temps d'être corrigée et qu'elle sera «sûre».

• Appz :

Terme désignant des applications piratées, vient de l'association entre «application» et «warez», il existe aussi «gamez», «isoz», «romz», «serialz», etc.

• Axx :

Définit les accès dans le monde de la scène

• Board :

Board est le mot anglais qui désigne un forum. Dans certains cas, il s'agit de sites de téléchargements qui sont sous forme de forum. À l'intérieur des catégories, on trouve des liens de téléchargement par Direct Download (MegaUpload, RapidShare, etc.), des fichiers Torrent ou des liens ed2k.

• BBS :

Les Bulletin Board System (littéralement «système de bulletins électroniques») sont (il en existe encore) des serveurs permettant des échanges de messages et de fichiers via un ou plusieurs modems reliés à des lignes téléphoniques. Populaires dans les années 1990, les BBS ont cédé la place à Internet.

● **Credit System :** il s'agit d'un système qui permet de déterminer qui a le droit de télécharger quelle quantité de données sur un topsite. Plus vous fournissez FTP et plus vous avez droit de télécharger de release. Attention vous pouvez perdre vos crédits en soumettant des nukes.

● **Flaming :**
Campagne de dénigrement contre une personne ou une team sur les réseaux.

● **Fake :**
C'est un fichier qui n'a rien à voir avec ce qui était annoncé. Il s'agit la plupart du temps des majors qui placent ces fichiers pour tromper les utilisateurs et les décourager.

● **Dupe :**
Une release est dite «dupe» quand elle a déjà été pré. Pour éviter le dupe, il est de coutume de pré un internal

● **DupeCheck :**
Site Web recensant les releases du jour distribuées par les teams

● **Dump :**
Stro privé, fiable, ayant un bon disque dur et une bonne bande passante. Il n'est jamais donné aux membres, il sert à stocker les releases afin de pouvoir les FR

● **DupeCheck :**
Site Web recensant les releases du jour distribuées par les teams

● **DRM :** Il s'agit d'un verrou numérique appliqué sur un fichier musical, vidéo ou un ebook qui restreint l'utilisation pour éviter le piratage.

● **Homebrew :**
Littéralement «brassé à la maison», il s'agit en fait d'un programme (la plupart du temps, des jeux) «fait à la maison» avec ou sans autorisation des ayants droit. Il existe par exemple de nombreux jeux homebrew sur Wii, Game Boy Advance, PSP, etc.

● **Offshore :**
un hébergeur offshore propose des solutions d'hébergement très laxiste concernant les lois sur la propriété intellectuelle. Hong Kong ou l'Ukraine proposent par exemple ce type de service et garantissent une tranquillité au webmaster de site de téléchargement.

● **Limited :**
Ce tag rare signifie que la release n'a eu qu'une diffusion restreinte dans les cinémas. Films d'art et essai, courts-métrages et autres raretés...

● **NFO :**
Il s'agit d'un fichier qui est inclus dans une release et qui permet d'en savoir plus sur le fichier, la team, etc.

● **iNT ou iINTERNAL :**
Release non publiée, à l'attention exclusive des membres de la team, cela peut être dû à plusieurs raisons : soit la team ne souhaite pas faire un « DUPE » (car plusieurs rips circulent déjà ...), soit le rip est de qualité médiocre et pour ne pas compromettre sa réputation, la team préfère ne pas le diffuser de manière publique

● **Leecher :**
Un utilisateur qui télécharge sans jamais proposer ses fichiers aux autres utilisateurs ou qui ne «seed» pas une fois son Torrent téléchargé.

● **Keygen :**
Mot-valise pour «key» et «generator». C'est un programme qui va générer une clé d'activation valide pour un logiciel donné. Généralement réalisé par un coder qui aura utilisé une technique de «reverse engineering».

● **Nuked :**
Une release ne respectant pas les standards. Local Nuked signifie qu'elle ne respecte pas les règles d'un site.

• **Pre :**
Action de releaser. Se dit aussi d'un PRE-RETAIL DVD, une pré série qui a les mêmes caractéristiques que le RETAIL

• **PROPER :** Il s'agit d'un tag qui est ajouté pour signifier que cette version est la meilleure à ce jour (ou qu'une précédente version a été corrigée).

• **Proxy :**
Ou «serveur mandataire» en français. C'est un serveur qui fait tampon entre un utilisateur et un réseau (le plus souvent Internet). Fréquemment utilisé pour passer inaperçu sur le Net ou pour éviter de voir son adresse écrite «en clair».

• **Racer :**
Les personnes qui amènent les releases sur les serveurs.

• **Release:** Cette expression d'origine anglaise définit une version d'un fichier (film, ebook, etc.) Il existe souvent plusieurs releases d'un même contenu réalisé par différentes team (différence dans l'encodage, la qualité, le poids, etc.)

• **RETAIL :** Il s'agit d'une release qui est issue du DVD final, celui qu'on achète dans le commerce.

• **Ring :** Désigne l'ensemble des membres d'un topsite

• **Rules :**
règlement d'un topsite

• **Scene:** Il s'agit de groupes de personnes (team) qui partagent du contenu soumis aux droits d'auteur (films, série, ebook, MP3, etc.) La plupart de ces groupes sont en compétitions les uns avec les autres et essayent de fournir en premier des contenus de qualité sur les «topsites».

• **Rip :** Procédé qui consiste à capturer le flux audio et vidéo des supports disque (DVD, Blu-ray). Une fois extrait le fichier «rippé», brut, est prêt à être encodé.

• **Screeener :** Il s'agit d'un DVD dédié à la promotion d'un film exploité en salle (ou sur le point de l'être) à l'attention des critiques, des journalistes ou des membres d'un jury. Très intéressant pour la Scene, ces DVD sont souvent à l'origine de fuites. À ne pas confondre avec un film enregistré avec une caméra dans une salle de cinéma (CAM)...

• **Serialz :**
Il s'agit d'un code d'activation pour un logiciel ou un jeu qui a été généré par un keygen ou qui a été volé.

• **Stro :**
Ou pubstro, FTP piraté, avec login et pass. On y stocke plusieurs releases

• **Siteop ou Sysop :**
C'est l'administrateur d'un topsite. Il dispose d'un accès sans limites contrairement aux visiteurs.

• **Topsite :** inaccessible pour le commun des mortels, il s'agit d'un serveur FTP privé où l'on trouve des releases à foison. Pour avoir le privilège d'avoir un accès, la personne devra montrer patte blanche et aider la team d'une manière ou d'une autre (accès à des DVD Screeener, encodage, etc.)

• **VPN :** Virtual Private Network ou réseau privé virtuel. Il s'agit d'une connexion sécurisée entre ordinateurs via Internet. Le but est de recréer en ligne le même fonctionnement qu'un réseau local. Chiffré, personne ne peut savoir ce qui passe par les postes des utilisateurs connectés.

• **Tag :**
Traduction littérale : Etiquette/Mot clé/ Marqueur. Utile pour l'archivage, donc la recherche par mots clé.
Exemple : Titre du Film.2011.FRENCH.DVDRiP.XViD-Nom-de-la-Team

• **Team :** Il s'agit d'une équipe qui inonde les réseaux de release. Souvent composé de plusieurs internautes ayant chacune une spécialité (encodage, traduction, incrustation, seed, etc.) Le nom de la team figure souvent à la fin du nom du fichier.

• **Warez :**
Ce terme désigne des contenus numériques protégés par copyright diffusés illégalement. De manière générale, la diffusion de contenus numériques affichant le terme warez a une connotation de pratique illégale.

PIRATAGE : Réseaux mafieux ou contre-culture ?

Qui alimente les réseaux P2P ou Direct Download ? Qui en tire profit ? Derrière le partage « grand public », il existe un deuxième type de réseau, plus efficace, plus rapide et plus opaque : la Scene.



La « Scene ». Elle se fait discrète, mais, sans elle, pas de P2P ou de téléchargement direct. C'est le premier maillon de la chaîne. Une grande partie des fichiers piratés apparaît d'abord ici avant d'être diffusée petit à petit sur les réseaux plus traditionnels. Le terme « Scene » ne renvoie pas à une structure bien organisée. Il s'agit plutôt d'un concept fourre-tout qui définit d'abord une communauté internationale réunissant des milliers de jeunes pirates partageant la même passion : réaliser puis partager les premières copies numériques des nouveaux films, albums ou jeux mis sur le marché. Ils sont les premiers à y accéder, les premiers à les numériser, les premiers à les partager. Un monde souvent fermé, réservé aux « initiés ». Neuf fois sur dix, les

internauts », voilà de quoi nourrir l'égo de jeunes qui se font souvent une très haute idée de qu'ils font. Mais en lieu et place de l'« élite » qu'ils aimeraient être, on se rend souvent compte en surfant sur les forums spécialisés qu'on y trouve une population très hétérogène et parfois décevante, au vocabulaire et à la culture souvent très médiocres. Skyblog et Warez, même combat... parfois.

L'une des motivations de ces teams est d'être reconnue, sinon appréciée par ses pairs. Quantité et diversité des « releases », exclusives : c'est une concurrence acharnée qui s'opère sur les réseaux. Avec le côté émulation qui profite à tous, mais aussi les petits coups bas, le parasitage, les insultes voire des dénonciations.

DANS LA COUR DES GRANDS

Mais l'esprit entre teams reste généralement bon enfant. On est alors en marge de la Scene véritable, entre réseaux très privés et grands publics. Au niveau au dessus, dans la « cour des grands », au cœur de la Scene, les motivations sont très différentes. Il y a les vrais apôtres d'une culture libre et gratuite pour tous et qui disposent d'un réseau haut de gamme. Ces pirates de films, de logiciels ou d'albums de musique ont des complicités, plus ou moins proches, au sein même de l'industrie audiovisuelle et des éditeurs pour obtenir des copies avant même les sorties officielles (copies de promotion, workprint, projections en avant-première, etc.). Mais certains sont aussi attirés par l'argent et le côté obscur de la force... Si une team met la main sur une release convoitée et véritablement exclusive (copie d'un blockbuster encore non sorti en salle par exemple), les plus cyniques seront tentés de vendre ce fichier au plus offrant. Et il y a

Une concurrence acharnée s'opère sur les réseaux

nouveautés (les « releases ») sont d'abord accessibles sur les forums et serveurs de la Scene, appelés « topsites », avant de se retrouver sur ces maudits réseaux peer-to-peer (ouverts au plus grand nombre et donc si... vulgaires !). Organisée en « teams », la Scene n'a pas, à l'origine, de mauvaises motivations : le partage, la notoriété et l'appartenance à un groupe.

UNE COMMUNAUTÉ DE « TEAMS »

Cela est d'autant plus vrai qu'il s'agit le plus souvent d'adolescents, biberonnés à l'informatique depuis leur plus jeune âge. Appartenir à une communauté « secrète », « illégale », inaccessible au « commun des

un marché ! Premièrement le marché noir d'Europe de l'Est, d'Asie et d'Amérique du Sud. D'où viennent à votre avis une partie des DVD vidéo, CD musique ou logiciels que vous trouvez dans les rues de nombreuses mégapoles ?

DÉRIVES MAFIEUSES

Il suffit de payer pour accéder à certains topsites mafieux et récupérer les dernières nouveautés. Bien sûr, il faut être un loup parmi les loups pour obtenir les bonnes adresses. Car pour accéder à ce genre de «TOP», il faut d'abord connaître l'adresse et l'IP de connexion. Cette dernière change toutes les trois semaines. Ensuite il faut y avoir été invité et pour cela il faut soit fournir du contenu, soit fournir un espace de stockage ou payer. Les tarifs varient de 20 à 80 dollars par mois.

Dernier point, et pas des moindres : il est impossible de surveiller les données qui transitent par ces serveurs. Tout ce petit monde se sécurise via le chiffrement des communications, en mode SSL, un

Il suffit de payer pour accéder à certains topsites mafieux et récupérer les dernières nouveautés

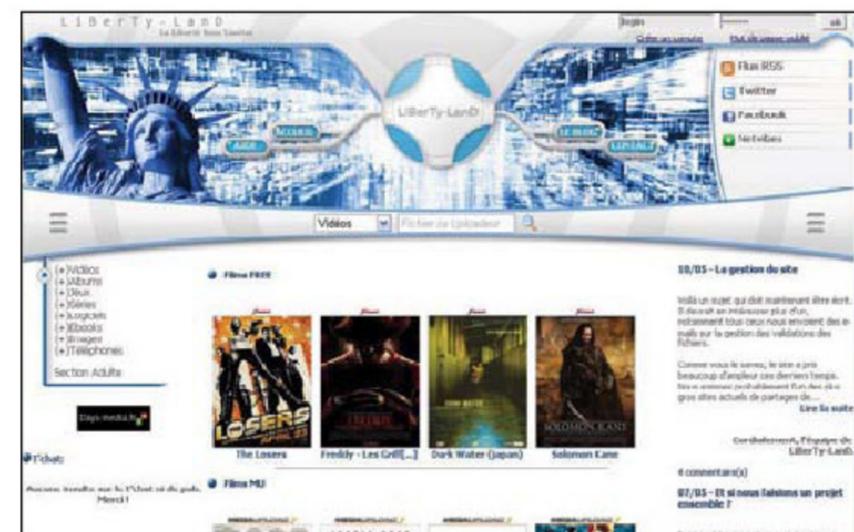
standard de cryptage inviolable. Autant dire que même si un «espion» se place au milieu de la ligne de communication, il ne pourra rien lire, rien comprendre.

ARRESTATION D'UN CAMCORDER

Les pros du warez ont depuis très longtemps compris ce qu'était la mondialisation. Pour preuve, le gros poisson péché, début mai 2011, par la police judiciaire de Bayonne. Le camcorder Serenity, un homme d'une quarantaine d'années, avait mis en place un réseau qui, selon certaines sources, lui rapportait beaucoup d'argent. Derrière Serenity, un autre internaute connu sous le sobriquet de Cedric et un tracker, le site xtrem-torrent, lancé sur la toile en février 2008. A noter qu'un compte VIP, sur ce site, coûtait 30 euros. Compte VIP qui permettait de télécharger les copies effectuées par le camcorder. Comme ce fût le cas pour la copie du film «rien à déclarer» de Dany Boon. D'après une source marocaine du site Zataz.com, le pirate revendait ses «news» à des trafiquants locaux de DVD comme Jake Casaoui (Casablanca), l'un des plus importants fournisseurs de DVD pirates du royaume. Ce dernier pouvait d'ailleurs récupérer les films volés par Serenity 24 heures avant la diffusion officielle sur les sites et trackers. «Comme d'habitude, souligne une source du site ZATAZ.COM, il n'y a pas de partage. Tout est du business». Il semble que Serenity travaillait aussi avec les Russes du site relizlab (relizlab.org) et les Américains du groupe Imagine (Arthur, Source code, ...



Certains sites de liens MegaUpload ou RapidShare, des trackers ou annuaires Torrent ou encore des sites de stream sont aussi de bons clients. Vous pensez que les administrateurs de ces sites mettent à disposition des centaines de contenus illégaux juste pour vos beaux yeux ? Vous rêvez ! Avec Google Adsens, les pop-ups, et les diverses autres sources de publicités, certains sites, sous couvert de culture, font énormément d'argent. Bien sûr, pour certains, une discrète bannière en haut du site permet de payer la location du serveur et le dépôt du nom de domaine, mais cela ne s'arrête pas là pour nombre d'entre eux.



L'EXEMPLE DE LIBERTY-LAND

L'exemple récent du site Liberty-Land, qui prônait la liberté et le partage pour tous, est assez saisissant. Les administrateurs se cachent derrière des VPN pour anonymiser leurs actions et les sommes récoltées étaient placées sur des comptes off-shore, sur une île basée dans le Pacifique. Liberty-land comptait 800.000 membres. Mais le 24 mai dernier, le site était fermé après l'arrestation de trois administrateurs du site par la gendarmerie de Rennes. Frédéric Delacroix, délégué général de l'Alpa, se réjouissait à l'époque de ces arrestations : « C'est une opération majeure. Liberty-Land.net était l'un des plus gros sites de Direct Download en France, avec plus de 51 000 films, 81 000 séries et 25 000 documentaires, de la musique... » Et selon les estimations, ce site aurait rapporté quelque 36000 euros de recettes publicitaires à ses créateurs chaque mois.

Mais le Warez est un monde impitoyable, sans pitié. «À côté», rigole notre contact, «Al Capone c'est de la blague». Dans le Warez, dès qu'un groupe prend un peu trop d'importance, donc égratigne le business des petits camarades, la délation va bon train.



LES COULISSES DE LA SCENE

Entrevue avec
l'administrateur d'un
Ring français

Nous sommes partis à la rencontre de «Jeje», un jeune sysop d'un Ring français, afin de mieux vous donner une idée de comment est structurée la Scene.

QU'EST-CE QU'UN RING ?

Un Ring est une communauté d'internautes, souvent restreinte, qui participent à la vie d'un ou de plusieurs serveurs de type Topsite où s'échangent des fichiers en avant-première. Ces derniers sont bien sûr illégaux pour leur quasi-totalité. La qualité d'un Ring se mesure à la quantité et à la diversité des fichiers stockés sur ses serveurs, aux vitesses de transfert, mais surtout à la qualité de ses membres. C'est notamment vrai pour ceux qui sont chargés de débusquer

et d'offrir en partage les nouveautés du moment : films sortis en salle ou en DVD ; vidéos théoriquement introuvables sur un marché donné (par exemple un film coréen non disponible en import et proposé avec un sous-titrage en Français) ; logiciels crackés, etc. Contrairement à un tracker BitTorrent ou à un site de téléchargement direct, chacun des membres doit participer activement à la vie du Topsite ce qui garantit la fiabilité, la réactivité et la qualité de la médiathèque.

Surtout, la concurrence entre Rings fait que c'est à l'intérieur de ces mini réseaux que l'on retrouvera les dernières nouveautés, bien avant leur publication sur les réseaux grand public de type P2P ou Direct Download. La plupart des Rings sont des communautés de passionnés, mais certaines ont un but exclusivement commercial : alimenter le marché noir ou les sites de téléchargements qui vivent de la pub. Ces sites ont donc besoin d'accéder

↳ Pouvez-vous vous présenter en quelques mots ?

Je me nomme Jeje, étudiant de mon état. Je suis administrateur d'une petite communauté ultra privée depuis maintenant deux ans. Cette communauté possède un petit Ring pour simplement profiter des news de la Scene.

↳ Quel a été votre parcours pour vous retrouver finalement sur la Scene ?

J'ai commencé par des boards publiques, ensuite des boards FTP privées. J'ai monté des dumps, fait pas mal de hacks et, finalement, j'ai créé ma propre communauté, d'abord avec un partage en FTP, puis on est passé en ultra privé avec une refonte totale du système de partage...

« Un certain filtrage est nécessaire. Sinon, on verrait arriver des personnes pour prendre le meilleur et repartir sans rien partager »

↳ Pourquoi n'importe qui ne peut-il pas entrer sur la Scene comme sur un tracker public ou une board ?

De nos jours, les gens veulent tout pour rien, et surtout que ça aille vite. Malheureusement, ils ne se rendent pas compte que derrière il

rapidement aux dernières nouveautés pour fidéliser leur audience et sont prêts à payer pour accéder à des Topsites mafieux : on perd l'aspect communautaire du « entre soi » pour dériver vers des rapports strictement commerciaux. C'est pourquoi les puristes considèrent qu'on ne peut plus parler de Ring dès lors qu'une partie des utilisateurs n'est là que pour récupérer des fichiers sans participer autrement qu'avec leur contribution financière.

Il y a énormément de travail, d'investissement personnel et surtout financier, car les serveurs ne sont pas gratuits. Donc je pense qu'un certain filtrage est nécessaire. Sinon, on verrait arriver des personnes pour prendre le meilleur et repartir sans rien partager ou, encore pire, mettre la pagaille sur les différents sites, Rings, dumps, communautés, etc.

↳ Dans quelles conditions peut-on alors intégrer la Scene ?

Cela dépend des siteops et de la place que l'on veut avoir. Le "petit riche" va payer les serveurs, mais en général nous n'avons pas besoin de ces gens-là : on préfère avoir peu de place (on parle en 'To' quand même) et ne pas dépendre de ce genre de personne. Ensuite, on peut devenir racer si on a déjà des axx Scene, afin de racer sur différents tops. Ou, sinon, il faut trouver une personne qui vous parraine et payer une cotisation, afin de télécharger tranquillement et de façon sécurisée.

↳ Quelle est la répartition des rôles au sein des différents topsites et Rings de la Scene ?

Il y a d'abord les sysops : ce sont eux qui gèrent le serveur (mises à jour, administration, etc.). Ensuite les racers, les personnes qui amènent les releases sur les serveurs. Les supplys, ceux qui payent pour avoir un axx sur les serveurs. Les nukers, les personnes qui vérifient les releases. Et les affils, les teams affiliées à un serveur



pour mettre en exclusivité leurs releases sur ce serveur.

↳ Quel est le protocole d'échange de fichiers utilisé ?

Le plus souvent, sur la Scene, c'est du FTP. Ensuite, certains vous diront les newsgroups, le http, le torrent. Mais le plus répandu, et surtout où les news arrivent en premier, ce sont sur les serveurs FTP.

Chaque team a ses sources et ne les dévoile pas, et c'est mieux ainsi

↳ Où sont hébergés les serveurs ?

Le plus souvent hors de France. Mais on ne va pas se voiler la face : si le master est hors d'Europe, rien n'empêche de mettre des slaves en France, surtout chez OVH, qui possède quand même pas mal de serveurs de la Scene française. En effet, sur un serveur hors Europe, le coup de la bande passante peut être élevé si le serveur possède une grosse bande passante et une communauté importante.

↳ Qu'est-ce qui différencie une team de Scene de n'importe quelle team œuvrant sur les réseaux P2P ?

Honnêtement, la qualité de la release. Mais après, certaines teams P2P sont très bonnes, elles n'ont juste pas axx à la Scene, ou alors n'en ont pas envie et

Les Rings sont de petites communautés ultras privées ou s'échangent les dernières releases du moment

préfèrent le P2P. Mais en majorité, sur la Scene, les règles sont respectées sous peine de Nuke, alors que sur le P2P il n'y a aucun contrôle.

↳ D'où proviennent les différentes sources utilisées par les teams pour rendre accessibles gratuitement jeux, films, séries, musique... ?

Ça dépend des releases. Chaque team a ses sources : cinéma, loueur de vidéo, personne connue dans les studios, magasin de vente, etc. Sinon, certains font la demande à une team pour prendre leurs releases et coller leurs sources. Par exemple, sur un dvdrip, on prend le son en cinéma français ou ailleurs, puis on prend la vidéo allemande ou celle d'un autre pays où cette vidéo est disponible. En règle générale, chaque team a ses sources et ne les dévoile pas, et c'est mieux ainsi.

↳ Pouvez-vous nous expliquer quel chemin parcourt un fichier sur la Scene ?

Un très long chemin... D'abord, il est «créé» par la team qui le release. Ensuite, il est mis sur le serveur privé pour être balancé sur les serveurs où ils sont affiliés. Puis des racers vont le récupérer sur ces serveurs pour le placer à leur tour sur d'autres serveurs, et ainsi de suite... En même pas dix minutes, la release est sur un bon paquet de serveurs. Enfin, des personnes la téléchargent, puis la reuploadent sur des newsgroups, trackers, boards, etc.

↳ Comment peut-on expliquer que la plupart des données qui sont censées être exclusives à la Scene se retrouvent sur les réseaux P2P, ou sur des marchés de pays émergents ?

Car des personnes qui ont des axx à la Scene revendent ces fichiers ou leurs prestations pour transférer ces fichiers vers des serveurs P2P. Ou encore des personnes qui sont sur la Scene s'inscrivent sur des forums publics et uploadent ces fichiers...



Les échanges de fichiers se font majoritairement par FTP

↳ Y a-t-il des «magouilles» comme la vente d'axx au sein de la Scene ?

De la vente d'axx, oui. Les supplys en sont le bon exemple. Après, si c'est pour payer les serveurs, ça passe. Si c'est pour se payer des soirées ou son loyer, non ! C'est sûr que certaines personnes doivent en faire un commerce, mais bon, c'est la dure réalité du monde dans lequel on vit...

↳ Existe-t-il des formes de «punition» pour les personnes ne respectant pas les règles ?

Oui, heureusement, les releases peuvent être nuked, la team peut se faire ban de la Scene, ou même des supplys...

↳ Auriez-vous un message final pour nos lecteurs ?

Arrêtez de courir après les news, elles arrivent tôt ou tard... Respectez les releases, ne les renommez pas, et surtout respectez la Scene, les serveurs, les staffs des serveurs, et respectez les règles mises en place par les siteops. Le téléchargement d'œuvres ne vous empêche pas de temps en temps d'acheter ce que vous aimez : un jeu, un dvd, c'est toujours mieux de l'avoir en collector !

INTERNET COUPÉ OU FILTRÉ :

LES MOYENS DE LA RÉSISTANCE

Imaginez que nous nous retrouvions avec un Internet coupé ou filtré. Qu'il s'agisse d'une coupure volontaire du gouvernement pour museler la *vox populi* ou d'une intervention d'un pays hostile, comment pourrions-nous communiquer ou nous défendre ?



Nous l'avons dernièrement vu en Tunisie, en Égypte ou en Libye, la coupure générale d'Internet dans un pays n'est pas de la science-fiction. Le régime de Hosni Moubarak a, en effet, utilisé cette «arme» pour éviter la fuite de vidéos ou la mise en place de réseaux organisés visant son gouvernement. Ici, la méthode avait été radicale : le blocage des protocoles BGP (Border Gateway Protocol) et DNS (Domain Name Server). Le premier permettant aux sites de signaler leurs adresses IP et le deuxième de savoir où joindre quel serveur. La Libye n'a pas agi de la même manière. Le gouvernement de Kadhafi a préféré ralentir la bande passante disponible pour avoir le loisir d'utiliser le réseau quand il le désirait. Pas besoin de jeter le bébé avec l'eau du bain...

Le RTC AU SECOURS DES INTERNAUTES ÉGYPTIENS

Alors, peut-on imaginer un scénario similaire en France ? Selon Benjamin Bayart de FDN (French Data Network, le

plus ancien FAI français), la structure du réseau égyptien est différente de celle de la France. Le nombre de FAI est limité alors qu'en France, «la structure du réseau français repose sur des milliers d'opérateurs ayant chacun plusieurs connexions à l'international. Pour couper Internet en France, un ministre devrait appeler quelques milliers de gens et beaucoup ne voudraient pas coopérer». Le FAI historique a même pensé, lors des événements, à un système permettant aux Égyptiens de se connecter au Web via la France grâce à leur structure bas débit. Pour un utilisateur, il suffisait de se connecter avec un modem RTC au numéro +33 1 72 89 01 50 (utilisé pour dépanner les clients français en panne d'ADSL). Le nom d'utilisateur et le mot de passe étaient «toto». Bien sûr, le coup de l'appel téléphonique était à la charge de l'utilisateur, mais le système fonctionnait. On peut donc imaginer que si une telle coupure arrivait en France, il faudrait que des pays «amis» fassent la démarche de nous aider.



Farouche opposant d'HADOPI, Benjamin Bayart est aussi un défenseur des logiciels libres

LE FILTRAGE, INTERNET EN SEMI-LIBERTÉ

Plus fourbe que la déconnexion pure et simple, le filtrage est à la mode dans tous les pays despotiques : Chine, Iran, Biélorussie, etc. Le but est d'interdire l'accès libre à l'information et d'épingler les fortes têtes qui iraient contre les idées du régime en place.

Même s'il s'est développé une méfiance du côté des citoyens (par exemple, les internautes chinois ne parlent jamais de la manifestation de la place Tien'anmen du 4 juin 1989, mais plutôt de l'événement du «35 mai»), de nombreux blogueurs ou webmasters sont emprisonnés ou tués dans le monde pour défendre leurs idées.

TOR ET LE «ROUTAGE EN OIGNON»

Pour éviter d'avoir la visite inopportune d'une quelconque police politique à la maison (bonjour !), il existe plusieurs solutions permettant aux plus modestes de se protéger. La première consiste à utiliser un VPN ou un réseau décentralisé de routeurs comme Tor (voir notre pas à pas). Comme les serveurs proxy ne permettent pas de protéger correctement les individus (le simple fait de s'y connecter



Le moteur de recherche numéro 1 en Chine est Baidu. Ce dernier ne permet pas d'accéder à tout le contenu que propose Internet.

rend immédiatement l'internaute suspect), ce type de logiciel «routage en oignon» sert à éviter que les autorités ne sachent qui échange quoi en faisant «rebondir» les paquets d'informations au sein d'Internet. Comme le tout est chiffré, même une attaque «man in the middle» (où un espion essaierait de recueillir des informations en s'installant dans le réseau) est inopérante. note au site de votre choix et avertir les autres utilisateurs sur son contenu (pornographie, warez ou blog et site marchand).

LES FREEDOMS BOX

Les Freedom box sont des mini-serveurs matériels à peine plus gros qu'un téléphone portable permettant à chaque utilisateur de gérer son propre réseau social, de contrôler l'accès et la diffusion de ses propres données tout en étant «étanches» aux organismes de surveillance. Alors que les grands réseaux sociaux s'articulent autour d'un noyau central, ces Freedom box permettraient de créer une multitude de mini-réseaux reliés les uns aux autres.



http://freedomboxfoundation.org

3 Étapes > Une navigation anonyme avec TOR



Étape 1 > L'installation

Après avoir téléchargé, lancez l'installation. Si vous utilisez Firefox, sélectionnez Torbutton et choisissez le dossier par défaut. Une fois que le processus d'installation est terminé, appuyez sur Suivant et enfin sur Terminer en laissant la case Démarrer les composants installés maintenant. Si votre connexion est protégée par un pare-feu, il vous faudra la configurer afin d'autoriser Tor et Privoxy à se connecter à Internet. Normalement un message de votre firewall devrait s'afficher et vous devrez confirmer l'exception.



On aime : - La simplicité - Un anonymat presque inviolable. On n'aime pas : - Un léger ralentissement de la connexion. www.torproject.org GRATUIT

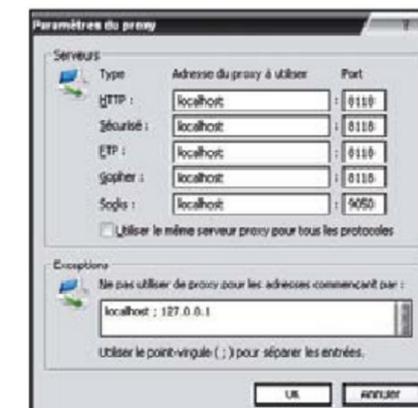
Étape 2 > La fenêtre principale

Dans le systray (les icônes à côté de la pendule Windows) deux icônes sont normalement apparues : une en forme d'oignon (Tor) et une ronde avec un P sur fond bleu (Privoxy). Double-cliquez sur l'icône Tor, une fenêtre s'ouvre contenant trois parties. En haut vous pouvez voir si Tor est actif et au milieu vous pourrez gérer les relais (ou «onion router»)



Étape 3 > Certaines options

Voir le réseau vous permet de voir par quels serveurs vous passez. Vous pouvez aller y faire un tour si vous êtes curieux. Utiliser une nouvelle identité sert tout simplement à faire croire que vous venez de vous connecter. Pratique si votre connexion est devenue trop lente. Graphe bande passante permet de suivre l'évolution de votre bande passante et Journal des messages enregistre tout ce qui se passe avec Tor, y compris les erreurs. N'allez dans les Paramètres que si vous êtes sûr de votre coup. Normalement, il n'y a rien à modifier ici.



LE MANIFESTE DU HACKER

Considéré comme le fondement de la culture «hacking», le Manifeste du Hacker (The Hacker Manifesto) a été écrit en 1986 par Loyd Blankenship peu de temps après son arrestation. Ce hacker ayant appartenu aux groupes Extasy Elite et Legion of Doom sous le pseudo de The Mentor explique dans son texte la frustration de certains élèves envers un système scolaire et la curiosité qui pousse les gamins à aller toujours plus loin dans le plaisir de manipuler la technologie. Âgé maintenant de 46 ans, il évolue toujours dans le monde de l'informatique...

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

La conscience d'un hacker

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

Saleté de gosses. Tous pareils.

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

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

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

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

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

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

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

Ou qu'il se sent menacé par moi...

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

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

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

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

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

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

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

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

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

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

LOGICIELS ET SERVICES INDISPENSABLES : NOTRE TOP 30



Anonymat

❖ Grabit

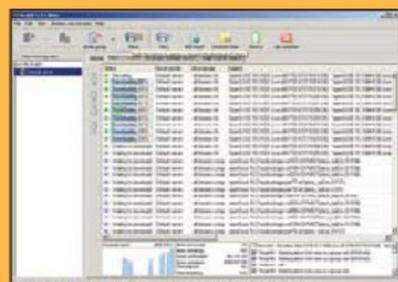
Un outil particulièrement efficace pour télécharger des fichiers binaires sur les newsgroups. On apprécie particulièrement la clarté de l'interface, l'absence de publicité et de spyware. Il suffit de récupérer la liste des forums, puis la liste des messages avant de faire son marché.

🌐 www.shemes.com

❖ StealthNet

StealthNet est un client pour Rshare, un réseau P2P anonyme et crypté. L'anonymat est basé sur un réseau décentralisé et chiffré. Lors d'une communication, les paquets sont routés entre différents nœuds avant d'arriver à destination, afin de brouiller les échanges.

🌐 www.stealthnet.de



❖ IPjetables

IPjetables est un service de tunnellation (VPN) qui permet d'emprunter une IP néerlandaise.

🌐 <http://ipjetable.net>

❖ Fetch.io

Un très bon service permettant de stocker vos fichiers dans le «cloud»...

🌐 <http://fetch.io>

❖ Kickass

Anonyme et sécurisé, ce service fusionne le P2P et le téléchargement direct.

🌐 www.kat.ph

Multimédia

❖ MediaCoder

MediaCoder est un logiciel permettant d'encoder tout et n'importe quel type de fichiers. Il est bien sûr fourni avec tous les codecs idoines. Un outil indispensable pour tout aficionado qui se respecte...

🌐 www.mediacoderhq.com

❖ Subtitle Workshop

Subtitle Workshop permet de créer, éditer ou convertir ce genre de sous-titres pour une vidéo donnée. Le logiciel supporte plus de 50 formats de sous-titrage différents !

🌐 <http://subtitle-workshop.softonic.fr>

❖ CDBurnerXP

CDBurnerXP est tout simplement le meilleur logiciel de gravure gratuit.

🌐 <http://cdburnerxp.se>

❖ Gspot

GSpot identifie avec précision un codec audio ou vidéo manquant.

🌐 www.headbands.com/gspot

❖ OpenSubtitles

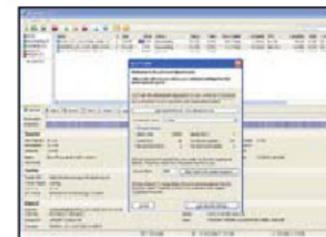
La meilleure source pour trouver vos sous-titres !

🌐 www.opensubtitles.org

P2P

❖ µTorrent

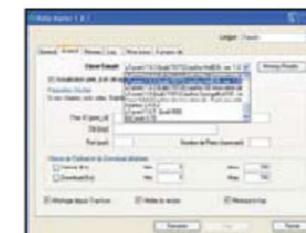
Chez µTorrent (prononcez «micro torrent») on mise avant tout sur l'efficacité et la simplicité. L'interface est minimaliste et idéal pour les débutants. Le logiciel est surtout ultra léger. Attention, ce n'est pas un poids plume pour autant !



🌐 www.utorrent.com

❖ RatioMaster

RatioMaster est une application qui permet de tromper les outils statistiques de la plupart des trackers privés en gonflant votre ratio upload/download et en vous ouvrant ainsi plus de privilèges sur ces sites (et qui vous évitera aussi de vous faire bannir).



🌐 <http://ratiomaster.net>

❖ LimeWire Pirate

La nouvelle version «boostée» du célèbre client P2P

🌐 www.limewire.com

❖ Opera

Un navigateur qui télécharge aussi sur le réseau BitTorrent !

🌐 www.opera.com

❖ Torrent 411

Le tracker privé à la mode qui monte, qui monte...

🌐 www.torrent411.com

WareZ/Hacking

❖ TrueCrypt

Nous avons tous sur nos ordinateurs des données «sensibles» sous différentes formes : images, films, musiques, mais aussi mots de passe, projets d'entreprise ou carnets d'adresses. TrueCrypt va vous permettre de crypter ces informations «à la volée» pour vous constituer un coffre-fort numérique

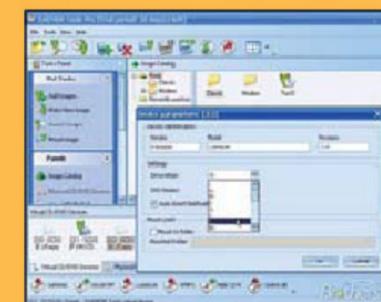
🌐 www.truecrypt.org



❖ Daemon Tools

Daemon Tools permet de créer des lecteurs de DVD virtuels. Le but de la manœuvre est de pouvoir lire les images de CD ou de DVD que vous téléchargez sur le Net ou que vous aurez créées avec votre logiciel de gravure. Le logiciel permet aussi de passer outre certaines protections anticopie.

🌐 www.daemon-tools.cc



❖ Recuva

Recuva permet de récupérer des fichiers perdus ou effacés par erreur.

🌐 www.recuva.fr

❖ AirSnare

AirSnare surveille votre réseau sans fil à la recherche d'ordinateurs non autorisés.

🌐 <http://airsnare.softonic.fr>

❖ Eraser

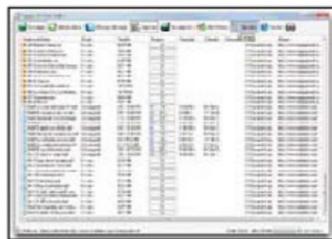
Le logiciel utilise l'algorithme de Guttmann pour être sûr de la destruction d'un fichier.

🌐 <http://eraser.heidi.ie>

Téléchargement Direct

❖ Mipony

Mipony est un gestionnaire de téléchargement direct. Au programme : un navigateur intégré pour tout faire dans la même interface,



la gestion des comptes Premium de plus d'une vingtaine de sites d'hébergement (MegaUpload, etc.), le contrôle à distance, etc.

🌐 www.mipony.net

❖ All Debrid

All Debrid permet d'outrepasser les limitations des sites de téléchargement direct. Près de 60 serveurs et autant de sites qui sont débridés, voilà ce que propose AllDebrid, qui n'a jamais aussi bien porté son nom !

🌐 www.alldebrid.fr



❖ LibertyLand

Le site LibertyLand est, sans conteste, la plus importante plateforme de liens de téléchargement direct.

🌐 www.libertyland.tv

❖ QuickPar

Grâce à QuickPar, vous pourrez rassembler des parties de fichiers que vous trouverez sur Usenet ou sur les sites de téléchargement direct.

🌐 www.quickpar.org.uk

❖ File & Image Uploader

File & Image Uploader permet de grouper vos uploads avec les sites de téléchargements directs

🌐 <http://z-o-o-m.eu>

FTP

❖ FireFTP Extension

FireFTP Extension permet d'ajouter des fonctionnalités de client FTP au navigateur Mozilla Firefox. Directement depuis votre navigateur, vous pouvez donc télécharger vos fichiers via FTP sans installer de logiciel particulier...

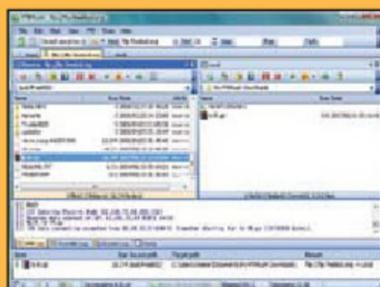
🌐 www.nightlight.ws



❖ FTP Rush

FTP Rush est un client FTP complet compatible avec les protocoles FTP, FXP, SFTP et TFTP. Il permet de télécharger rapidement des fichiers à partir du serveur FTP vers le local, du local à un serveur ou de serveur à serveur. Pour une meilleure sécurisation des échanges, cet utilitaire supporte les transferts en SSH

🌐 www.wftpserver.com/ftprush.htm



❖ FileZilla

FileZilla permet de se connecter à un serveur FTP et de paramétrer un serveur sur votre machine.

🌐 www.filezilla.fr

❖ Mon-ip.com

Vérifiez que vous avez bien une IP fixe pour paramétrer un serveur à la maison !

🌐 www.mon-ip.com

❖ DynDNS.com

Le site DynDNS propose de se confectionner une IP fixe

🌐 www.dyndns.com

UN MAGAZINE LIBRE & ENGAGÉ



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 : Click & 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 infractionnel 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°11 - AOÛT / OCTOBRE 2011

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

Ont collaboré à ce numéro :
Benoît Bailleur, Michael Couvret,
Damien Bancal, Stéphane Parisot

Secrétaire :
Karima Allal

Directeur artistique :
Sergueï Afanasjuk

Imprimé en France / Printed in France :

Léonce Deprez
ZI Le Moulin 62620 Ruitz

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 2109-2303

«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 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.



HostGator

we eat up the competition

Toll Free: **1.866.96.GATOR**

Local: **1.713.574.5287**

Now hosting over 5,000,000 domains!



LIVE CHAT

[HOME](#) | [WEB HOSTING](#) | [RESELLER HOSTING](#) | [VPS HOSTING](#) | [DEDICATED SERVERS](#) | [SUPPORT](#) | [AFFILIATES](#)

Unlimited Web Hosting

Web Hosting made **EASY** and **AFFORDABLE!**

- ✓ **UNLIMITED** Disk Space
- ✓ **UNLIMITED** Bandwidth
- ✓ **FREE** SiteBuilder ([Try Demo](#))
- ✓ **EASY** Control Panel ([Try Demo](#))
- ✓ **1-CLICK** Script Installs
- ✓ **4,500** Free Website Templates
- ✓ **99.9%** Uptime Guarantee
- ✓ **45** Day Money Back Guarantee
- ✓ **24/7/365** Technical Support
- ✓ **\$100** Google AdWords Credit

Now
20%
OFF!

STARTING AT
\$3.96*
/mo

[VIEW WEB HOSTING PLANS](#) ▶



Reseller Hosting

Make money with your own web hosting business!

STARTING AT
\$19.96* /mo



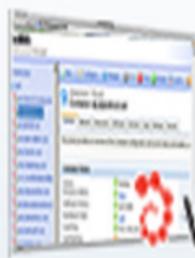
WHM

[VIEW RESELLER PLANS](#) ▶

VPS Hosting

Get dedicated functionality without the expense!

STARTING AT
\$15.96*
First Month



VIRTUOZZO

[VIEW VPS PLANS](#) ▶

Dedicated Servers

Feel the power and flexibility of a HostGator dedicated server!

STARTING AT
\$139*
First Month



[VIEW DEDICATED PLANS](#) ▶

**SUR NOTRE CD : BEST OF
LOGICIELS & SERVICES**

WEB INTERDIT 100% PRATIQUE

**P2P, TÉLÉCHARGEMENT DIRECT,
ANONYMAT, HACKING...**



BEL : 5 € ; DOM : 5,10 € ;
CAN : 7,95 \$ Can ; POL/S : 6,20 CFP

L 11970 - 11 - F: 3,90 € - RD

