+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 27

PIRATE [INFORMATIQUE]

0% PUB 0 CENSURE

GUIDE PRATIQUE! avec CD GRATUIT
> Les meilleurs logiciels avec PAS À PAS !

LE GUIDE DU PIRATE

HACKEZ-LES TOUS !

VPN Gratuit
Mot de passe
Web anonyme
Qbittorent
Confidentiel
Aurous
NirSoft
Décryptage

ANONYMAT • HACKING • SURVEILLANCE • MOBILE

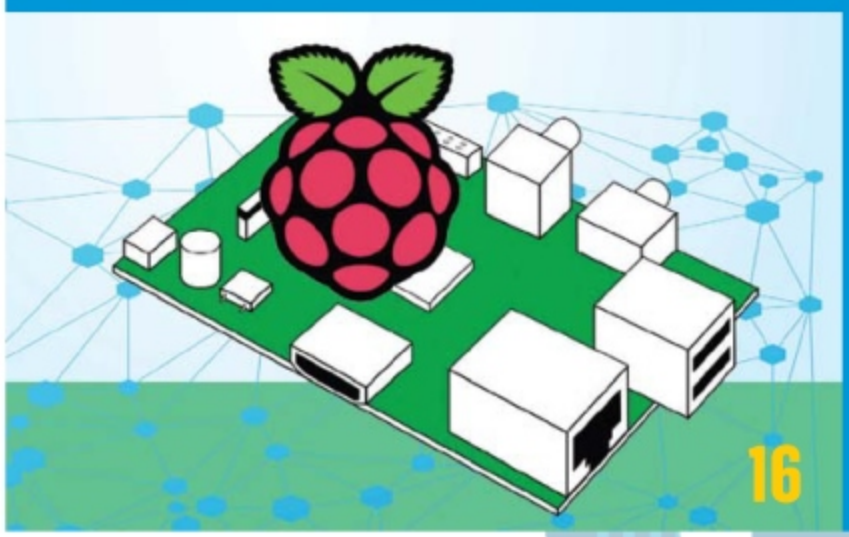
NOUVEAU
KALI LINUX 2
LA SUITE GRATUITE AUX 1001 CRACKS

SURVEILLANCE
DÉBARRASSEZ-VOUS DES MOUCHARDS DE WINDOWS 10

HACKING
CARTE BANCAIRES, MOBILES, BADGES : LES FAILLES DU NFC

SOMMAIRE

PROTECTION/ANONYMAT



HACKING

MULTIMÉDIA

46

CONCERNANT NOTRE CD

Certains lecteurs inquiets nous envoient régulièrement des e-mails concernant notre CD. Ce dernier serait selon eux rempli de virus en tout genre ! Il s'agit bien sûr de faux positifs. Les détections heuristiques des antivirus ne s'appuient pas sur les signatures de malware, mais sur les comportements des logiciels. Et il faut bien reconnaître que certains des logiciels que nous plaçons sur le CD ont des comportements semblables à des programmes malveillants. Bref, il n'y a pas de virus sur nos galettes. Ce serait dégoûtant non ?

LES CAHIERS DU HACKER
PIRATE [INFORMATIQUE]

N°26– Nov.2015/Jan.2016

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme
Seiya : Benoît BAILLEUL
Ikki : Yann Peyrot
Marine & Shiryû :
Stéphanie Compain & Sergueï Afanasiuk
Shaina : Virginie Bouillon

Imprimé en France par / Printed in France by :
Léonce Deprez
ZI Le Moulin 62620 Ruitz

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS : Marseille 491 497 665
Capital social : 2000,00 €
Parution : 4 numéros par an.

ÉDITO

Ah, vous vouliez plus d'articles sur Linux ? Et bien, nous vous avons écouté puisque dans ce numéro vous trouverez la présentation de la dernière version de Kali ainsi qu'un papier sur la mise en place d'un VPN «maison» en utilisant Raspbian, une version de Debian pour Raspberry Pi. Bien sûr, nos utilisateurs «Windowsiens» n'ont pas été oubliés avec la dernière partie de notre série d'articles sur les protections du format PDF et un tutoriel complet pour éradiquer les mouchards de Windows 10. Dans la rubrique X-Matériels nous avons testé le YubiKey, un sacré gadget assurant une sécurité optimale lors des authentifications et nous verrons aussi comment supprimer la peu sûre technologie NFC de nos cartes bancaires (délicatement... à la perceuse !)

Comme à chaque fois, vous retrouverez sur notre CD tous les logiciels dont nous parlons dans le magazine ainsi que certains anciens articles qui vous aideront à mieux comprendre nos démonstrations. Enfin, nous vous invitons à vous rendre à la page 21 pour vous abonner gratuitement à la mailing-list de magazine et être tenu au courant des parutions.

N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur **benbailleul@idpresse.com**

Bonne lecture !

Benoît BAILLEUL.

HACKTUALITÉS

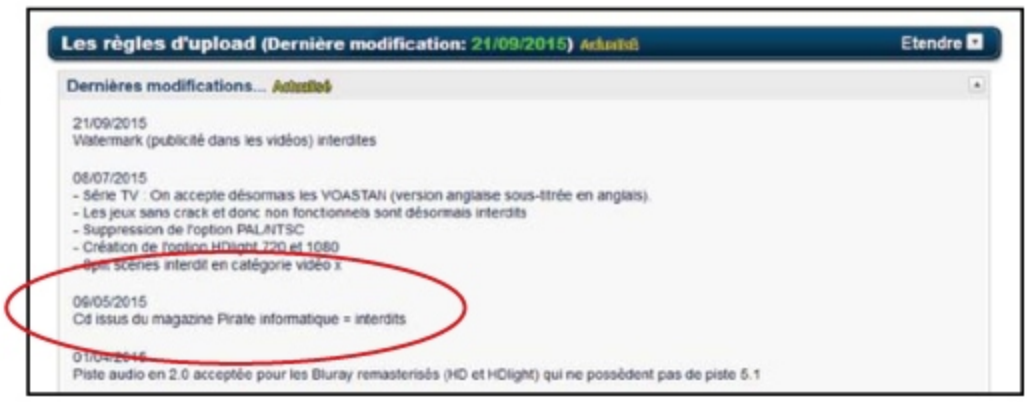
LAVABOOM
C'EST DÉJÀ TERMINÉ !

C'est l'hécatombe du côté des webmails chiffrés ! Après Lavabit c'est au tour de Lavaboom de fermer ses portes après seulement un an de fonctionnement. C'est d'autant plus dommage que nous vous avions recommandé ce service dans le dernier numéro de *Pirate Informatique*. Le directeur général du site Félix Müller-Irion a jeté l'éponge peu de temps après la parution de notre article. Il semble en effet qu'une enquête est en cours en Allemagne (pays de résidence du service) concernant certains utilisateurs impliqués dans une affaire criminelle. Les investisseurs ont alors botté en touche ce qui a contraint Félix a déposé le bilan. Les utilisateurs ont eu une semaine pour transférer leurs données vers d'autres webmails chiffrés comme Tutanota (voir *Pirate Informatique* n°23). Que c'est compliqué la protection de la vie privée sur Internet...

"Nous avons le regret d'annoncer à tous nos utilisateurs que Lavaboom a fermé ses services le 27 août. [...] Je suis désolé de vous laisser tomber"

Nos CD bannis de T411 !

Si vous nous lisez depuis longtemps, vous connaissez sans doute le tracker semi-privé T411. Ou peut-être est-ce l'inverse puisque de nombreux lecteurs connaissent le magazine pour l'avoir piraté en premier lieu sur ce site. Nous encourageons le partage et remercions régulièrement les personnes qui prennent le temps de poster nos publications sur T411, car comme nous le disons souvent : «*Si 1 téléchargeur sur 10 achète parfois le magazine sous sa forme papier, nous serons tous gagnants*». Nous avons donc été surpris de voir dans la FAQ (**Les règles d'upload** > **Dernières modifications**) que nos CD sont... bannis du site ! Dans les commentaires, les spéculations vont bon train : est-ce parce que nous sélectionnions parfois le logiciel RatioMaster (qui permet de bidouiller son ratio sous certaines conditions) ou est-ce à cause des nombreux logiciels qui affolent, à tort, les antivirus ? Le mystère reste entier, mais cette mise à l'écart est savoureuse : *Pirate* est trop «pirate» pour nos amis les pirates...



Lien : www.t411.in/faq

LE CHIFFRE

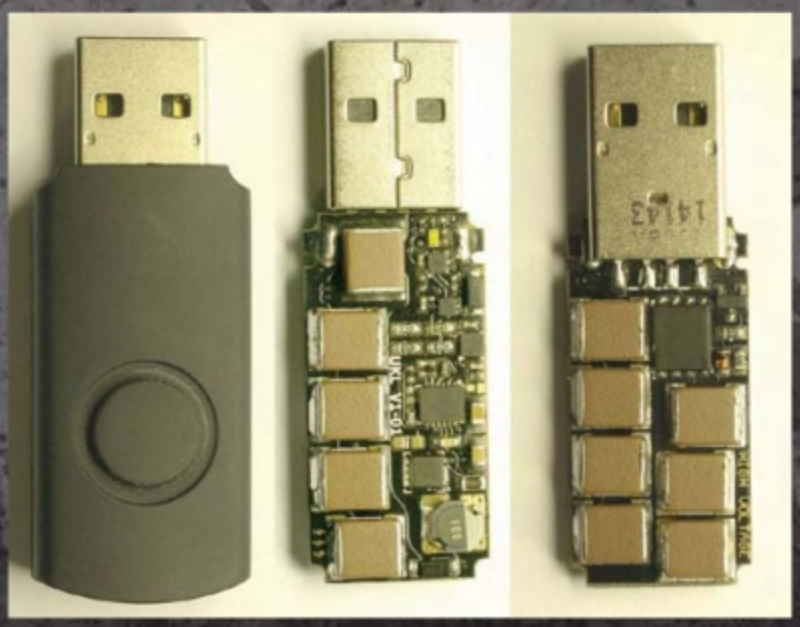
27 MILLIONS

C'est la somme totale en euros qui a été dérobée sur plusieurs comptes bancaires au Royaume-Uni. Les malfrats, sans doute des hackers d'Europe de l'Est utilisent un trojan baptisé Dridex (ou Bugat, Cridex et Feodo selon les versions). Ce dernier s'attrape tout simplement en cliquant sur un lien malicieux. Une fois sur la machine hôte, ce malware va récupérer les informations de connexion bancaire avec des keyloggers et des modules de captures d'écran sophistiqués. Le FBI et la NCA britannique travaillent main dans la main avec Europol et les autorités allemandes et moldaves pour mettre la main sur les brigands. Pour se protéger, mettez à jour votre antivirus, ne cliquez pas sur des liens louches, ne téléchargez pas de pièces jointes suspectes et en cas de doute, changez le mot de passe de votre site bancaire après avoir fait une analyse complète de votre système. La France est peu concernée (2% des attaques), mais la prudence est de mise...

Jamais votre banque ne vous enverra un e-mail pour vous demander de confirmer votre identité. N'ouvrez ces liens sous aucun prétexte et en cas de doute, appelez votre banquier !

USB KILLER : BARBECUE SUR CLAVIER !

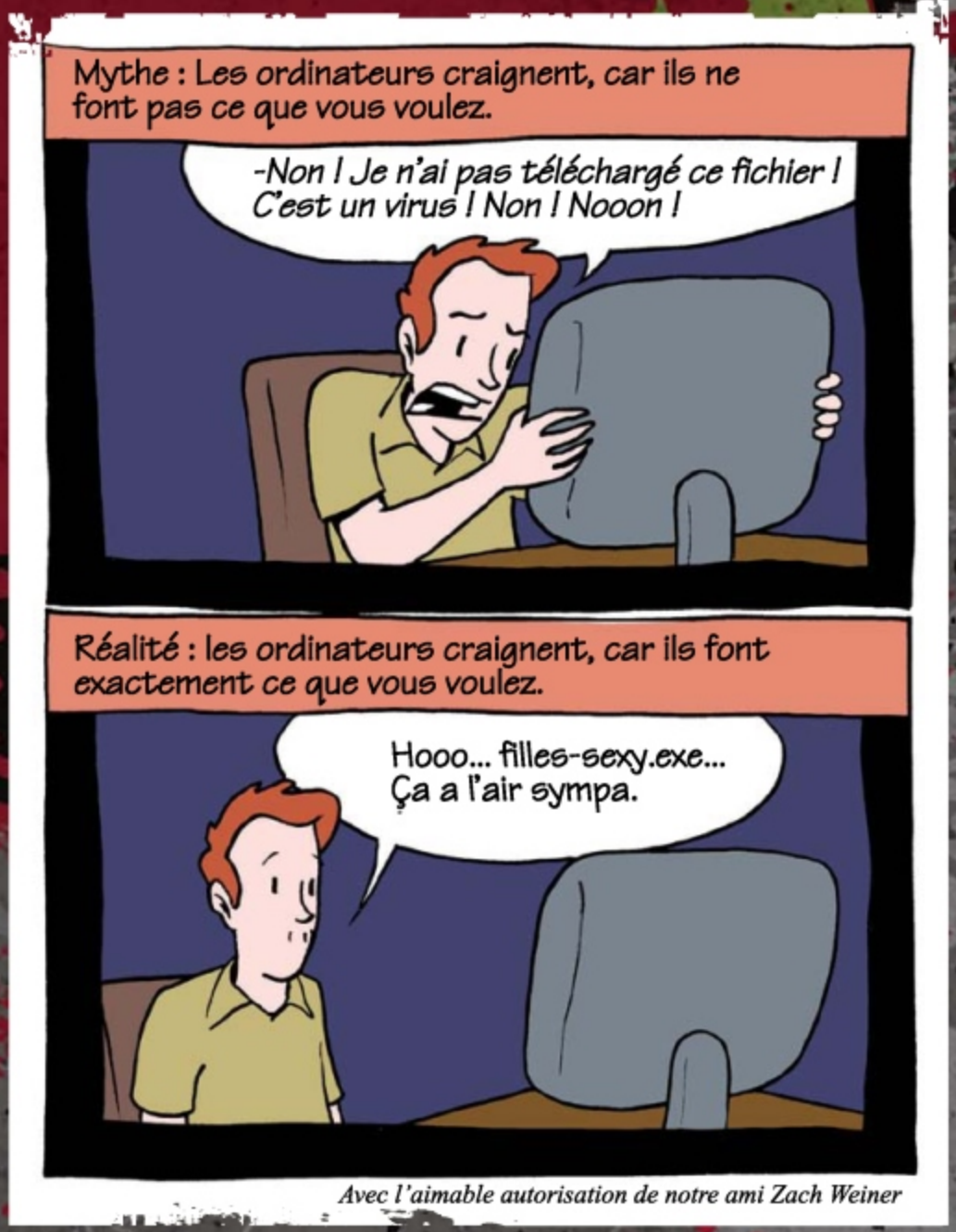
Vous savez sans doute que les clés USB sont une des causes principales de contamination entre ordinateurs. Et bien, il faudra encore redoubler de vigilance à cause des USB Killer. Ces clés particulières, qu'il est possible de trouver sur le Net pour quelques dizaines d'euros, sont en fait de redoutables appareils qui peuvent détruire les composants électroniques du système hôte. En relâchant une tension stockée sur un condensateur, elles détruisent carte mère, carte graphique, etc. Sur une télévision, un téléphone ou un média center le résultat sera la même. Encore une raison supplémentaire de faire attention à ce que vous branchez sur votre matériel...



SCOOP : WINDOWS DEFENDER n'est pas un antivirus (mais alors pas du tout !)

Nous avions des doutes, mais nous avons fait le test pour être bien sûr... Depuis le passage à Windows 10, nous avons décidé de faire tourner un des PC de test uniquement avec Windows Defender. Avec un pare-feu correctement configuré, mais sans antivirus tiers. Après moins d'une semaine d'utilisation et alors que nous n'avons pas pris plus de risque que d'habitude, c'est la douche froide ! En installant un malheureux logiciel (ne vous inquiétez pas, celui-là vous n'en entendrez jamais parler ici), le PC affichait publicité et autres pop-ups louches. Windows Defender s'est alors réveillé pour me prévenir d'une contamination... sans pour autant résoudre le problème. Windows 10 était tellement à la rue qu'il a fallu désinfecter le système avec AVG Rescue CD (voir *Pirate Informatique* n°19). Au final, il s'agissait d'une infection de Win32/heri qui a créé un faux Firefox.exe communiquant avec un bot. Nous avons réussi à éviter le formatage, mais Windows Defender a définitivement été oublié au profit d'un antivirus gratuit, mais efficace.

HACKTUALITÉS



Avec l'aimable autorisation de notre ami Zach Weiner

CITATION

«Les gens sont enclins à prendre des raccourcis mentaux. Ils savent sans doute qu'ils ne devraient pas donner certaines informations, mais la crainte de ne pas être agréable, la crainte de paraître ignorant ou la crainte de l'autorité sont des déclencheurs qui peuvent être utilisés pour convaincre une personne de passer outre les procédures de sécurité établies.»

- Kevin Mitnick,
sur le social engineering

La voix de son maître ?

Savez-vous ce qu'ont en commun Cortana, Google Now et Siri ? Oui c'est vrai, ils envoient tous ce que vous leur demandez directement à la NSA, mais il s'agit ici d'autre chose... Deux chercheurs ont dernièrement démontré qu'il était possible de pirater ces applications en envoyant des fréquences comprises entre 80 et 108 MHz vers un kit mains libres relié à un téléphone. Le câble de l'appareil fait alors office d'antenne. Les ondes vont induire un signal électrique qui va être interprété comme une commande vocale ! On peut imaginer envoyer une commande qui ouvrirait un site malveillant par exemple. Heureusement, il existe des restrictions : la présence d'un kit mains libres et la mise en route de Siri/Now/Cortana au moment de l'attaque. Encore une bonne raison de se méfier quand même...

LES CLÉS USB *PIRATE INFORMATIQUE* ARRIVENT BIENTÔT !

Dans le numéro 26 de notre magazine *Pirate Informatique*, nous vous avions parlé de la possibilité de pré-commander des clés USB contenant tous les numéros de nos magazines *Pirate Informatique* et *Les Dossiers du Pirate*. En effet nous avons noté que beaucoup de lecteurs désiraient acheter d'anciens numéros ou nous demandent des articles que nous avons déjà réalisés. Comme il n'est pas possible pour nous de fournir les numéros passés pour des questions pratiques et logistiques, nous vous proposons cette solution originale. Il s'agirait de clés de quelques Go en édition limitée. Les lecteurs qui ont déjà pré-commandé seront prioritaires pour la livraison. Lorsque les clés seront prêtes, vous recevrez un e-mail vous indiquant la marche à suivre pour la commande.

Il n'est pas trop tard pour pré-commander !

Les lecteurs qui nous rejoignent peuvent bien sûr toujours pré-commander une clé ou se manifester à cette adresse : **usb@idpresse.com**. Cela ne vous engage à rien. Le prix est toujours fixé à 15 € (+les frais de port). Les CD vendus avec *Pirate Informatique* ne seront pas intégrés aux données de la clé.

PUB SUR INTERNET : CHOISIS TON CAMP CAMARADE !

Mal nécessaire, pollution sonore et visuelle : la publicité sur Internet divise selon que l'on soit un acteur ou un utilisateur du réseau des réseaux. Les webmasters et sociétés gérants du contenu trouvent injustifié que leur travail ne soit pas rémunérateur tandis que les citoyens lambda n'en peuvent plus de ces publicités qui envahissent leurs écrans.

Les bloqueurs de publicité ont le vent en poupe ! Ces programmes ne cessent de grimper en popularité (+41 % d'installation depuis l'année dernière) et le manque à gagner pour les sites représentera 61 milliards de dollars en 2016 ! De quoi faire trembler les acteurs du Net, des plus petits blogueurs aux plus gros éditeurs. Il faut dire que la publicité sur Internet, souvent mal ciblée, redondante et envahissante, les internautes n'en veulent plus surtout si c'est pour se taper 30 secondes de pub pour 10 secondes de «lolcat».

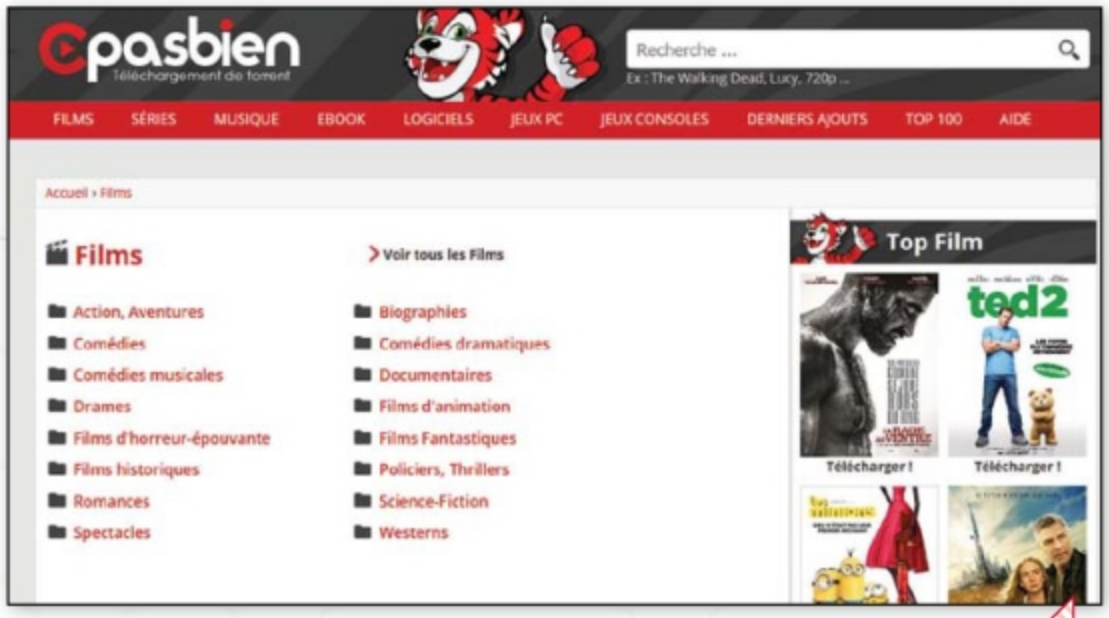
Le retour de bâton

La situation est telle que l'IAB, un syndicat qui regroupe les acteurs de la publicité sur Internet, vient de publier un communiqué pour expliquer qu'ils sont allés trop loin... Incroyable !
En effet, avec l'explosion de la bulle Internet du début des années 2000, les «survivants» ont été pressés de monétiser leur contenu pour éviter de disparaître à leur tour. C'est là que sont apparues les publicités sonores, très lourdes plombant la bande passante, la batterie et la patience des Internautes. C'est à ce moment que les utilisateurs ont commencé à installer des logiciels

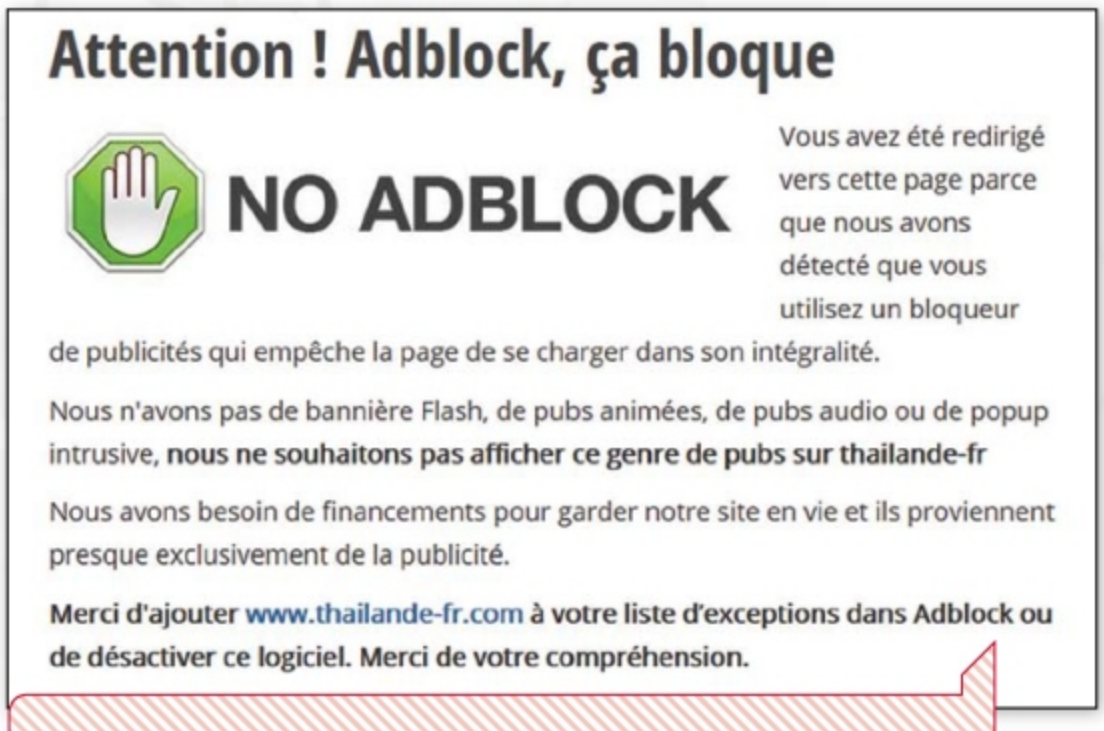
comme Adblock. Ce type de logiciels fonctionne avec des listes. La liste noire est gérée par chaque Internaute. À lui de décider si oui ou non il doit afficher de la publicité sur un site «méritant» à leurs yeux. Le concept de liste blanche existe depuis 2011 et est géré par la société Eyeo, éditrice d'Adblock. Si un site est sur la liste blanche, elle affichera sa publicité, même si encore une fois l'utilisateur a le choix d'outrepasser ces restrictions. Bien sûr, chaque site désirant figurer sur cette liste blanche doit montrer qu'il propose des publicités non intrusives : pas d'animation, de son, de dissimulation de contenu, etc.

Aux Internautes de jouer le jeu!

Le problème reste que la plupart des internautes utilisent des listes noires déjà validées par d'autres et ne prennent pas le temps de gérer la publicité au cas par cas. Ils «oublient» ainsi fréquemment de valider la publicité sur un site qu'ils fréquentent souvent et qu'ils aiment. Il y a aussi les Internautes qui désirent bloquer absolument toutes les pubs parce qu'ils préfèrent faire des dons à leurs sites préférés ou parce que ce sont des «rebelles de la société» (comme Jean-Kévin, 13 ans). Et la guerre a commencé ! Loin de se laisser impressionner et de demander une intégration à la liste blanche de Eyeo, le groupe Axel Springer éditeur du journal *Bild* (le plus gros tabloïd d'Allemagne) a décidé de bloquer la lecture aux utilisateurs d'AdBlock ! Pour profiter du contenu, il faut retirer *Bild* de sa liste noire. *Bild* n'a pas envie de demander gentiment à une startup le droit d'afficher une publicité sur laquelle le magazine n'aurait plus la main... Il existe donc un juste milieu. Pourquoi ne pas utiliser Adblock pour les sites qui abusent complètement (suivez mon regard) et laisser les journalistes et webmasters vivrent de leur travail en autorisant l'affichage sous certaines conditions ? Ce n'est pas parce que nous ne faisons pas de pub dans ce magazine que tous nos confrères peuvent se le permettre...



Le tracker public Cpasbien.pw est un très bon exemple de site qui abuse. Voici la version avec Adblock. Sans ce logiciel c'est la foire aux popups, publicités très graveleuses et dégradantes pour l'image de la femme...



De plus en plus de sites demandent à leurs visiteurs de les ajouter à leur liste d'exceptions. Ils pensent, à raison, que ce n'est pas à une autre société de décider quel type de publicité est adéquat ou non et refusent de céder au «chantage» de la liste blanche d'Eyeo.

BOULET, LE DESSINATEUR QUI N'AIME PAS LA PUBLICITÉ

À la rédaction, nous aimons le dessinateur Boulet et nous suivons sont travail depuis des années. Boulet n'aime pas la pub... même sur son site. Nous vous invitons à lire sur son blog ce qu'il pense de la publicité sur Internet dans cette planche baptisée *Pub et Caca* : **http://goo.gl/r6l8uK**

MICROSOFT JOUE AUSSI LA CARTE «BIG BROTHER»

Vous connaissez sans doute l'adage *«si c'est gratuit, c'est que c'est vous le produit»* ? Et bien, cela se vérifie encore avec ce Windows 10. Copiant sur ses concurrents Google et Apple, la firme de Redmond épie vos petites habitudes. Il s'agit officiellement d'améliorer «l'expérience utilisateur», mais êtes-vous dupe ?

Sur Internet, c'est la levée de boucliers contre Microsoft depuis que les utilisateurs ont mis le nez dans le menu **Paramètres**>**Confidentialité** du dernier OS de la firme. La société américaine se permet par défaut de scruter ce que nous tapons, de nous écouter (via les demandes vocales que nous formulons à Cortana), de s'emparer du contrôle de la webcam, de nous localiser ou de lire nos SMS ! C'est terrible, mais c'est exactement ce que font Google et Apple sur leurs systèmes et services respectifs. Bien sûr, ce n'est pas une raison pour accepter sans broncher cette politique de l'espionnage d'autant qu'il est facile de désactiver ces mouchards.

DES ESPIONS DOCILES...

Car Microsoft a eu la bonne idée de presque tout mettre dans le même menu et même de nous expliquer exactement à chaque fois ce que Windows espionne. Lorsque Windows 10 vous dit qu'il veut «*apprendre à reconnaître votre voix*» et «*collecter [...] l'historique des frappes*» pour proposer de meilleures suggestions il faut lire «*enregistrer tout ce que vous racontez et ce que vous écrivez pour mieux vous vendre des trucs par la suite*». Il faut savoir lire entre les lignes donc... Pour aller plus loin dans cette lutte contre la surveillance de Microsoft, nous utiliserons enfin le logiciel Windows Privacy Tweaker de Jean-Pierre Lesueur que nous avons interviewé dans le précédent numéro.

DÉSACTIVEZ LES APPLICATIONS DU WINDOWS STORE

Depuis Windows 8, Microsoft essaie de réunir les utilisateurs mobiles et PC en créant une interface commune et des applications (les fameuses tuiles Metro ou ModernUI). Même si Windows 10 revient un peu en arrière en proposant de base un bureau «standard», ces applications sont toujours de la partie. Sur Windows 10, ces applis préinstallées sont au nombre de 23 sur votre système : Photos, Xbox, Store, Money, Maps, etc. Si vous utilisez Windows 10 sur un PC et que vous ne comptez pas acheter d'appareil mobile avec l'OS de Microsoft, ces applications sont complètement superflues puisque vous avez déjà vos programmes «desktop» préférés. Le logiciel 10Appsmanager va enterrer ces «tuiles» pour ne plus jamais les voir dans votre menu démarrer ou ailleurs.

Lien : **http://goo.gl/YMUr5y**

PAS À PAS

Désactiver les mouchards de Microsoft

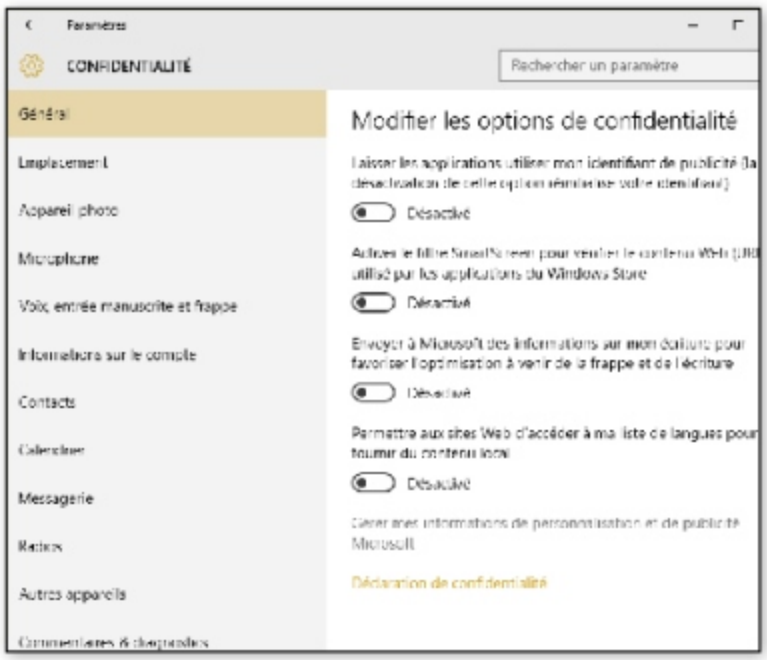
CE QU'IL VOUS FAUT

MICROSOFT WINDOWS 10

DIFFICULTÉ :

01 LE MENU CONFIDENTIALITÉ

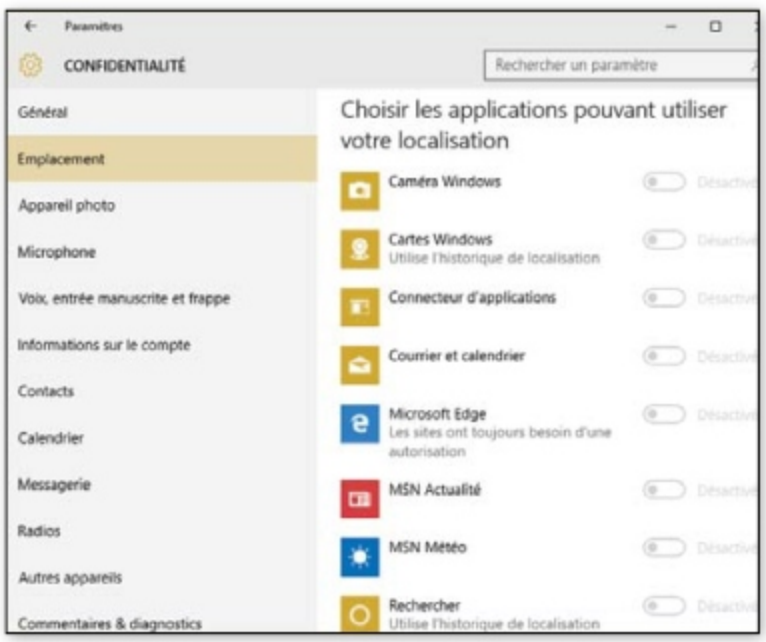
Pour commencer le ménage dans les petites intrusions de Microsoft, allez dans **Paramètres** (menu **Démarrer**) puis



Confidentialité. Dans chaque onglet, vous trouverez des choses à désactiver. Dans **Général** par exemple, pourquoi ne pas désactiver l'envoi d'information sur votre écriture? Oui vous avez bien lu, cette option n'est rien d'autre qu'un keylogger...

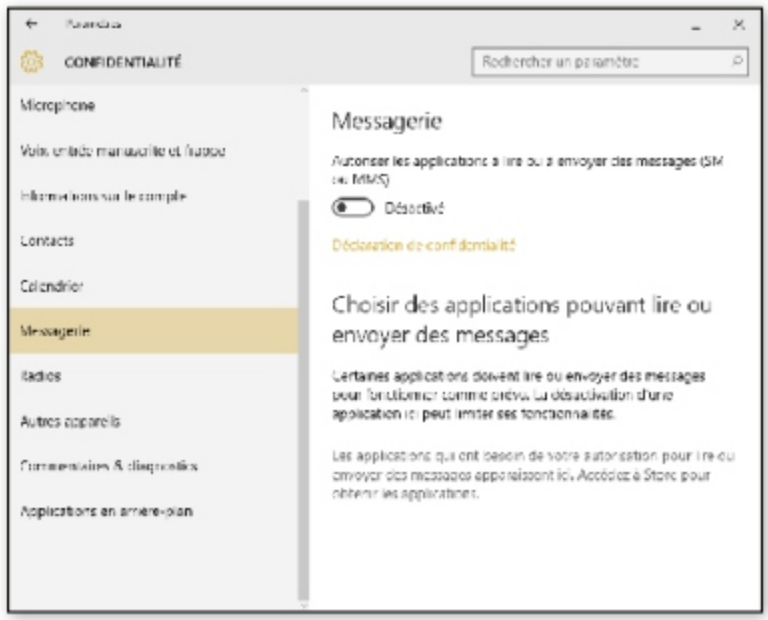
02 STOPPEZ L'ESPIONNAGE

Dans **Emplacement,** il est possible de désactiver l'envoi de votre position ou de choisir quelles applis pourraient y avoir accès. Dans **Appareil photo**, désactivez l'accès à votre webcam et faites de même pour votre microphone dans l'onglet suivant. Dans **Voix, entrée manuscrite et frappe**, cliquez sur **Arrêter de me connaître** pour rendre Cortana sourde et aveugle.



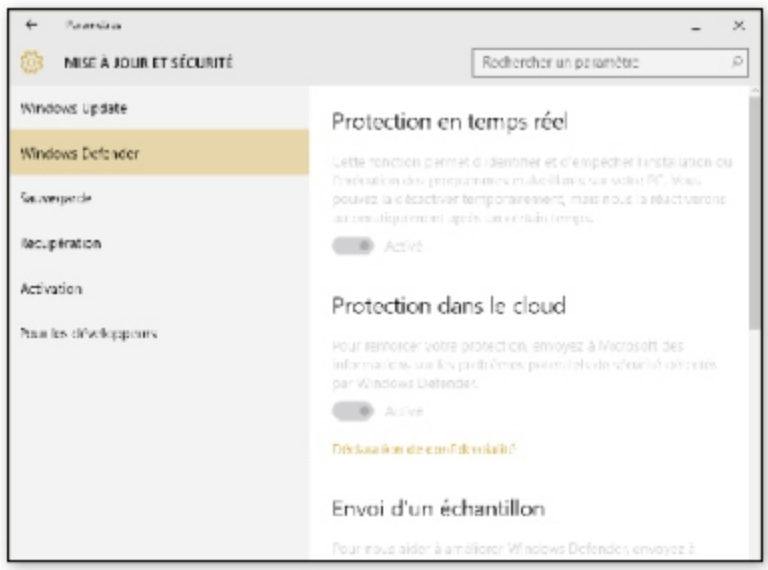
03 FAITES LE TRI

Faites de même pour tous les autres onglets et demandez-vous à chaque fois: «*Ai-je vraiment besoin de ça?*». N'oubliez surtout pas l'accès à vos contacts, à la lecture de SMS, au Bluetooth (**Radios**), etc. Si vous n'utilisez pas les applis Metro préinstallées, allez les désactivez dans **Applications en arrière-plan** et désactivez la synchronisation avec d'autres appareils.



04 WINDOWS DEFENDER AUSSI !

Si vous n'avez pas d'antivirus tiers, Windows Defender sera alors activé par défaut (ce que nous déconseillons fortement). Ce logiciel enverra aussi des informations chez Microsoft si vous ne l'empêchez pas! Allez dans **Paramètres** > **Mise à jour et sécurité** > **Windows Defender** et désactivez **Envoi d'un échantillon** et **Protection dans le cloud**. Ne touchez pas à **Protection en temps réel** si vous ne voulez pas devenir vulnérable.



PAS À PAS

Allons encore plus loin...

CE QU'IL VOUS FAUT

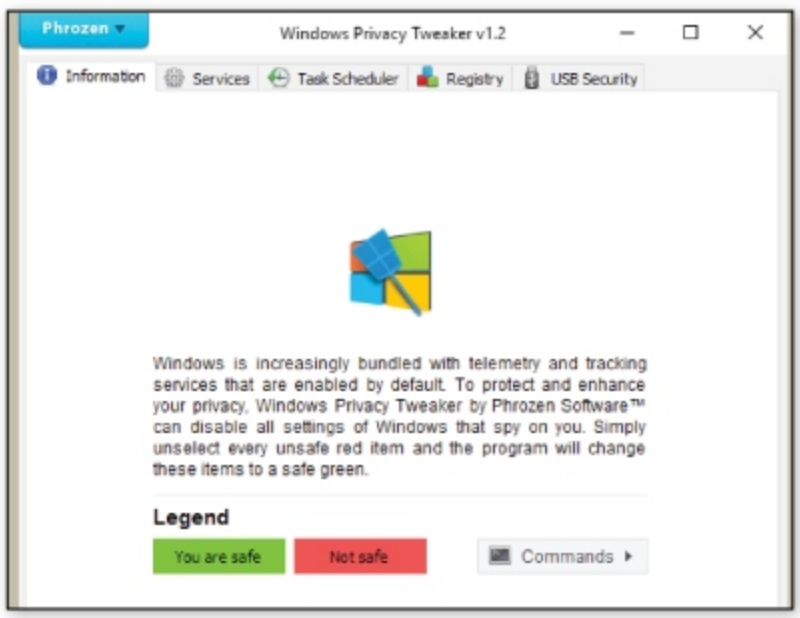
WINDOWS PRIVACY TWEAKER

OÙ LE TROUVER ? :
www.phrozensoft.com/freeware

DIFFICULTÉ :

01 LE CODE COULEUR

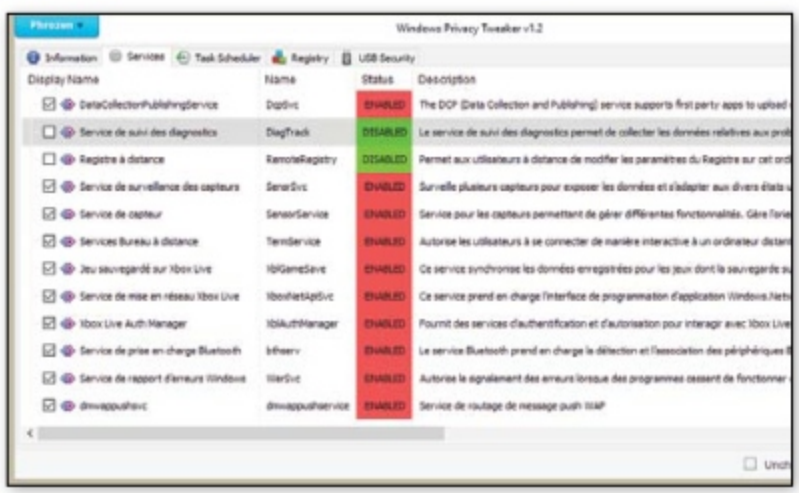
L'utilisation de Windows Privacy Tweaker n'a vraiment rien de sorcier. Lorsque l'icône est verte, c'est que vous ne risquez pas de voir compromettre vos habitudes, vos données ou que les



interactions entre votre PC et les serveurs de Microsoft sont désactivées. Même en ayant fait le ménage dans **Paramètres** > **Confidentialité** (comme expliqué dans le précédent pas-à-pas), vous verrez que la plupart des paramètres sont dans le rouge...

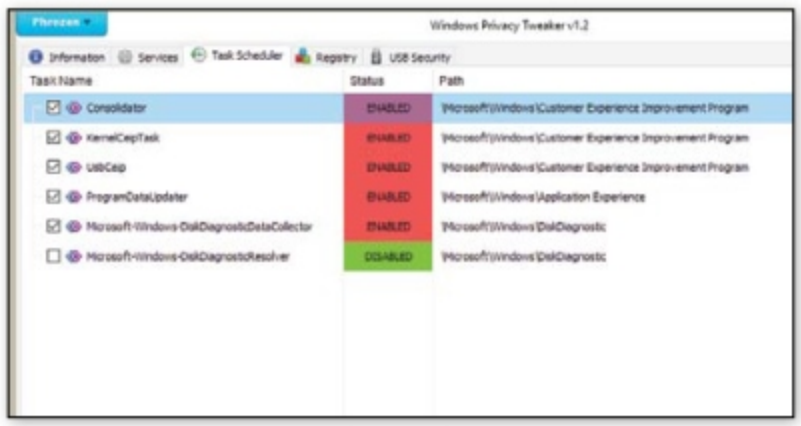
02 LES SERVICES WINDOWS

Dans l'onglet **Services**, vous pouvez par exemple désactiver le **DcpSvc** qui permet à certaines applis d'uploader des données dans un cloud propriétaire. Pour chaque ligne, vous trouverez une description en français. Pas la peine de désactiver les fonctions jeu Xbox si vous possédez cette console et que vous souhaitez synchroniser les informations du Live avec votre PC. À l'inverse, avez-vous vraiment besoin du **Service de bureau à Distance**, du **SensorService** ou du **Registre à distance**?



03 LE PLANIFICATEUR DE TÂCHES

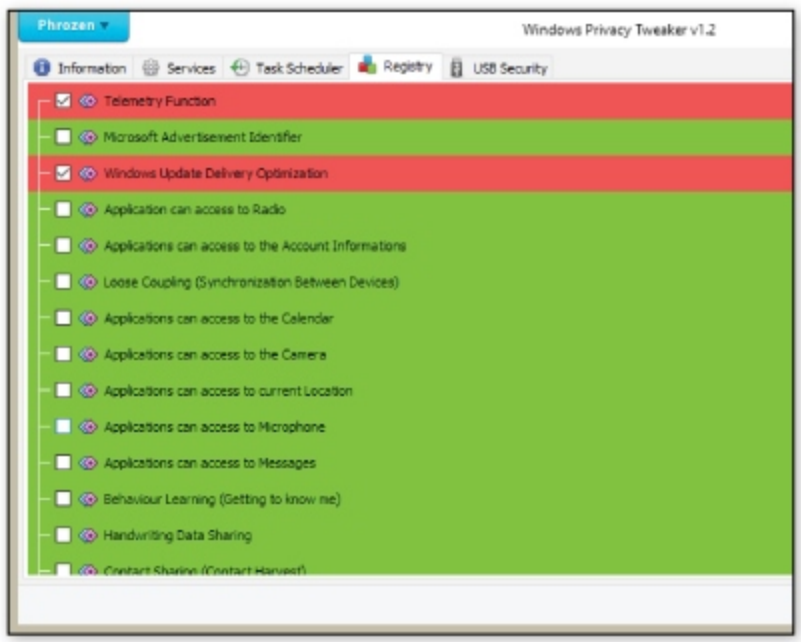
Dans **Task Scheduler**, il s'agit autant de fuites de données que d'opérations réalisées sur votre système à votre insu: diagnostic de vos disques durs, vérification des mises à jour de certains



programmes, statistiques liées à vos périphériques USB, etc. Consolidator est aussi un mouchard qui envoie des données sur vos petites habitudes. Vous pouvez tout remettre en **DISABLED** et revenir en arrière si vous connaissez des problèmes avec certaines fonctions.

04 LA BASE DE REGISTRE

Ce qui se trouve dans **Registry** est plus complexe, mais si vous avez suivi notre précédent pas-à-pas, la plupart des lignes devraient être vertes (accès au Calendrier, au micro, géolocalisation, etc.) Décochez **Telemetry Function** et **Windows Update Delivery Optimization**. En bas, supprimez ce dont vous n'avez pas besoin: **Bing**, **Smartscreen**, **Microsoft Feedback**, etc. Dans le doute, virez tout! Le dernier onglet permet de mettre les clés USB en lecture seule, mais ce n'est vraiment pas nécessaire.



CHEZ VOTRE MARCHAND DE JOURNAUX

MINI PRIX
3,50 €
seulement

LE 1ER MAGAZINE
100% ANDROID ET 100% PRATIQUE

DANS NOTRE CD !

Si vous avez raté notre précédent article sur nbound (hébergement local de son propre serveur DNS), sachez que le PDF de cet article se trouve dans notre CD !

OpenNIC : VOS DNS LIBRES !

Dans notre précédent numéro, nous avons vu comment héberger soi-même son propre serveur DNS en local. Cette manipulation permet d'éviter le tracking et la censure. Il existe une solution encore plus simple : utiliser les services d'OpenNIC, un fournisseur ouvert, neutre et démocratique...

Nous avons déjà vu que les DNS des FAI peuvent censurer les sites sur lesquels vous voulez vous connecter (l'exemple de t411 est le plus récent) tandis que ceux de Google sont piégeux. La société américaine s'en sert pour promouvoir ses propres services et vos données ne sont pas protégées (rien n'empêche Google d'en faire ce qu'il veut ou de vous «tracker»). Pour éviter que des individus ou des robots n'aient accès à la liste des sites que vous visitez, pourquoi ne pas utiliser OpenNIC ? Ce service va trouver des serveurs DNS triés sur le volet et le plus près de chez pour vous éviter les temps de latence.

POURQUOI LUI FAIRE CONFIANCE ?

OpenNIC est un «Network Information Center» détenu et contrôlé par ses utilisateurs offrant une alternative démocratique et non nationale aux registres traditionnels des domaines de premier niveau comme l'ICANN (l'autorité de régulation d'Internet qui gère et enregistre les noms de domaine et l'adressage d'IP). Chaque personne enregistrée dispose d'un accès à une mailing-list et à un droit de vote concernant les décisions de développement. Bien sûr, pour avoir accès au service vous n'avez pas besoin de vous inscrire, mais pourquoi ne pas participer aux débats ?

LES DNS DE FDN

French Data Network est un FAI français avec le statut d'association loi 1901. Il est d'ailleurs le plus ancien fournisseur de service Internet, avant même la création du Web ! Trop confidentiel pour être concerné par les injonctions de l'État concernant la censure, FDN propose gratuitement ses services de serveurs DNS. Si OpenNIC est décevant ou si vous voulez des DNS basés en France les voici : 80.67.169.12 et 80.67.169.40.

LEXIQUE

***DNS :** Acronyme de Domain Name System. Système ayant remplacé le fichier «préhistorique» Hosts.txt contenant les IP des principaux sites du Web. Ce système permet de diriger un Internaute vers un site (et donc son adresse **http://www.un-site.com**) sans pour autant connaître son IP.

***TRACKING :** Il s'agit de mesures permettant à des sociétés d'en savoir le plus possible sur vos habitudes de surfs, vos achats en ligne, vos recherches, etc. Le but est bien sûr de vous proposer des produits et services qui sont susceptibles de vous intéresser.

***FAI :** Acronyme de Fournisseur d'Accès Internet. En France, on a Free, SFR, Orange et... French Data Network bien sûr !

PAS À PAS

Changez vos DNS sous Windows et Android

CE QU'IL VOUS FAUT

OPENNIC

OÙ LE TROUVER ? :
www.opennicproject.org

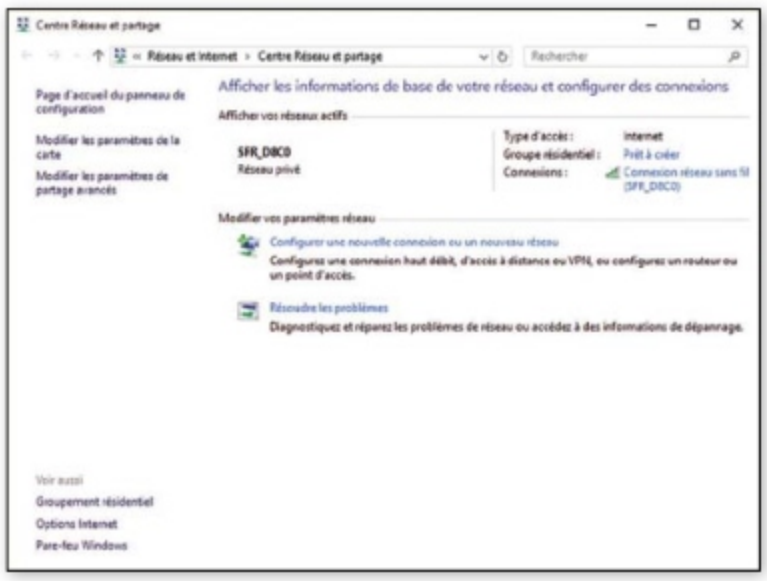
DIFFICULTÉ :

01 LE SITE

Sur le site OpenNIC, faites **Get Started Now!** et notez les deux DNS les mieux notés sous **Your Nearest OpenNIC DNS Servers**. Il faudra refaire cette opération si vous sentez que vos temps d'accès à certains sites sont moins bons. Pas la peine de le faire tous les jours non plus...

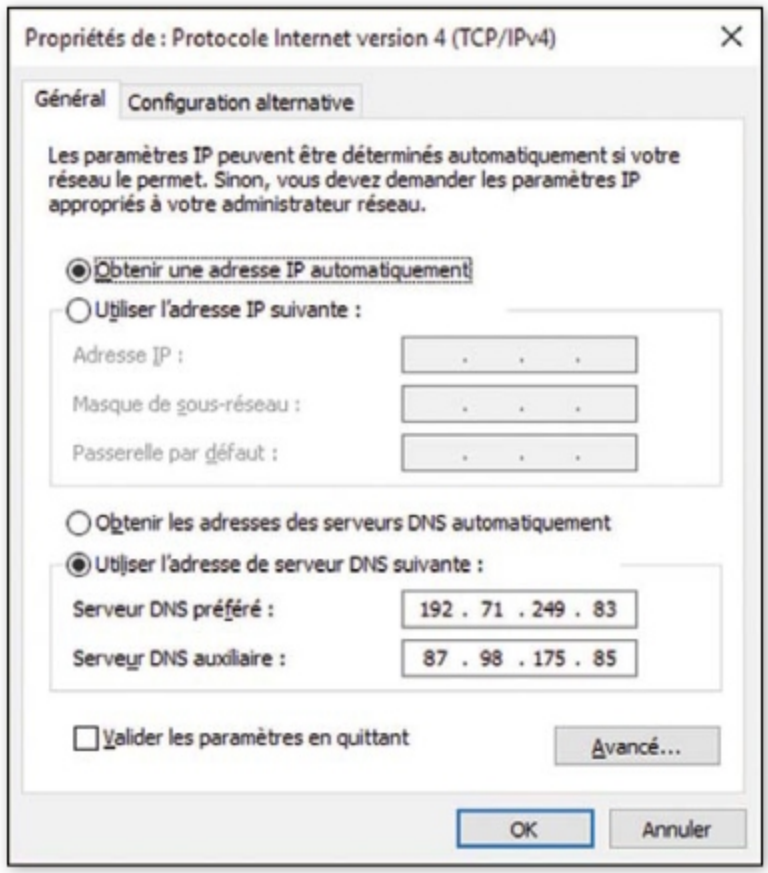
02 SOUS WINDOWS

Sous les différentes versions de Windows (Vista, 7, 8 et 10), la procédure est très similaire. Il faut déjà avoir accès à votre **Centre Réseau et partage** depuis le **Panneau de configuration**, le **GodMode** (voir les microfiches de la partie Hacking) ou en faisant un clic droit dans l'icône de votre carte réseau.Cliquez ensuite sur **Connexion réseau sans fil_[votre SSID]** puis sur **Propriétés**.



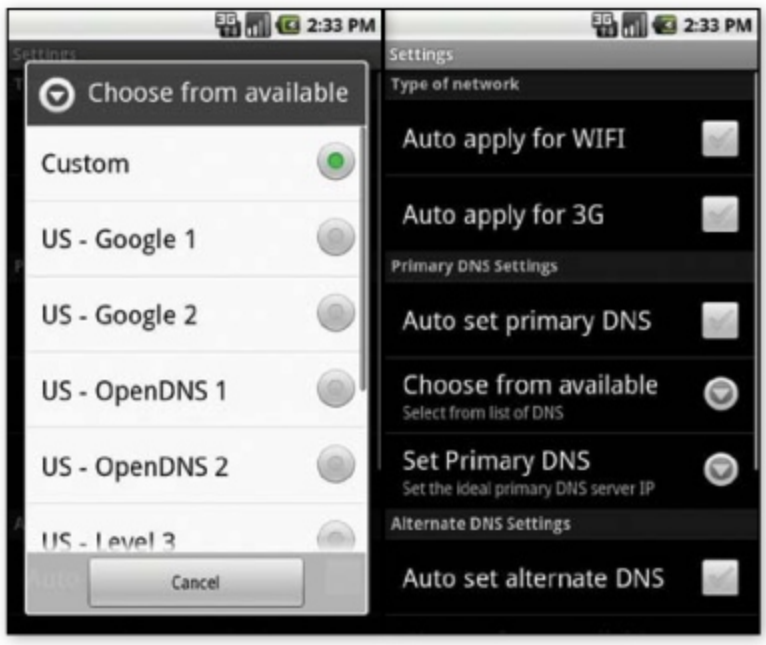
03 VOS NOUVEAUX DNS

Ensuite, il faudra surligner la ligne **Protocole Internet version 4 (TCP/IP v4)** et faire **Propriétés**. Notez que si vous utilisez l'IPv6 c'est cette ligne qu'il faudra surligner (faites les deux dans le doute !). En bas de cette nouvelle fenêtre, choisissez l'option **Utiliser l'adresse de serveur DNS suivante** puis notez les chiffres que vous avez obtenus sur OpenNIC.



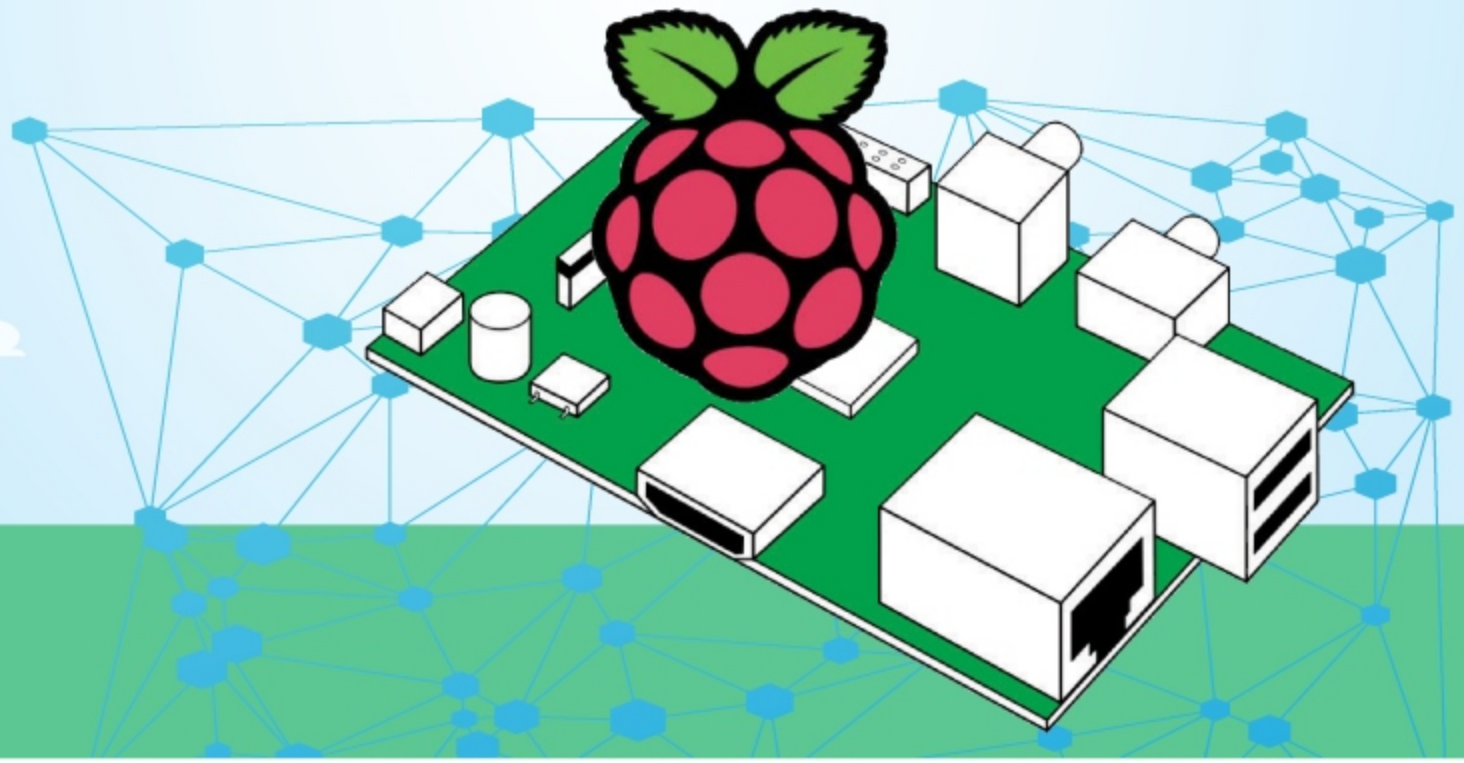
04 ET SUR ANDROID ?

Sur appareil Android, il est aussi possible de changer ses DNS. Sans le root, vous pouvez utiliser DNSet. Le seul problème est qu'il ne fonctionne pas sur les versions



récentes du système (à partir d'Android 4.0). Pour les utilisateurs root, DNS Changer se chargera de la basse besogne. Bien sûr, cela fonctionne aussi bien avec le WiFi que la 3G...

UN VPN AUTO-HÉBERGÉ!



Lorsque l'on se connecte sur un point d'accès WiFi extérieur, il existe toujours le problème de la sécurité. Entre les pirates à la petite semaine et les intrusions dans la vie privée, on serait bien tenté de passer par un VPN. Le problème c'est qu'on ne sait jamais lequel choisir. Payant ou gratuit ? Et dans quel pays ? Pour en finir avec ces incertitudes, nous allons héberger nous-mêmes un VPN à la maison sur notre bien-aimé Raspberry Pi...

À la maison, bien au chaud sur son réseau local pas de problème, mais lorsqu'on met le nez en dehors de chez soi avec son PC ou son téléphone, les scripts kiddies guettent la moindre faiblesse sur les réseaux publics et non sécurisés. Opter pour la connexion via VPN c'est bien, mais encore faut-il y voir clair dans les dizaines d'offres qui nous sont proposées. Mes données sont-elles en sécurité ? N'y a-t-il pas un risque d'exploitation ? Quelle est la législation en ce qui concerne mes journaux de connexion dans tel ou tel pays ? La plupart des utilisateurs ne vont pas au bout de la démarche, abandonnent et croisent les doigts pour ne pas tomber sur un petit malin qui ira pirater leur compte Facebook ou Gmail depuis le WiFi de la bibliothèque ou du McDo.

ON EST TOUJOURS MIEUX CHEZ SOI

La solution ne serait-elle pas d'héberger soi-même un VPN à la maison ? Une machine distante sur laquelle se connecter lorsque vous êtes loin de votre vaisseau mère et qui chiffrerait en plus vos données ? C'est tout à fait possible ! Il faudrait alors un PC dédié à cette tâche à la maison... À moins d'avoir un Raspberry Pi ! Peu gourmand en énergie et de taille très réduite, ce nano-ordinateur à 35 € est l'appareil idéal pour ce genre de tâche. Pour ce faire, nous verrons donc comment installer la distribution Linux Raspbian sur notre appareil puis nous paramètrerons un petit serveur PPTP. Enfin, nous ajouterons une redirection dynamique pour pouvoir y accéder depuis l'extérieur du réseau !

LEXIQUE

***VPN :**
Réseau privé virtuel en français. Il s'agit d'une sorte de tunnel, chiffrée ou pas, qui permet de créer un lien direct entre des ordinateurs distants.

***SCRIPTS KIDDIES :**
Des pirates ayant peu de capacités techniques, mais utilisant des programmes malveillants puissants.

PAS À PAS

Votre VPN à la maison !

CE QU'IL VOUS FAUT

- **Un Raspberry Pi (1 ou 2)**
- **Une carte SD de 4 Go (microSD pour le Raspberry Pi 2)**
- **Un câble Ethernet RJ45**
- **Une alimentation micro USB (celle d'un smartphone)**

DIFFICULTÉ : ☠☠☠

WIN32 DISK IMAGER

OÙ LE TROUVER ? : **http://sourceforge.net/projects/win32diskimager**

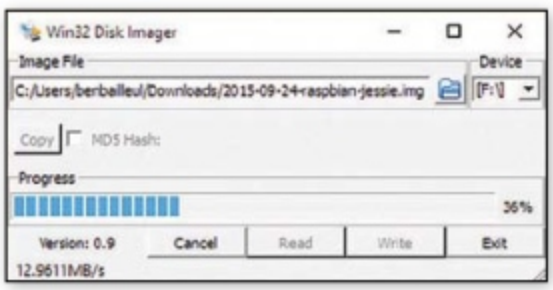
RASPBIAN «WHEEZY»

OÙ LE TROUVER ? : **www.raspberrypi.org/downloads**

PUTTY (CLIENT SSH)

OÙ LE TROUVER ? : **www.putty.org**

01 LE SYSTÈME SUR LA CARTE SD



Comme le Raspberry Pi n'a pas de système d'exploitation, il va falloir lui en donner un sur la carte SD. Nous avons choisi Raspbian, une version «Raspberry» de la distribution Linux Debian. Lancez Win32 Disk Imager, sélectionnez le fichier **2015-05-05-raspbian-wheezy.img** avec l'icône en forme de dossier puis spécifiez l'emplacement de la carte SD dans la colonne Device. Faites **Write** et attendez la fin du processus. Insérez ensuite la carte dans votre Raspberry Pi. Attention, n'utilisez pas «Jessie» si vous souhaitez uniquement passer par PuTTY.

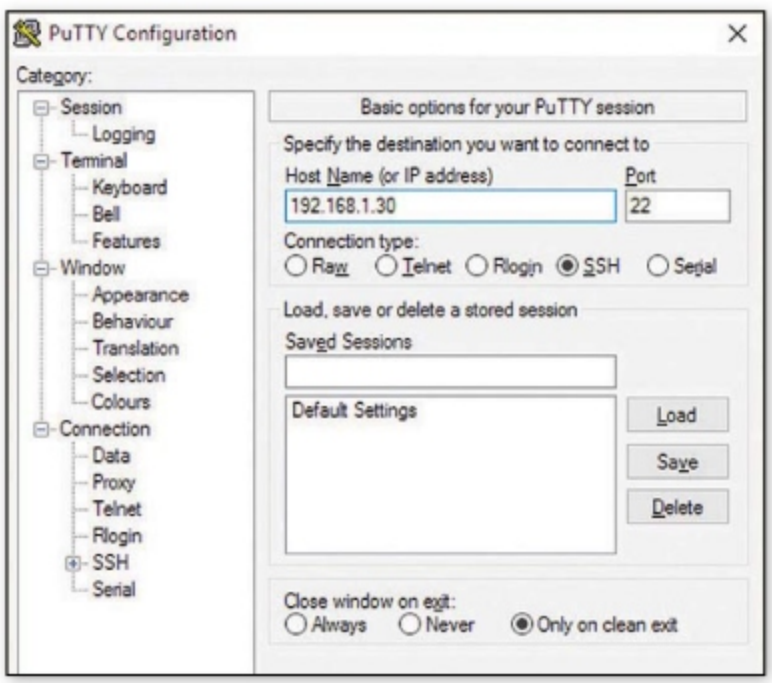
02 BRANCHEMENT ET RÉCUPÉRATION DE L'IP

Commençons par brancher le Raspberry Pi sur votre routeur/box avec le câble Ethernet. Branchons aussi l'alimentation. Au bout de quelques secondes, votre réseau va donner une IP locale à votre Raspberry. Allez dans les paramètres de votre box (généralement **192.168.1.1**), mais pour la Freebox, il faudra aller sur Free.fr) et retrouvez cette IP. Pour nous, ce sera **192.168.1.29**.

POURQUOI UN VPN ?

*Pour chiffrer vos données personnelles.
*Pour se protéger des pirates et des mouchards.
*Pour éviter la censure des gouvernements (t411, The Pirate Bay, etc.).
*Pour avoir une IP française même à l'étranger (télévision à la demande, Canal+, etc.).

03 COMMUNIQUEZ AVEC PUTTY

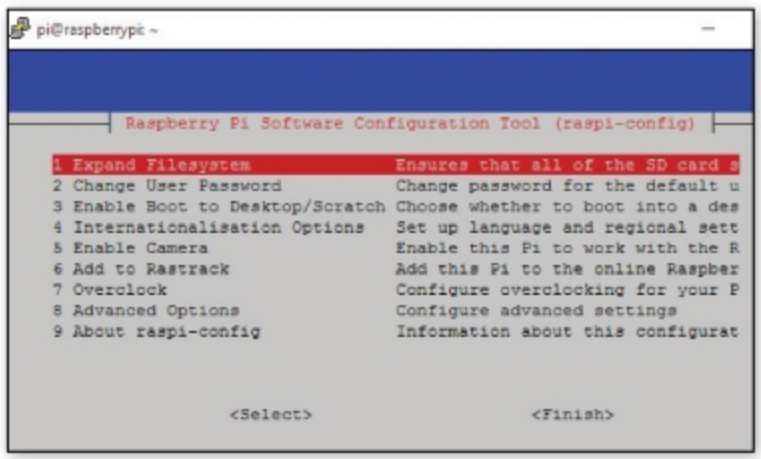


Pour communiquer avec le Raspberry Pi à travers le réseau local, nous allons utiliser PuTTY, un client SSH. Notez que vous pouvez utiliser l'appareil comme un ordinateur avec clavier/souris/écran si vous le désirez. Ouvrez le programme et tapez l'IP du Raspberry dans **Host Name (ou IP address)**. Laissez le port**22**, cochez **SSH** et cliquez sur **Open**.

POURQUOI PAS OPENVPN ?

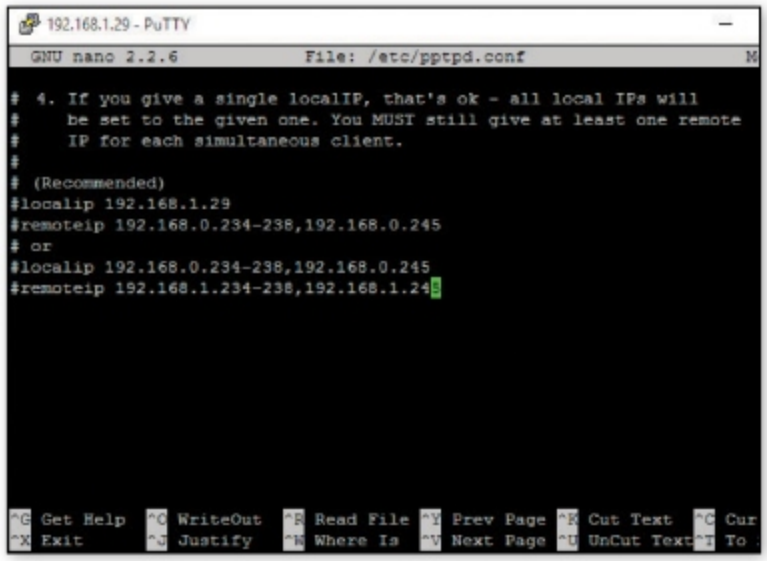
Les experts vous le diront, rien ne vaut le protocole OpenVPN pour protéger sa connexion. Alors pourquoi avons-nous choisi le vieillissant PPTP de Microsoft ? Pour commencer, nous partons du principe que vous désirez juste échapper aux scripts kiddies qui sévissent sur les réseaux. La plupart de ces pirates à 2 kopecks lâcheront l'affaire avec un chiffrement, même faible (128 bits contre 256 pour OpenVPN). Pour protéger des communications sensibles par contre, OpenVPN est indispensable. Notez aussi que le PPTP est relativement simple à mettre en place alors que l'OpenVPN et ses certificats constituent une autre paire de manches...

04 INSTALLATION DE MOTION



Dans la nouvelle fenêtre, tapez pi après login as: et raspberry après password. Tapez sur Entrée pour avoir accès au prompt **pi@raspberrypi ~ $**. Faites **sudo raspi-config** et allez dans **Expand Filesystem** pour optimiser la place sur la carte SD (vous pouvez aussi overclocker votre appareil ici). Allez sur **Finish** et faites **Yes** pour le redémarrage. Vous allez perdre la connexion avec PuTTY, c'est normal. Relancez-le et tapez **sudo passwd root** et trouvez-vous un mot de passe correct. Tapez ensuite **reboot** et utilisez à l'avenir root comme identifiant et le nouveau mot de passe. Bravo, vous avez un accès root sur votre Raspberry Pi !

05 LE FICHIER .CONF



Installons maintenant PPTP avec la commande (en root) **sudo apt-get install pptpd**. Faite **Y** lorsqu'on vous le demandera. À la fin du processus, il faudra éditer le fichier de configuration de PPTP avec l'éditeur Nano. Tapez **sudo nano /etc/pptpd.conf** et trouvez les lignes

#localip 192.168.0.1
#remoteip 192.168.1.234-238,192.168.1.245

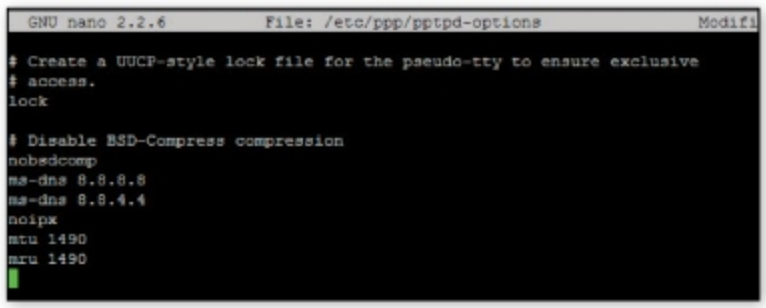
Retirez les # et remplacez la première IP par l'IP local de votre Raspberry Pi (pour nous **192.168.1.29**). Pour la seconde ligne, laissez comme cela. Ces IP sont en fait les plages allouées aux appareils qui se connecteront au VPN. Pour valider les changements, faites **Ctrl + X** puis **Y** et **Entrée**.

06 LE FICHIER « OPTIONS »

Éditons un autre fichier de configuration en tapant **sudo nano /etc/ppp/pptpd-options**. Il faudra ajouter les lignes suivantes à la fin du fichier :

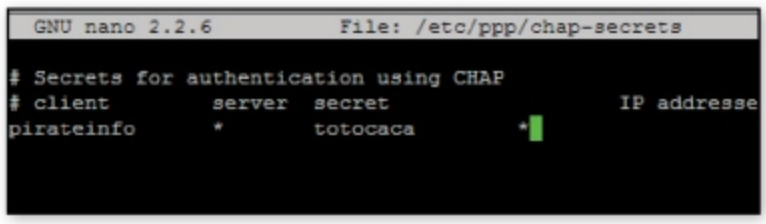
ms-dns 192.168.1.1
nobsdcomp
noipx
mtu 1490
mru 1490

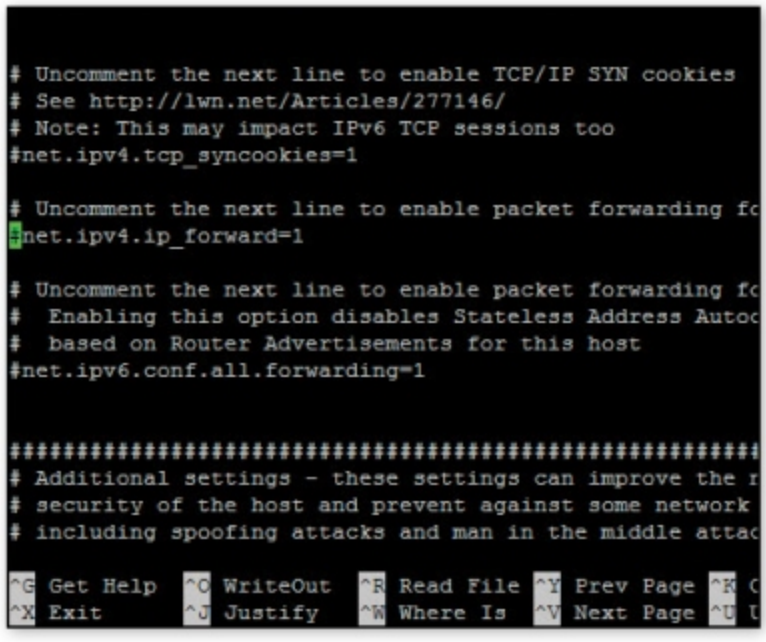
Validez de la même manière. Attention pour la première ligne, les DNS de votre FAI sont peut-être différents. Dans le doute, mettez 8.8.8.8 ou un DNS d'OpenNIC (voir l'article dans cette rubrique).



07 VOS IDENTIFIANTS

Nous allons maintenant configurer les identifiants du VPN. Faites **sudo nano /etc/ppp/chap-secrets** et entrez les identifiants que vous désirez en faisant **utilisateur[tab]*[tab]motdepasse[tab]***. Notez que [tab] correspond à la tabulation (la touche aux deux flèches à côté du A). Validez et tapez sudo service pptpd restart pour redémarrer. Bidouillons ensuite la redirection d'IP. Faites **sudo nano /etc/sysctl.conf** et retirez le # devant **#net.ipv4.ip_forward=1**. Sauvegardez les modifications et faites **sudo sysctl -p**.





08 LA TRANSLATION DE PORT

Retournez dans l'interface de votre box/routeur et dirigez-vous vers **Translation de ports** ou **NAT** (le nom peut différer). Mettez l'IP de votre appareil dans l'IP de destination ainsi que les ports **1723** en externe et en destination. Choisissez **TCP** comme protocole et validez. Votre VPN est prêt pour une connexion en local! Mais pour l'extérieur du réseau ? Il va falloir paramétrer une adresse dynamique. Vous pouvez soit le faire depuis le Raspberry Pi (suivez ce lien http://goo.gl/ErjNQp et allez dans la section **DNS Dynamique**) ou faites-le depuis votre box/routeur en vous aidant de notre article du numéro 23 téléchargeable gratuitement ici : https://goo.gl/g4gfKS.

POURQUOI ÇA NE MARCHE PAS ?

Si vous rencontrez un problème et que le VPN ne fonctionne pas, cela peut malheureusement venir de différents paramètres très différents (problème d'iptables, configuration du fichier rc.local, etc.) Faire un inventaire complet aurait pris des pages entières. Pour vous aider, voici une compilation d'articles qui nous a servi à faire ce tutoriel...
Lien : http://goo.gl/8qTXqo
Lien: http://goo.gl/G7jEBm
Lien: http://goo.gl/J88FUD

SUR NOTRE CD

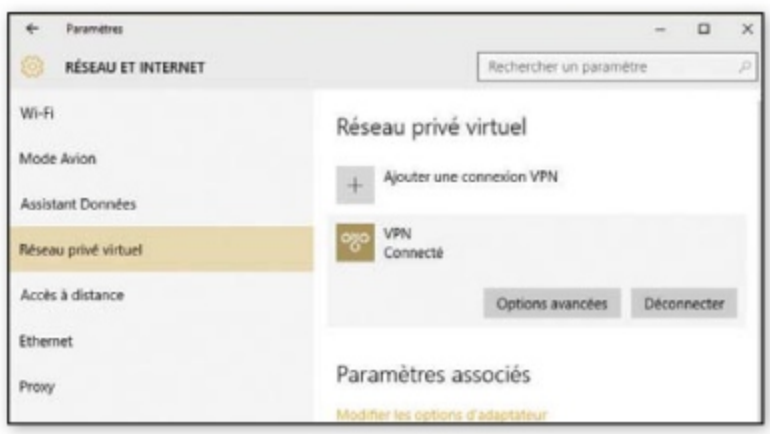
Si vous avez raté les derniers numéros de Pirate Informatique, retrouvez tous les précédents articles concernant le Raspberry Pi sur notre CD : la présentation de l'appareil, la conception d'un Media Center, d'un système de vidéosurveillance, d'une borne d'arcade, d'un récepteur Webradio, d'une radio FM amateur et d'un cloud personnel. Retrouvez aussi notre article du mois dernier avec le comparatif des Raspberry 1 et 2 ainsi que l'installation de Kali Linux !

PAS À PAS

Connexion à votre VPN

01 AVEC WINDOWS

Pour la plupart des versions de Windows, vous devrez passer par le C**entre réseau et partage**. Cliquez sur **Modifier les paramètres de la carte** puis clic droit dans **Connexions entrantes**. Windows 10 nous mâche le travail en proposant directement un menu VPN dans la zone de notification (la bulle «style BD» en bas à droite). Faites **Ajouter une connexion VPN** et remplissez les champs.



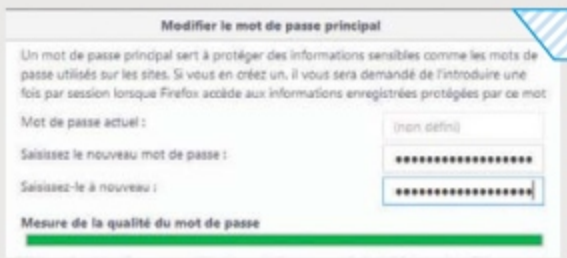
02 AVEC ANDROID

Sous Android ou CyanogenMod, vous pouvez aussi paramétrer les données de votre VPN pour vous y connecter en WiFi ou en 3G. Il faudra aller dans **Paramètres>Plus...>VPN** et faire +. Ici, mettez les diverses informations de connexion: PPTP, DNS éventuel et validez. Vos identifiants vous seront demandés lors de la première connexion.

SECURE LOGIN : AUTHENTIFICATION FACILE AVEC FIREFOX

De plus en plus de logiciels indésirables utilisent des moyens détournés pour vous mener la vie dure. Même armé d'un antivirus et d'un pare-feu correctement configuré, il arrive que des processus activent des redirections au niveau de votre navigateur pour afficher de la publicité, détourner la page de démarrage ou installer des barres d'outils....

Secure Login est une extension Firefox permettant d'améliorer les fonctionnalités du gestionnaire de mots de passe de Firefox. Une fois installée vous pourrez vous authentifier sur un site en un clic, même si vous disposer de plusieurs comptes sur un même site. Il est possible de voir si les identifiants sont enregistrés avec un code couleur. D'ailleurs Secure Login fait aussi office de protection contre le phishing puisque les identifiants ne se chargeront pas s'il s'agit d'un site frauduleux. En cochant l'option adéquate, vous pourrez même vous connecter directement depuis le marque-page. Si vous utilisez Firefox (qui ne vient pas d'un grand groupe américain, mais d'une fondation à but non lucratif), cette extension est absolument indispensable.



Si vous utilisez la fonction Mots de passe enregistrés de Firefox, n'oubliez pas de définir un Mot de passe principal dans Options>Sécurité. Ce sésame général vous donnera accès à tous les autres. Secure Login ajoute un peu plus d'ergonomie.

PAS À PAS

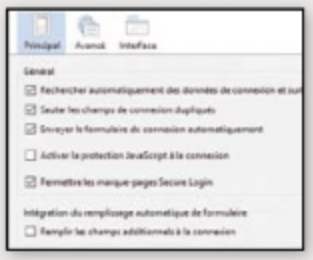
Secure Login en 3 étapes

SECURE LOGIN
OÙ LE TROUVER ? : **https://goo.gl/xEVnqc**
DIFFICULTÉ :

01 LES OPTIONS

Sur le site, faites **+ Add to Firefox** puis **Installer** et enfin **Redémarrer maintenant**. Un nouveau bouton devrait apparaître dans la barre d'outils en haut à droite. Faites un clic droit dans ce dernier et choisissez **Options**. Ici, vous aurez l'onglet **Principal** qui vous permettra de paramétrer un code couleur : si Firefox connaît les identifiants, vous verrez les champs de formulaire entourés d'orange par exemple (pratique si vous avez par exemple oublié que vous aviez déjà un compte).

02 UNE PROTECTION CONTRE LES FAILLES XSS



Dans le même onglet, on trouve aussi la protection JavaScript pour empêcher les vols de mots de passe par XSS et la fonction permettant de s'authentifier depuis les marque-pages. Dans **Avancé**, on pourra ajouter des sons lorsque les identifiants ont été trouvés ou quand vous vous connectez avec succès. Enfin dans **Interface**, on pourra paramétrer un **Raccourci clavier** et définir l'endroit où vous désirez le bouton Secure Login.

03 AUTHENTIFICATION EN UN CLIC !

Faites le test et lancez une page ou un service Internet sur lequel vous êtes enregistré. Sur la page de connexion, faites un clic sur le bouton ou utilisez le raccourci clavier que vous avez paramétré. Et voilà, vous êtes loggé ! Si vous avez activé l'option des marque-pages Secure Login, faites un clic droit dans le bouton et enregistrez votre page comme un favori.

NOUVEAU !

INSCRIVEZ-VOUS GRATUITEMENT !

Le mailing-list officielle de *Pirate Informatique* et des *Dossiers du Pirate*

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...

TROIS BONNES RAISONS DE S'INSCRIRE :

1. Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
2. Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
3. Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

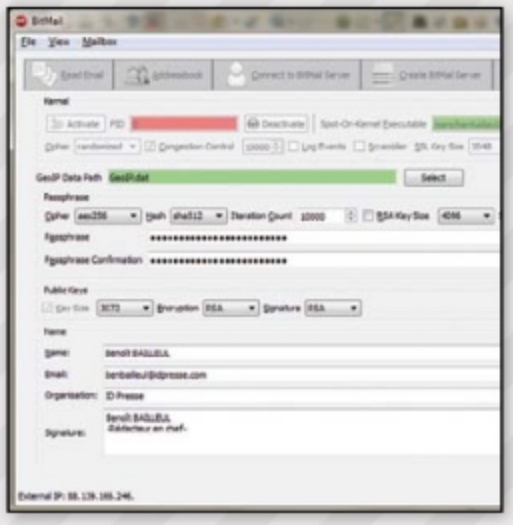
Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

#1 Des messages cryptés

AVEC BITMAIL

Dans notre précédent numéro de *Pirate Informatique* nous vous avions déjà parlé de BitMessage, un logiciel de messagerie (instantanée et e-mail) permettant des échanges chiffrés sans connaissances particulières ou mises en place complexes. BitMail se présente comme une alternative. Le but est d'envoyer des messages qui, même s'ils étaient interceptés, ne pourraient être déchiffrés. Il s'agit pour les citoyens lambda de protéger leur vie privée et pour les professionnels d'éviter



l'espionnage industriel par exemple. Un peu plus difficile à prendre en main que son homologue, BitMail est par contre très complet au niveau des réglages (choix de l'algorithme, du type de hash, etc.)

Lien: **http://sourceforge.net/projects/bitmail**

#2 Des recherches ciblées

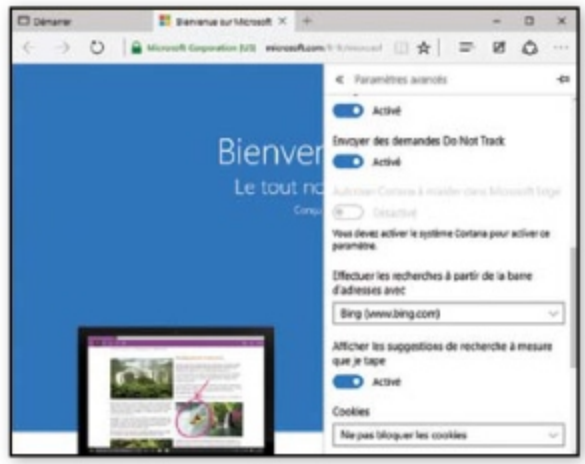
AVEC QWANT

Dans notre précédent numéro, nous vous avions présenté Qwant, un moteur de recherches respectueux de la vie privée, qui ne mémorise pas les recherches et ne fouille pas dans l'historique. Notre article est malheureusement sorti trop tôt pour parler de la nouvelle fonctionnalité de Qwant : les Qwick's. Il s'agit d'une méthode permettant d'effectuer une recherche directement «à l'intérieur» d'un site internet. En ajoutant **&** suivi du nom du site ciblé, vous accédez directement au résultat. Par exemple **Eminem &w** vous donnera directement la page Wikipédia du rappeur. Ce genre de raccourci existe pour des centaines de sites : Facebook (**&fb**), Twitter (**&tw**), Le Bon Coin (**&lbc**), etc. Vous trouverez la liste complète en suivant notre lien et il est même possible de remplir un formulaire pour demander d'ajouter le vôtre !

Lien: **www.qwant.com/qwick**

#3 Faire la guerre aux mouchards

AVEC EDGE ET DO NOT TRACK



Comme vous le savez, les sites marchands (et les autres) scrutent vos petites habitudes de surf, vos recherches et ce que vous achetez. Le but est de vous proposer des produits qui pourraient vous intéresser ou au pire, de refiler les infos à d'autres sites. La fonctionnalité Do Not Track du nouveau navigateur intégré à Windows 10 permet de notifier aux différents sites que vous ne voulez pas être «traqué». Libre à eux de respecter ou non cette volonté... Pour activer cette fonction, ouvrez Edge, cliquez sur les trois petits points en haut à droite puis sélectionnez **Paramètres** > **Afficher les paramètres avancés** puis positionnez **Envoyer des demandes Do Not Track** sur **Activé**.

#4 Contourner la censure

AVEC PSIPHON

Disponible sous Windows et Android, Psiphon fonctionne un peu comme Tor même si la philosophie est légèrement différente puisqu'il est possible de faire passer uniquement certains logiciels ou protocoles dans les tuyaux. Attention, il s'agit plus de contourner la censure que d'une vraie solution d'anonymat puisque même si elles sont chiffrées, les données transitent par des serveurs de confiance gérés par la société canadienne derrière le logiciel. Si vous êtes déjà dans un pays où le Net est contrôlé, vous pouvez demander que le logiciel vous soit envoyé par e-mail...

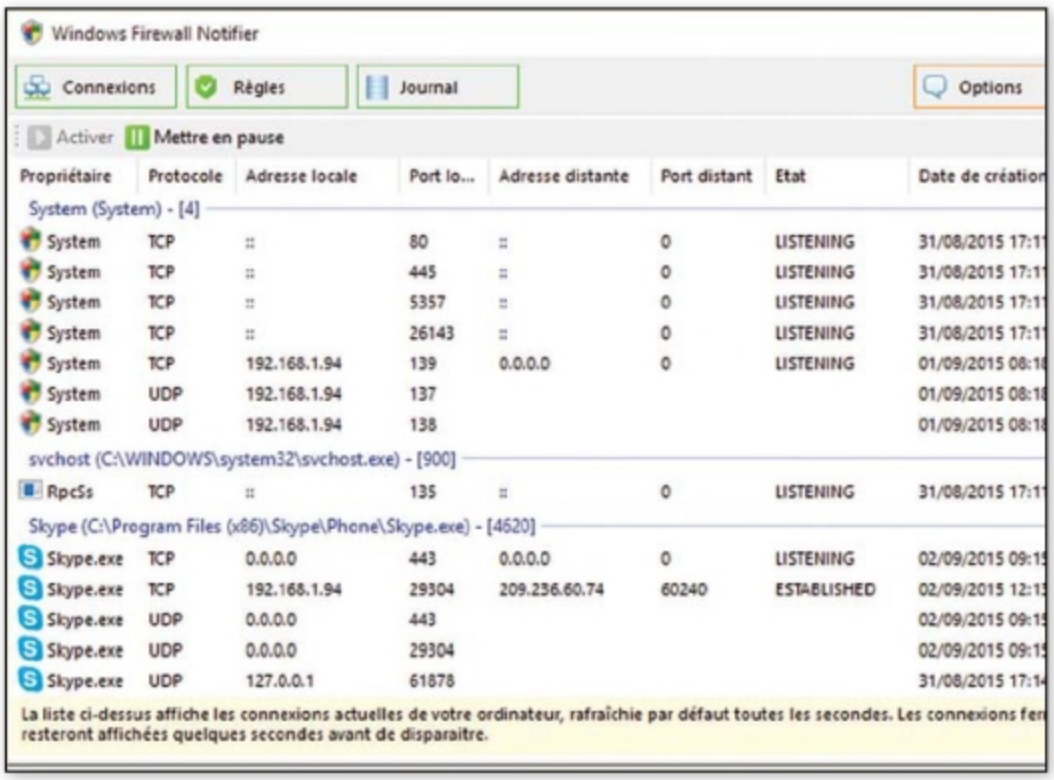
Lien: **https://psiphon.ca/fr**

#5 Un meilleur pare-feu

avec Windows Firewall Notifier

Windows Firewall Notifier est le complément idéal du pare-feu de Windows. Comme TinyWall (*Pirate Informatique* n°15), il active le filtrage par défaut des connexions sortantes. Dès qu'une connexion est détectée comme non autorisée, plusieurs choix s'offrent alors à vous : autorisation temporaire de l'application, création d'une règle de connexion spécifique ou blocage définitif. Windows Firewall Notifier prend peu de ressources et améliore grandement l'efficacité du pare-feu. Après le téléchargement, lisez le fichier lisez-moi.txt pour savoir comment l'utiliser...

Lien: **https://wfn.codeplex.com**

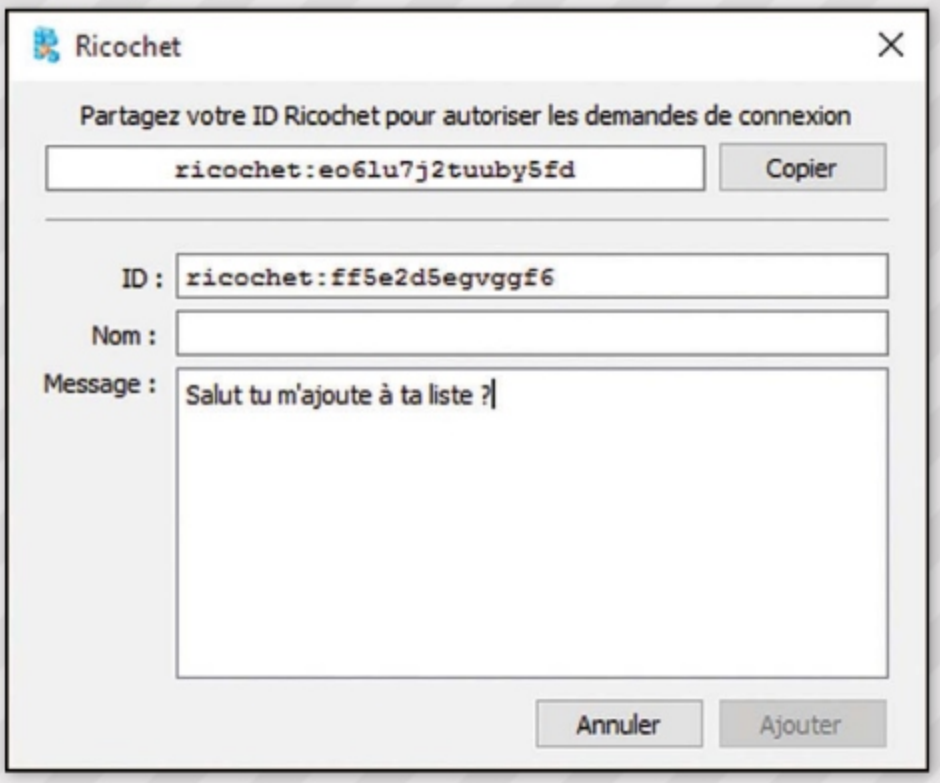


#6 Des conversations décentralisées

avec Ricochet

Ricochet est un logiciel de messagerie instantanée qui fonctionne avec le réseau Tor. Comme TorChat, vous pouvez discuter avec vos amis sans pour autant révéler votre emplacement géographique. Les différents intervenants disposent tous d'une adresse du type **ricochet:8x6jdgst52d9sraf** qu'il faudra partager pour être joignable. Dès le premier lancement, un assistant vous aidera à paramétrer la connexion en fonction de votre profil (utilisation d'un proxy, etc.) Attention le logiciel est encore en phase de test.

Lien: **https://goo.gl/lM3Pah**



#7 Un Webmail chiffré

avec Mailvelope

Compatible avec des services comme Gmail, Yahoo ou Outlook.com, Mailvelope est une extension pour Chrome ou Firefox permettant de chiffrer le contenu de vos e-mails avec OpenPGP. Une fois installée, Mailvelope va faire apparaître des menus dans votre interface Web

pour gérer vos clés publiques et privées: génération, import/export, stockage, etc. Le moyen le plus simple si vous voulez vous mettre au chiffrement. Seul point noir : Mailvelope ne gère pas les pièces jointes.

Lien: **www.mailvelope.com**

0101001010010101010010000111010101010101101010100010010

PRÉSENTATION DE KALI LINUX 2

Dans notre précédent numéro, nous avons vu comment installer Kali Linux sur un Raspberry Pi. Le hasard fait bien les choses puisque la version 2 de cette distribution est sortie juste après la parution du magazine. Nous allons donc voir comment profiter de ce système et faire connaissance avec les logiciels qu'il contient.

LEXIQUE

KALI LINUX : Anciennement BackTrack, Kali Linux est une distribution spécialisée dans l'audit réseau, le pentesting et plus généralement le hacking. Parmi les outils inclus, vous trouverez des logiciels pour cracker des mots de passe, des logiciels de rétro-engineering, des modules pour pénétrer des réseaux sans fil, mais aussi le langage Arduino ou CHIRP (radioamateur). Une vraie mine d'or pour les hackers débutants ou confirmés.

***BOOT :** Le boot est la procédure de démarrage d'un ordinateur. Généralement, le PC va «booter» sur le disque dur principal pour charger le système, mais il est possible de booter sur un DVD ou une clé USB pour installer un autre système, lancer un Live CD ou tenter une restauration. On parle de dual boot lorsque deux systèmes sont installés et que le PC vous donne la possibilité de charger l'un ou l'autre (Windows ou Kali par exemple).

***LIVE CD :** Un live CD est un CD ou un DVD qui contient un système ne nécessitant pas d'installation sur un disque dur. Idéal pour commencer un apprentissage sous Linux sans avoir à partitionner son disque et risquer une erreur de manipulation. Dans notre exemple, le Live CD Kali Linux est inclus de base dans le fichier ISO.

***PENTESTING :** Mot valise réunissant «penetration» et «testing». Il s'agit de tester les forces et faiblesses d'un ordinateur, d'un réseau, d'un site ou d'une base de données avec des logiciels spécialisés. Bien sûr, ces derniers peuvent être utilisés à des fins moins nobles.

Depuis 2013 et son changement de nom (de BackTrack à Kali Linux), cette distribution basée sur Debian n'avait pas connu de bouleversement majeur hormis l'ajout du logiciel Cryptsetup permettant d'autodétruire vos propres données (voir Pirate Informatique n°24). Kali 2 propose une interface plus conviviale (Gnome 3), fonctionne sur le noyau Linux 4.0, ajoute un outil de capture vidéo et d'autres logiciels indispensables aux hackers en tout genre : les dernières versions de John the Ripper, Aircrack, BeEF et Maltego.

A CHACUN SA VERSION

Notons aussi la possibilité de télécharger plusieurs versions de Kali Linux en fonction des appareils sur lesquels vous voulez l'installer. Quel que soit le matériel dont vous disposez, il y aura une manière de profiter de Kali Linux. Dans un deuxième temps, nous ferons la présentation des outils les plus emblématiques...

DE KALI 1 À KALI 2

Les utilisateurs de Kali en version 1.0 peuvent mettre à jour leur version en allant dans le fichier **/etc/apt/sources.list** puis en ajoutant ces deux sources dans l'éditeur de texte:

deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security sana/updates main contrib non-free

Lancez un terminal et faites:

apt-get update
apt-get dist-upgrade
reboot

À chacun son Kali !

CE QU'IL VOUS FAUT

KALI LINUX 2

OÙ LE TROUVER ? :
www.kali.org/downloads

DIFFICULTÉ : ☠☠☠

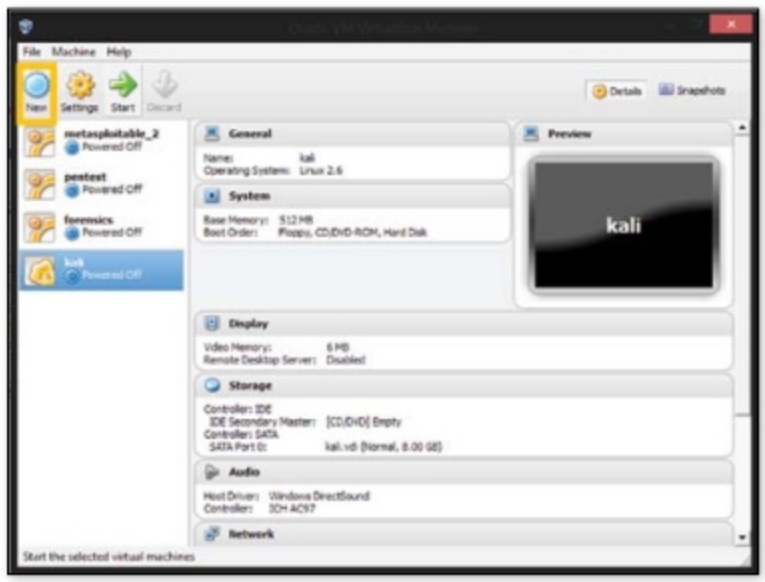
01 INSTALLATION OU LIVECD

Le plus simple pour utiliser Kali Linux est de l'installer sur PC bien sûr. Il existe des versions pour processeur 32 et 64 ainsi que différentes «tailles». Les images de plus de 3 Go contiennent tous les packs et logiciels tandis que les versions Light et mini (respectivement 800 et 28 Mo) permettent une installation sur

mesure. Ce sera à vous de vous confectionner votre propre Kali. Si vous n'êtes pas très à l'aise avec le partitionnement et le dual boot ou si vous souhaitez juste jeter un coup d'œil, il est possible d'utiliser l'option LiveCD. L'OS se chargera dans la RAM sans installation.

02 SUR MACHINE VIRTUELLE

Kali Linux propose aussi des versions pour machine virtuelle VMWare et VirtualBox. Ces deux logiciels sous Windows permettent de virtualiser l'environnement de Kali Linux depuis une image



disque. Cette méthode a deux avantages : vous n'avez pas besoin d'installer quoi que ce soit et le travail dans ces machines virtuelles permet d'utiliser au mieux les ressources de votre PC, mémoire vive et disque dur. Pour les utilisateurs d'autres versions de Linux, on trouve aussi des versions pour le logiciel Docker.

03 SUR APPAREILS «EXOTIQUES»

Kali Linux est également utilisable sur des appareils un peu plus exotiques. Comme nous l'avons vu dans *Pirate Informatique n°26*, il est possible de l'installer sur Rapsberry Pi, mais aussi sur d'autres machines intégrant un processeur ARM : Cubieboard, Chromebook, Odroid, etc.
Et si vous avez un Nexus (5, 6, 7, 9 et 10) ou un OnePlus One, vous pouvez déployer la version NetHunter de Kali : une distribution spécialement compilée pour tirer le meilleur de ces appareils mobiles.

L'INTERFACE DE KALI 2

Dans sa version standard, Kali Linux 2 utilisera l'interface graphique Gnome 3. Bien qu'un peu gourmande en ressource, celle-ci est très jolie. Voyons comment tout cela est organisé...

QUELLES APPLIS SUR KALI ?

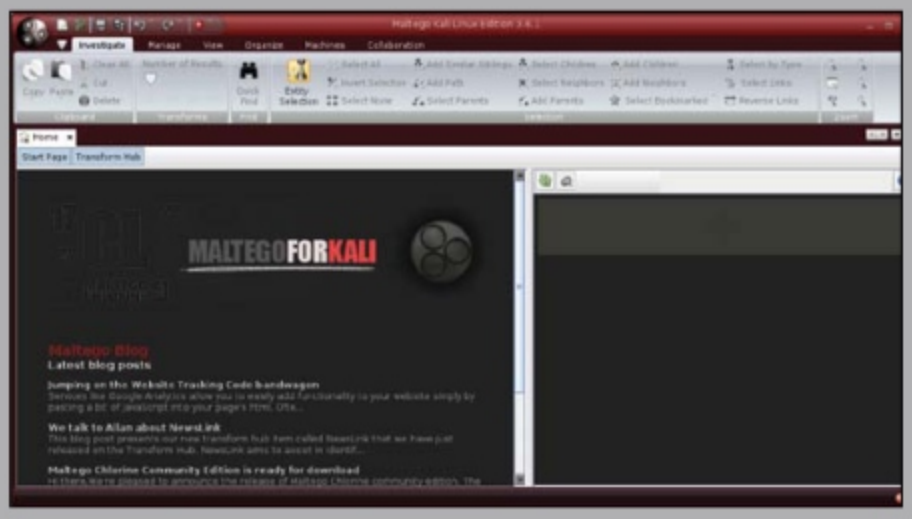
Bien sûr, cette petite liste de programmes est loin d'être exhaustive, mais cela nous permettra de faire connaissance avec les plus emblématiques. Nous en profiterons aussi pour croiser de vieilles connaissances...

1 JOHN THE RIPPER ET JOHNNY

John the Ripper est un logiciel de cassage de mot de passe: un «crack» du crack. Il dispose de plusieurs cordes à son arc: permutation de caractères, brute force, attaque par dictionnaire, etc. Le logiciel est en ligne de commande, mais pour ceux qui sont allergiques, Johnny est l'interface graphique qui se greffe dessus. Si John The Ripper vous intéresse, nous avons réalisé une série d'articles sur la version Windows dans *Pirate Informatique* n°19 et 20.

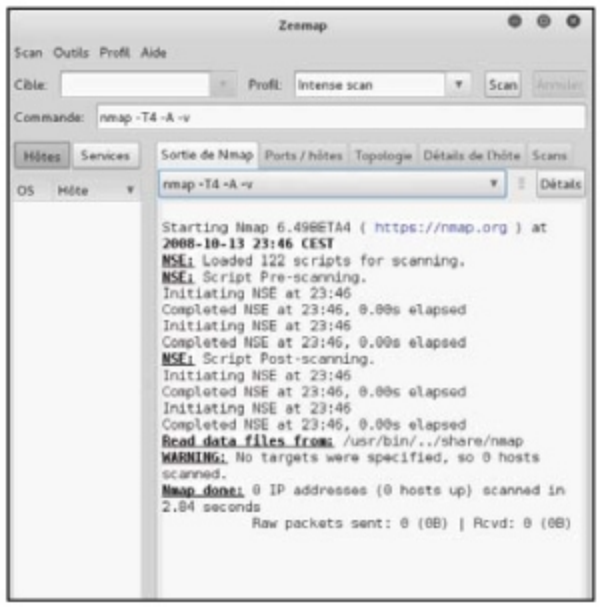
2 MALTEGO

Conçu pour recouper des informations numériques venues des 4 coins du Web, Maltego est une plate-forme open source de renseignements. Le programme va piocher des informations à la demande dans ses serveurs et va les afficher sous forme de diagramme. Tout est passé en revue: Facebook, LinkedIn, Twitter, adresse e-mail, numéro de téléphone, données de géolocalisation, etc. Diablement efficace pour trouver des informations personnelles sur des individus, des sites ou des sociétés, Maltego pourra vous aider pour une embauche par exemple ou pour du social engineering. Si Maltego vous intéresse, nous avons réalisé un article sur la version Windows dans *Pirate Informatique* n°23.



3 NMAP ET ZENMAP

ZenMap est l'interface graphique de Nmap, un logiciel permettant de mapper un réseau: scan des ports, noms des services utilisés par ces derniers, détection des versions des logiciels et systèmes, tests de vulnérabilité, exploitation des faiblesses, etc. Même les systèmes derrière des pare-feux ou des filtres à IP ne sont pas à l'abri. Un logiciel à ne pas mettre entre toutes les mains.

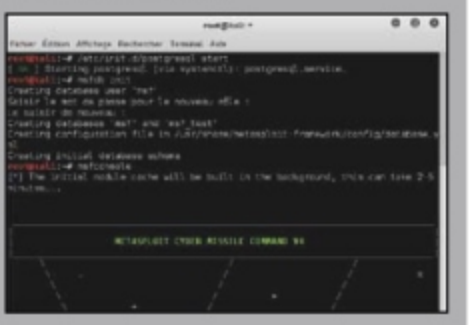


4 RAINBOWCRACK

RainbowCrack est un logiciel de crack de mots de passe qui se distingue des autres puisqu'au lieu d'utiliser les méthodes habituelles (dictionnaire, brute force) il se sert de rainbow table (littéralement table arc-en-ciel) pour le retrouver. Pour faire simple, il s'agit de retrouver un mot de passe en utilisant des tables mathématiques et des empreintes numériques (nous y reviendrons dans un prochain numéro). Pour accélérer la recherche, le logiciel utilise la puissance du GPU en plus du CPU.

5 METASPLOIT ET ARMITAGE

Armitage est l'interface graphique pour Metasploit. Ce dernier est une plate-forme fournissant des renseignements sur les vulnérabilités des systèmes informatiques: les fameux «exploits». Ce type d'informations peuvent être utilisées par les administrateurs pour tester la vulnérabilité de leurs systèmes afin de les rendre «étanches». Au programme: sniffing, backdooring, keylogging et des centaines d'autres fonctions impossibles à lister ici.



6 BURP SUITE, WIRESHARK ET BEEF

Ces trois-là n'ont rien à voir ensemble, mais nous nous devions d'en parler. Burp Suite est une solution de pentesting pour les applications Web: attaque Man-in-the-middle depuis un proxy, Web crawler, etc. Wireshark analyse les protocoles et inspecte les paquets de données qui transitent (avec capture à la volée et analyse hors ligne). Enfin, BeEF est spécialisé dans les failles cross-site scripting (XSS). Il s'agit, ici, de polluer un site avec des bouts de code malicieux pour que le navigateur de l'utilisateur interprète ce code et contamine le système.

DANS LE PROCHAIN NUMÉRO, NOUS VERRONS UN CAS PRATIQUE DE PENTESTING. ET COMME IL Y A DES CENTAINES DE CAS DE FIGURE DIFFÉRENTS, C'EST À VOUS DE DÉCIDER CE QUE NOUS ABORDERONS : TENTATIVE D'INTRUSION DANS UN RÉSEAU WIFI, FAILLE XSS, INJECTION MYSQL ? ENVOYEZ VOS IDÉES À **BENBAILLEUL@IDPRESSE.COM !**

DÉBLOQUEZ N'IMPORTE QUEL PDF

DANS NOTRE CD !

Si vous avez raté certains des derniers numéros et que vous voulez lire les deux premières parties de ce dossier, sachez que les PDF des articles se trouvent sur notre CD !

-PARTIE 3-

Dans les deux précédentes parties consacrées aux mots de passe du format PDF, nous avons vu les différences entre les restrictions, comment les appliquer sur un document et la méthode de crack par dictionnaire pour retrouver le mot de passe d'ouverture. Dans cette dernière partie, nous verrons la méthode par brute force.

LEXIQUE

***CRACK :**
Cracker un mot de passe c'est le «casser», réussir à l'obtenir en utilisant ses méninges et un logiciel (eh oui, il faut les deux !)

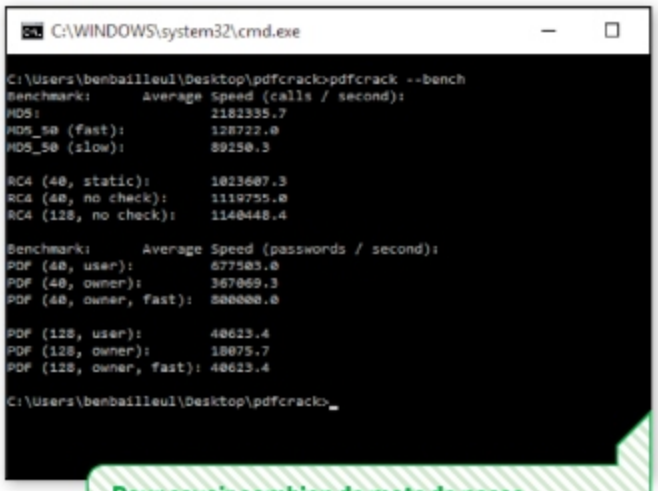
***DICTIONNAIRE :**
Il s'agit d'une liste de mots dont le logiciel va se servir en espérant trouver son bonheur dedans. Il existe de nombreux dictionnaires sur Internet et dans toutes les langues.

***BRUTE FORCE :** Méthode de récupération de mot de passe qui consiste à essayer toutes les combinaisons de caractères pour tomber sur la bonne entrée. Le logiciel va essayer toutes les combinaisons de lettres, de chiffres et autres caractères pour arriver à ses fins. Un mot de passe comme coucou peut être retrouvé en quelques heures, mais pour **dJer7(ghSg(^#H54 *DùDCµ,cj`/ fd,c çlcnb_**, c'est mission impossible (à moins d'avoir un super calculateur ou quelques siècles devant soi...)

Nous allons continuer avec le logiciel PDFCrack du précédent numéro. Dans ce dernier exemple de tentative de récupération d'un mot de passe de fichier PDF, vous n'aurez pas besoin de fichier avec des mots de passe puisque la méthode brute force ne consiste pas à trouver le sésame parmi une liste. Il s'agit ici d'essayer le plus grand nombre de combinaison possible de caractères pour trouver le bon mot de passe.

LE DERNIER ESPOIR

Pour nos tests, nous avons donc créé 3 fichiers PDF avec des mots de passe d'ouverture plus ou moins complexes pour vous montrer avec quelle facilité (ou non) nous avons récupéré ces mots de passe d'ouverture avec cette méthode. Le problème avec l'attaque par dictionnaire, c'est que même avec une liste de mots gigantesque, vous ne trouverez jamais le sésame s'il n'est pas dans votre dico.txt (voir les précédents articles). La méthode brute force est plus laborieuse, mais elle peut retrouver des mots de passe assez facilement à condition qu'ils soient «simples». Si l'attaque par dictionnaire n'a rien donné, la brute force est la dernière solution.



Pour savoir combien de mots de passe votre PC peut essayer à la seconde, tapez pdfcrack --bench. Regardez ensuite à la ligne PDF (128, user). Sur notre ordinateur bas de gamme, PDFCrack peut tenter plus de 40 000 sésames à la seconde !

Brute force avec PDFCrack

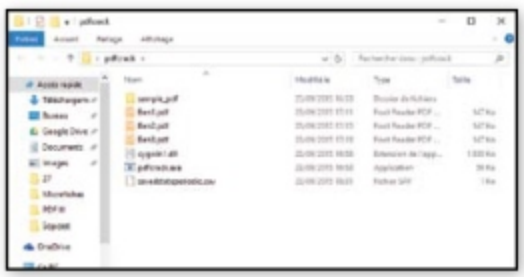
CE QU'IL VOUS FAUT

PDFCRACK

OÙ LE TROUVER ? :
http://goo.gl/VkYg03

DIFFICULTÉ :

01 NOS FICHIERS TEST



Précisons avant de commencer que dans notre exemple, les fichiers PDF à cracker s'appellent **Ben1**, **Ben2** et **Ben3**. Ils ont comme mot de passe **toto**, **delopa** et **Mx3^Zi_kL28**. Maintenez la pression sur la touche **Maj** du clavier, faites un clic droit dans le dossier contenant vos fichiers (et PDFCrack) et sélectionnez **Ouvrir une fenêtre de commandes ici**.

02 EXEMPLE D'UN MOT DE PASSE BIDON

Tapez **pdfcrack -f Ben1.pdf** et PDFCrack commencera à essayer tous les caractères, puis les mots de passe avec deux caractères, puis trois, etc. Il ne lui a fallu qu'une minute pour retrouver **toto**. C'est le temps qu'il faut pour un mot de passe de 4 caractères qui ne comprend que des lettres latines minuscules. De la même manière, le mot de passe de **Ben2** ne comprend que ce type de caractère, mais est plus long de deux unités.

```
C:\WINDOWS\system32\cmd.exe
O: 3c8d04adb8df0c5529f742bcbb24bdfe60be484e36b208018b0aa5201046ec73
Average Speed: 38857.6 w/s. Current Word: 'PGX'
Average Speed: 39134.6 w/s. Current Word: 'QAMa'
Average Speed: 39272.6 w/s. Current Word: 'ZF8b'
Average Speed: 38961.0 w/s. Current Word: '0lqc'
Average Speed: 38781.0 w/s. Current Word: 'vNed'
Average Speed: 39038.0 w/s. Current Word: 'Jz3d'
Successfully saved progress to savedstateperiodic.sav
Average Speed: 38556.4 w/s. Current Word: '7IRe'
Average Speed: 39070.2 w/s. Current Word: 'AyGf'
Average Speed: 39238.8 w/s. Current Word: '0Avg'
Average Speed: 38856.2 w/s. Current Word: 'zmjh'
Average Speed: 39004.2 w/s. Current Word: '4R0h'
Average Speed: 39038.2 w/s. Current Word: 'jEXi'
Successfully saved progress to savedstateperiodic.sav
Average Speed: 38902.0 w/s. Current Word: 'zfMj'
Average Speed: 39132.2 w/s. Current Word: '0BAk'
Average Speed: 39291.6 w/s. Current Word: '4fQl'
```

03 PLUS COMPLIQUÉ...

Tapez **pdfcrack -f Ben2.pdf** et allez-vous faire un café car ici, ce sera plus long. Nous avons choisi **delopa** car il y a très peu de chance que ce dernier se retrouve dans un dictionnaire (cette technique aurait alors échoué). Par contre avec seulement 6 caractères minuscules, PDFCrack n'a mis que deux heures à le retrouver. Nous ne le rappellerons jamais assez: alternez les capitales, les minuscules, les chiffres et les caractères spéciaux!

```
C:\WINDOWS\system32\cmd.exe
Average Speed: 37829.4 w/s. Current Word: 'hfymza'
Average Speed: 37905.4 w/s. Current Word: 'evnrea'
Average Speed: 37740.0 w/s. Current Word: 'wamgea'
Successfully saved progress to savedstateperiodic.sav
Average Speed: 37701.6 w/s. Current Word: 'evsnea'
Average Speed: 37745.2 w/s. Current Word: 'wzyqra'
Average Speed: 37698.0 w/s. Current Word: 'qvvwra'
Average Speed: 37462.0 w/s. Current Word: 'jngyta'
Average Speed: 37658.4 w/s. Current Word: 'jfijta'
Average Speed: 37896.2 w/s. Current Word: 'fvxaya'
Successfully saved progress to savedstateperiodic.sav
Average Speed: 37557.6 w/s. Current Word: 'rlfsya'
Average Speed: 36609.8 w/s. Current Word: 'ddbxya'
Average Speed: 37546.4 w/s. Current Word: 'btjuua'
Average Speed: 37454.6 w/s. Current Word: 'myikua'
Average Speed: 37867.6 w/s. Current Word: 'nizeia'
Average Speed: 37654.4 w/s. Current Word: 'yxmdia'
Successfully saved progress to savedstateperiodic.sav
Average Speed: 37513.0 w/s. Current Word: 'uisvia'
Average Speed: 36999.4 w/s. Current Word: 'fbbioa'
Average Speed: 37612.2 w/s. Current Word: 'jrkloa'
Average Speed: 37258.0 w/s. Current Word: 'jlurpa'
```

04 PRESQUE IMPOSSIBLE !

Justement, **Ben3** est à ce niveau très costaud. **Mx3^Zi_kL28** contient 11 caractères de plusieurs types. Nous aurions bien essayé de le cracker, mais il nous faudrait des millions d'années avec ce PC et ce logiciel. Selon le site howsecureismypassword.net,avec un logiciel et du matériel permettant d'essayer 4 milliards de mots de passe à la seconde (soit 100 000 fois plus puissant que ce que nous avons), il faudrait 4000 ans. Vous êtes tranquille avec ce dernier, mais dans le cas d'un mot de passe plus faible, il est quand même possible d'affiner la recherche pour gagner du temps...

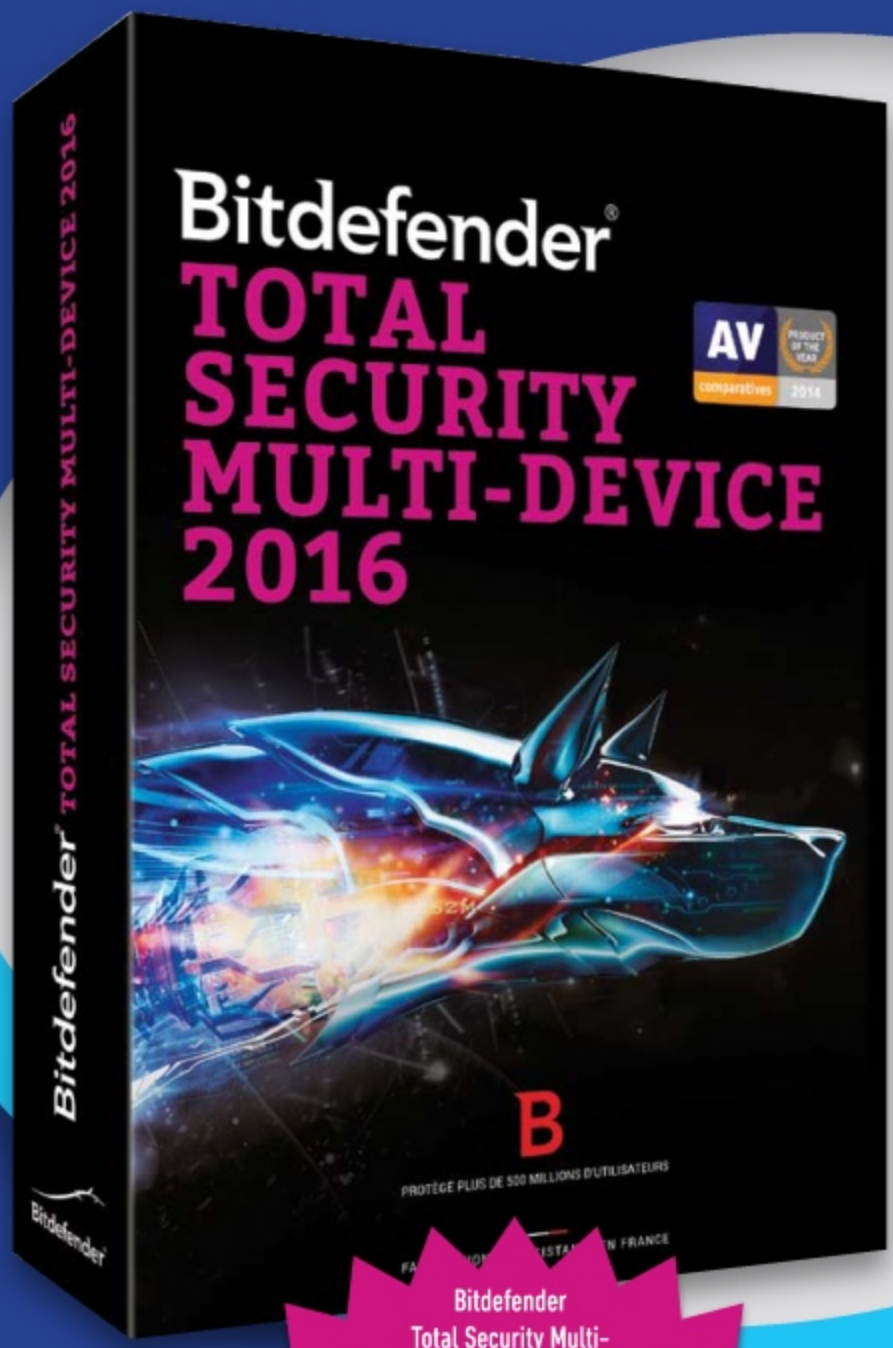
05 AMÉLIOREZ VOTRE RECHERCHE

On peut par exemple imaginer que vous souhaitiez retrouver un mot de passe en vous souvenant que ce dernier fait 6 ou 7 caractères, il faudrait taper **pdfcrack -f Ben2.pdf –minpw=6 –maxpw=8**. Pour **Ben2** il ne nous a fallu que 12 minutes au lieu de 2 heures pour trouver **delopa**! Et si vous vous rappelez que votre mot de passe n'est composé que de minuscules, utilisez la commande **--charset=STRING**. À la place de **STRING**, il faudra mettre les caractères que vous souhaitez voir intégrés à la recherche. Bien sûr, vous pouvez cumuler **minpw**, **maxpw** et **charset**. Notons enfin que la version Linux du logiciel permet de cumuler la puissance de plusieurs PC.

```
pdfcrack -f Ben2.pdf --charset=azertyuiopqsdfghjklmwxcvbn
C:\Users\benbailleul\Desktop\pdfcrack>pdfcrack -f Ben2.pdf --charset=azertyuiopq
sdfghjklmwxcvbn
PDF version 1.4
Security Handler: Standard
V: 2
R: 3
P: -1028
Length: 128
Encrypted Metadata: True
FileID: a4244bb7d9ab92a293b6d90c0d50a9d6
U: eb38a63b09d62bcb5eaa367dda3da2ed00000000000000000000000000000000
O: 790cc7b24955ebf1f628cc104e3fb990eef26cc0221ed0c7ea1d0cccdb96dc5d
Average Speed: 37849.8 w/s. Current Word: 'wvlp'
Average Speed: 37589.8 w/s. Current Word: 'hbqw'
Average Speed: 37606.0 w/s. Current Word: 'ferya'
Average Speed: 37822.0 w/s. Current Word: 'nxcha'
Average Speed: 37671.4 w/s. Current Word: 'ddhaz'
Average Speed: 37757.2 w/s. Current Word: 'dmosz'
Successfully saved progress to savedstateperiodic.sav
Average Speed: 37688.4 w/s. Current Word: 'ufzcz'
Average Speed: 37613.4 w/s. Current Word: 'hlmuo'
Average Speed: 37814.8 w/s. Current Word: 'kqfke'
Average Speed: 37638.6 w/s. Current Word: 'cwyer'
Average Speed: 37732.4 w/s. Current Word: 'evbdr'
```

GRAND CONCOURS

Bitdefender®



Licence de 1 an valable pour 3 utilisateurs et un nombre illimité d'appareils (Windows, Mac OS X et Android)

Bitdefender Total Security Multi-Device 2016 comprend :

- Antivirus, antiphishing et antispyware
- Chiffrement des fichiers
- Antivol
- Antispam
- Contrôle parental
- Pare-feu
- Gestionnaire de mots de passe
- Protection contre les ransomwares
- Protection de la vie privée sur Internet
- Achats en ligne sécurisés

Bitdefender Total Security Multi-Device 2016 est une suite de sécurité complète qui protège tous vos appareils contre les menaces connues et inconnues. Élu «Produit de l'année», Bitdefender est facile à utiliser et n'a aucun impact sur les performances de votre ordinateur. Bitdefender prend automatiquement les meilleures décisions de sécurité, protège vos données, sécurise vos paiements et votre vie privée. Bitdefender Total Security Multi-Device 2016 inclut également un pare-feu bidirectionnel, un contrôle parental, un outil d'optimisation en un clic et une fonction antivol pour vos appareils.

10 LICENCES À GAGNER !

d'une valeur de 59,95 € par licence

Pour participer, il suffit d'envoyer un e-mail à cette adresse :

concours@idpresse.com

N'oubliez pas de mettre **Bitdefender** dans l'objet et c'est tout !

Les gagnants seront tirés au sort parmi cette liste. Ils recevront leur licence par e-mail avec un tutoriel détaillé pour profiter de leur prix.

Attention, vous n'avez que jusqu'au 31 décembre 2015 !

Maelstom : LE NAVIGATEUR DU FUTUR ?

Et si les pages Internet que nous consultions n'étaient pas hébergées sur des serveurs, mais sur les machines de tous les internautes ? C'est le pari un peu fou de Maelstrom, un navigateur expérimental de la société BitTorrent. Explications...

Le principe n'est pas nouveau, car Freenet (voir notre article sur les darknets dans *Pirate Informatique n°24*) propose depuis longtemps un hébergement partagé de ses «freesites» sur différents ordinateurs participant au réseau. Encore en version bêta et ne proposant que très peu de contenu pour le moment, Maelstrom prend cette voie sauf qu'ici les échanges de données entre ordinateurs utilisent la technologie BitTorrent.

ENTREZ DANS LA DANSE !

Vous êtes webmaster et vous souhaiteriez rendre vos sites compatibles avec Maeltrom ? Torrent-web-tools est un projet qui veut réunir différents outils pour créer et «seeder» des sites aux contenus statiques. Pour l'instant seul le script Python Generator.py en fait partie. Ce dernier permet simplement (à condition de connaître les bases du fonctionnement du protocole BitTorrent) de transformer une page Web en lien magnet Torrent. Libre à vous de partager votre création pour que BitTorrent l'ajoute sur la page d'accueil de Maelstrom : **http://goo.gl/Xp4668.**

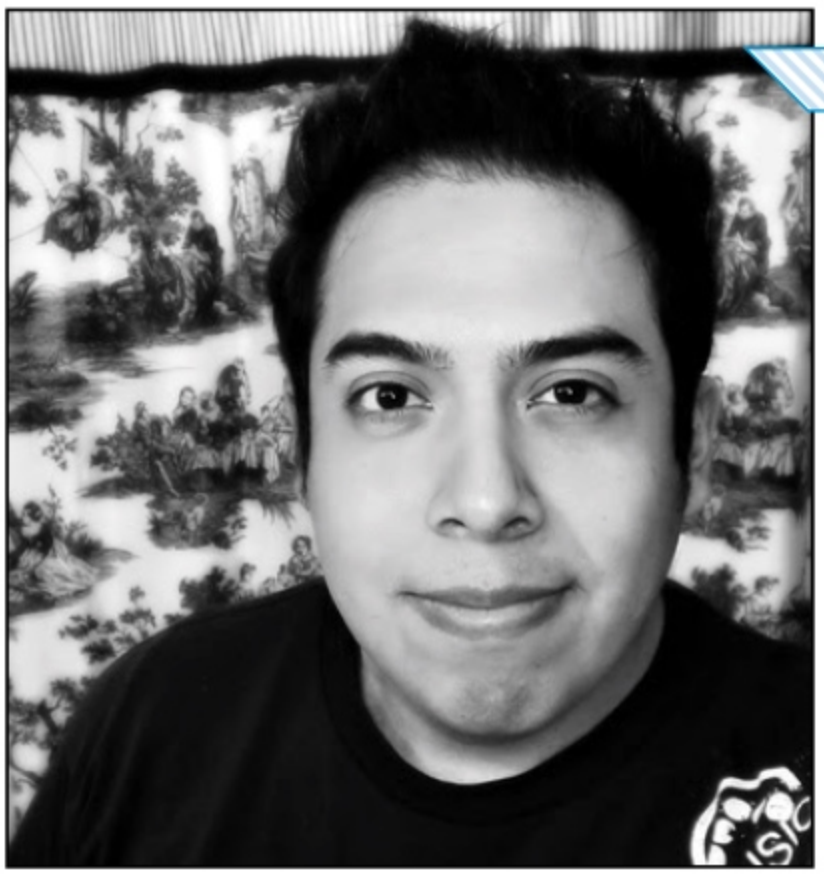
Lien : **https://github.com/bittorrent/torrent-web-tools**

LEXIQUE

***P2P :** Le peer-to-peer, ou «pair-à-pair» en français, est un modèle de réseau informatique où chaque client peut aussi faire office de serveur. Le protocole BitTorrent, très efficace dans le domaine du partage de fichier est un système P2P.

***DÉCENTRALISÉ :** Un réseau décentralisé est un réseau qui ne comporte pas de serveur. Chaque participant est à la fois serveur et client.

***SEED :** C'est un terme du vocabulaire BitTorrent. Un seed (graine en français) est un participant du réseau qui dispose d'un fichier complet et qui le partage avec les autres. Quand il n'y a plus de seed, le .torrent est mort, il est impossible de récupéré le fichier (ou le site, dans le cas de Maelstrom) auquel il est rattaché.



> *«Le but de ce logiciel est de le laisser dans les mains des développeurs et de voir ce qui va en sortir»*
> **Rob Velasquez – Chef de projet Maelstrom**

UN CONCEPT PLUS QU'UNE SOLUTION TANGIBLE

Le but est évidemment d'échapper à la censure. Un pays censure une information ? Un blocage de site ? Un document se retrouve filtré sur le Web ? Maelstrom peut devenir une vraie solution pour contourner ce problème. Ce navigateur peut aussi devenir une solution de choix pour les éditeurs souhaitant rester discrets puisque pour faire un site, vous n'avez pas besoin de partager des données privées, de faire appel à un registrar ou un hébergeur. Encore une fois, c'est ce que proposent déjà les darknets, mais le poids de la société BitTorrent peut devenir un plus pour populariser l'idée. Il ne reste qu'à ajouter le chiffrement. Car Maelstrom ne dispose pas encore de cette sécurité primordiale. Sans elle, le concept pourrait bien se heurter à la dure réalité de l'espionnage et des censures dictatoriales....

TÉLÉCHARGEMENT DE FICHIER ET SURF VIA BITTORRENT

Mais BitTorrent n'oublie pas non plus ses premiers amours : sur Maelstrom, les Torrents sont de la partie ! Les fichiers Torrent ou liens magnets sont directement pris en charge par le navigateur. Vous pouvez donc télécharger directement depuis l'interface. Si vous avez un site statique ou si vous avez envie de créer une page avec des éléments basiques (HTML + quelques images ou autres), il est même possible de les diffuser sous forme de Torrent (voir encadré). En attendant du contenu sympa et novateur, il faudra se contenter des quelques exemples qui sont mis en avant dans le navigateur...

BITTORRENT VEUT TOURNER LA PAGE DU «PIRATAGE»

Depuis que BitTorrent est devenu une société «respectable» elle n'a de cesse de proposer d'autres applications que du téléchargement «bête et méchant» : Sync pour la synchronisation de fichiers (*Pirate Informatique n°22*), Shoot pour le partage de fichiers via mobiles, Bleep pour le tchat multisupport ou Bundle, la plate-forme de téléchargement musical légal. Mais attention, même si la plupart de ces produits mettent en avant leur capacité de chiffrement, ils ne sont pas open source. Dans l'impossibilité d'analyser le code, il est impossible de savoir si ces logiciels comportent des backdoors permettant à «on-ne-sait-qui» de jeter un œil sur ce que vous faites ou sur les fichiers que vous partagez. Maelstrom est donc plus un modèle à suivre qu'une véritable solution de surf anonyme. D'ailleurs, le contenu «compatible» est très limité.

Présentation de Maelstrom

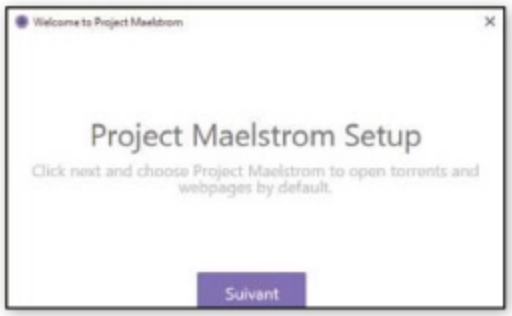
CE QU'IL VOUS FAUT

MAELSTROM

OÙ LE TROUVER ? :
http://project-maelstrom.bittorrent.com

DIFFICULTÉ :

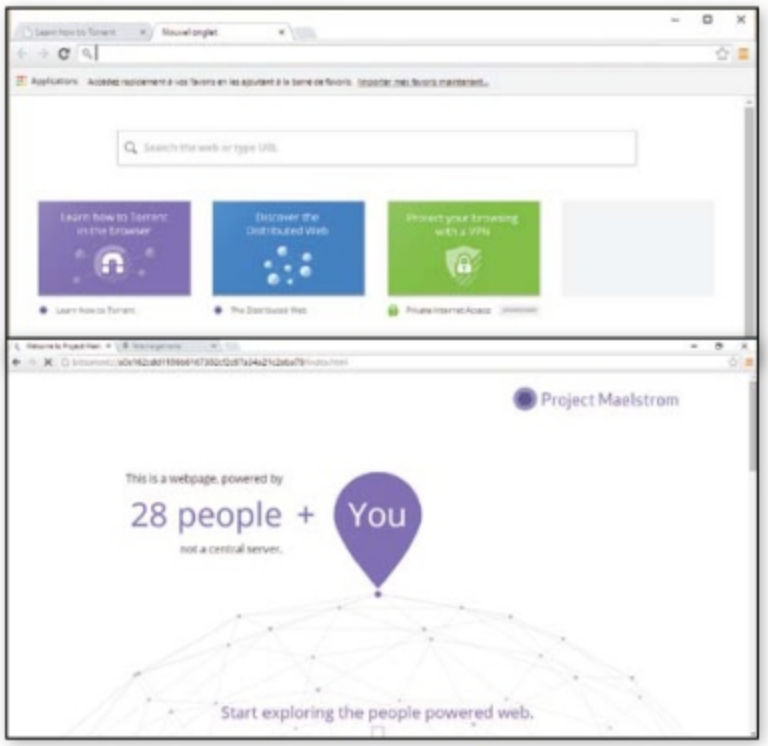
01 LE LANCEMENT



Dès le lancement, vous verrez que l'interface est la même que celle de Chrome. Maelstrom est en fait construit sur Chromium, une version libre de Chrome. Fermez la première fenêtre qui vous invite à faire de Maelstrom votre navigateur et client Torrent par défaut et intéressons-nous à la page d'accueil.

01 PREMIER CONTACT

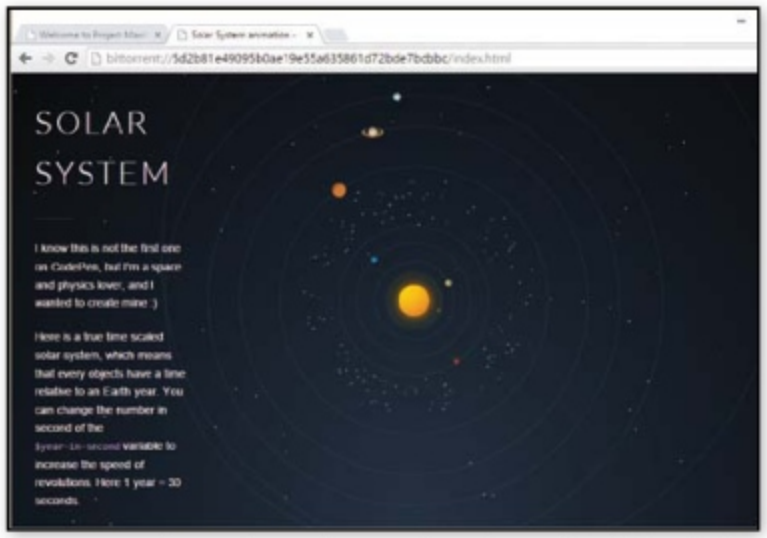
Celle-ci contient des miniatures qui vous proposent d'apprendre à utiliser les capacités de téléchargement, d'utiliser un VPN (c'est une publicité !) et une autre miniature vous invitant à



découvrir des exemples de sites. Cliquez sur **Discover the Distributed Web**. Vous verrez alors le nombre de personnes qui génèrent cette page avec vous et en dessous, des exemples de sites générés avec le protocole BitTorrent.

03 DES EXEMPLES DE SITES PAS TRÈS INTÉRESSANTS

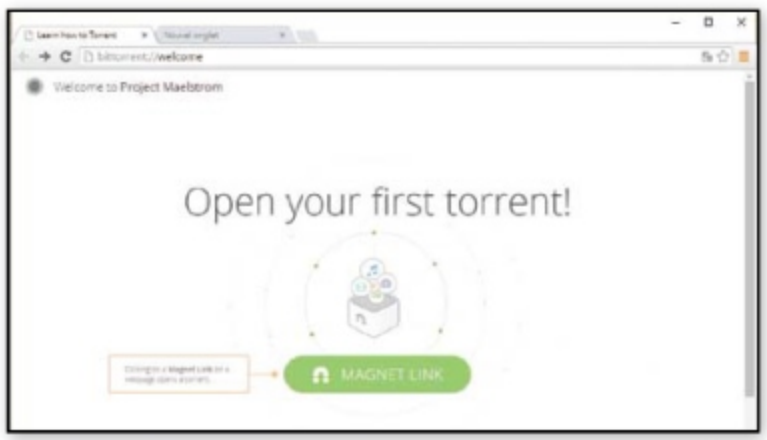
Comme Maelstrom est encore en version bêta, vous ne trouverez pas énormément de pages: un jeu dérivé de Galaga, un système solaire en temps réel assez réussi, un exemple de «to-do list» et un jeu d'échecs sans IA. Rien de bien folichon, mais la technologie se borne uniquement aux sites statiques,

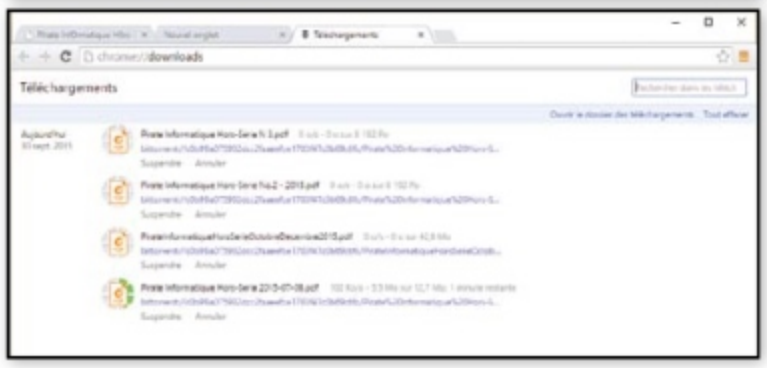


les contenus dynamiques n'ont pas leur place puisqu'il faudrait générer un .torrent à chaque changement de contenu ou modification du site.

04 UN CLIENT TORRENT QUI CHARGE DES SITES

Les choses deviennent plus intéressantes lorsque vous essayez vous-même de placer un fichier .torrent dans le navigateur (faites un glisser-déposer) ou en tentant d'ouvrir un lien magnet. Le fichier se téléchargera directement dans le navigateur et s'ouvrira sur votre PC dans le logiciel que vous lui avez associé. Un client dans votre navigateur en somme sauf que dans cette partie du logiciel vous pourrez aussi afficher des sites que des contributeurs auraient pu générer. Avec un .torrent, vous pouvez donc afficher un site et le faire «vivre» sur le réseau. Enfin, tant qu'il y aura des «seeders»...





NFC : LA TECHNOLOGIE DE TOUT LES DANGERS

Téléphones, cartes bancaires, ordinateurs, clés USB, antivols et même cartes de visite : on trouve des puces NFC partout de nos jours. Cette technologie sans fil et sans contact nous entoure alors que nous n'avions rien demandé. Car comme le WiFi ou le Bluetooth, le NFC ajoute sans doute du confort dans nos habitudes, mais aussi de l'insécurité ! Faisons le point sur les risques et les précautions à prendre...

LEXIQUE

***NFC :** Pour Near Field Communication ou «communication en champ proche» dans la langue de Nadine Morano. Dérivé de la technologie RFID, ce protocole permet différents échanges de données sur de très courtes distances. Les utilisations sont variables : billetterie, paiement bancaire, lecture d'information, déverrouillage d'un téléphone ou d'une voiture, domotique, etc.

CAGE DE FARADAY : Dispositif permettant d'isoler un espace des ondes électromagnétiques. Inventées par Michael Faraday, ces cages peuvent être de toutes tailles et sont composées d'aluminium. Elles sont bien connues des voleurs de supermarché !

SOCIAL ENGINEERING : Appelé «ingénierie sociale» dans la langue de Christian Estrosi, le social engineering est un ensemble de techniques qui permet d'obtenir des informations auprès de personnes autorisées sans qu'elles se rendent compte de la supercherie. Pour arriver à ses fins, le pirate va alors utiliser ses connaissances (pas forcément informatique), la crédulité ou l'ignorance de son interlocuteur, une dose de culot et sa capacité de persuasion...

Le NFC est une technologie de communication permettant des échanges sans fil à courte portée. Lorsqu'il s'agit de lire des informations (prix en magasin, caractéristiques d'un produit), de les synchroniser ou de faire joujou avec votre console de jeux, cela ne pose pas de problème. Mais lorsque les industriels commencent à trouver d'autres applications un peu plus sensibles, cela ouvre les portes aux malfaiteurs. Il est par exemple possible de démarrer sa voiture avec une puce NFC stockée dans sa clé. Et si cette dernière était clonée par un voleur ? Plus grave, les banques se sont engouffrées dans la brèche ! Tout contents de pouvoir proposer à leurs clients des paiements simplifiés, les deux géants du marché des cartes bancaires (Mastercard et Visa) ont commencé à implanter des puces NFC dans leur produit depuis quelques années. Ces cartes sont depuis majoritaires et peut-être en avez-vous une sans le savoir. La banque ne vous dit rien, et vous la propose d'office !

DES LIMITES PAS SI LIMITÉES...

Si la somme est inférieure à 20 € vous pouvez payer sans entrer la carte dans le terminal. Vous n'avez même plus de code à taper, la somme est débitée. Cette limite (qui diffère selon les banques) est d'ailleurs trompeuse, car il existe une limite par jour et par commerçant qui diffère selon les banques. Un pirate avec un terminal piraté pourra donc passer ses journées

dans les transports en commun à prélever sa dîme avant de se faire repérer par la banque. Car c'est bien connu, il vaut mieux voler 1000 fois 20 € que... Enfin, vous m'avez compris *Émile*. Il est aussi possible de voler votre argent en plaçant un lecteur à proximité et même de relayer les données bancaires à un complice qui fera ses achats en puisant dans votre compte. C'est un véritable retour en arrière au niveau de la sécurité puisque la communication entre la carte et le lecteur se fait de manière non chiffrée et non authentifiée. Et si cette limite n'existait plus ? Lors de la dernière *ACM Conference on Computer and Communications Security*, des chercheurs ont exploité une faille du protocole NFC permettant de faire sauter ces barrières à condition de demander un paiement dans une devise étrangère. Avec un téléphone transformé en terminal de paiement pirate, ces derniers ont pu demander un paiement de 999 999 «quelque chose» (dollars, euros ou livres, etc.) Bien sûr, un tel montant éveillera sans doute les soupçons de la banque débitrice, mais ce problème de sécurité est bien d'actualité.

LES DONNÉES CONFIDENTIELLES AU GRAND JOUR

Vous imaginez mal tomber sur un pirate avec un faux terminal dans le métro ? Très bien. Saviez-vous qu'il est possible de lire le contenu de votre carte bancaire depuis un simple smartphone Android ? L'application Lecteur de carte bancaire (super ce nom !) de Julien Millau peut sans problème accéder à diverses informations : type de carte, numéro, date d'expiration et historique des paiements. Il ne manque que le cryptogramme visuel au dos. Notons quand même que dans certains pays (États-Unis, Russie, etc.), ces informations sont suffisantes pour effectuer des achats par Internet. Avec un smartphone il faut être très près de sa cible, mais avec une antenne bricolée, un pirate peut partir à la pêche à 15 mètres et ne jamais revenir bredouille...

BIOHACKING ET NFC

Seth Wahle est un biohacker. Ce jeune ingénieur s'est greffé une puce NFC dans sa main droite. Lorsqu'il tient un téléphone Android dans sa main, sa puce NFC demande à l'appareil de se connecter à un site. Si le téléphone est mal sécurisé, la connexion se fait très facilement. Ce site est en fait frauduleux et permet d'installer sur le smartphone un trojan permettant un accès aux fichiers, aux contacts, etc. Un autre danger du NFC...

QUE FAIRE POUR SE PROTÉGER ?

Si vous appelez votre banque pour désactiver la fonction de paiement NFC, ce ne sera pas suffisant, car la puce sera encore là. Vous pouvez aussi vous équiper d'un étui en aluminium faisant office de cage de Faraday bloqueuse d'ondes (voir notre encadré ou allez ici : www.stop-rfid.fr). Attention, car au moment de payer votre carte sera vulnérable. La solution consiste alors à changer de carte. Dans la plupart des banques, cette opération ne sera pas facturée. Mais, si vous êtes à l'étranger ou que vous êtes en froid avec votre banquier, vous pouvez aussi repérer la puce NFC et lui mettre un bon coup de perceuse ! Nous avons d'ailleurs essayé cette technique pour vous, avec succès !

SIGNAL BLOCKING BAG, UNE CAGE DE FARADAY PORTATIVE !

Voici un gadget très sympa pour une somme très modique. Il s'agit d'une mini cage de Faraday portative pour téléphone portable ou carte bancaire. Ce type de dispositif bloque complètement les ondes quelles qu'elles soient : radio, GPS, GSM, Bluetooth, WiFi, NFC, RFID, etc. Aucun risque de fraude bancaire ! Les possesseurs de smartphones éviteront les piratages, économiseront de la batterie et pourront mettre leur appareil «hors ligne» sans avoir à l'éteindre ou le rallumer (cinéma, réunion, hôpital, etc.)

Prix : 3 € Lien : www.chinavasion.com

PAS À PAS

Lisez le contenu de votre carte bancaire !

CE QU'IL VOUS FAUT

LECTEUR DE CARTE BANCAIRE V3.1.1

OÙ LE TROUVER ? :
https://goo.gl/zgRQcw

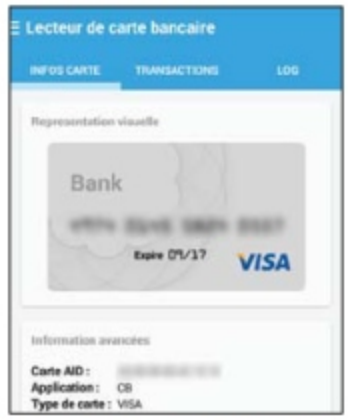
DIFFICULTÉ :

01 CAPTURE DES INFORMATIONS

Vous avez une carte bancaire avec la technologie NFC? Si c'est le cas, vous devriez avoir un petit logo en forme d'onde à côté de la puce électronique (on dirait le logo WiFi de travers !). Pour lire le contenu, installez l'appli **Lecteur de carte bancaire** sur votre smartphone Android et posez votre carte bancaire au dos de votre téléphone.

02 INFO CARTE

Si vous ne bougez pas la carte, les informations vont s'afficher au bout de quelques secondes. Outre le numéro complet, le type de carte (Visa ou Mastercard) et la date d'expiration, on trouve le numéro AID. Ce dernier permet de savoir le type de carte et le pays d'émission (vous trouverez une liste ici: **https://goo.gl/1HlbaS**)



03 LES TRANSACTIONS

Dans l'onglet **Transactions,** vous retrouverez la liste complète de vos derniers achats. Alors même si la liste n'est pas très détaillée (on y voit le montant, le pays et le type de transaction), cette partie peut devenir une mine d'or pour du social engineering en recoupant ces informations avec d'autres données. Une sérieuse atteinte à la vie privée en tout cas...

PAS À PAS

Désactivez (subtilement) la puce NFC de votre CB

01 REPÉREZ LA BOBINE...

La puce NFC est souvent trop près de la puce «normale» (celle qui est métallique à gauche) pour intervenir sans endommager la carte. Il faudra donc opérer sur la bobine qui interagit avec les champs magnétiques. Cette dernière prend la forme d'un fil très fin qui parcourt la carte. Bien sûr, suivant les modèles, le «chemin» emprunté sera différent.

Il faudra donc essayer de trouver ce fil très fin en vous mettant dans le noir. Avec une lampe torche puissante (ou le flash de votre smartphone) orientée sur le recto de la carte, vous devriez pouvoir trouver une partie de la bobine.

02 ...ET LA DÉTRUIRE «CHIRURGICALEMENT»

Une fois repéré vous devrez marquer l'endroit à l'aide d'un stylo bille. Suivant l'emplacement de la bobine, vous pourrez alors percer avec un Dremel ou couper avec une paire de ciseaux bien aiguisée pour complètement détruire la fonctionnalité de paiement sans contact. Attention ne coupez/percez pas dans la bande magnétique ! Vous pouvez vérifier que vous avez réussi en utilisant l'appli Lecteur de carte bancaire. Et surtout, tentez un retrait au guichet automatique pour être sûr que vous n'avez pas endommagé la carte.

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

Actuellement

LE GUIDE 2016 DU HACKER

#Guide pratique

NIRSOFT : LA BOITE À OUTILS DE LA BIDOUILLE !

Vous vous demandez comment scanner vos ports ? Surveiller votre trafic réseau ? Contrôler la santé d'un disque dur ? Comprendre pourquoi votre OS plante ? Dresser une liste de vos pilotes ? Sniffer des mots de passe sur votre réseau ou récupérer la clé produit de votre Windows ? Il y a forcément un logiciel pour vous sur le site de NirSoft...

Lancé en 2001 par Nir Sofer, NirSoft est un site très austère où vous trouverez plus de 180 logiciels programmés en C++. L'avantage de ce langage ? Des programmes très légers (la majorité fait moins de 200 ko), peu gourmands en mémoire et aucun droit à payer à qui que ce soit. Nir est un programmeur très consciencieux : la plupart de ses logiciels ne nécessiteront aucune installation et pourront se loger sur une clé USB sans laisser de traces dans la base de registre de l'ordinateur sur lequel vous les utilisez.

DES LOGICIELS ET RIEN D'AUTRE...

Pas de toolbar, d'adware ou autres surprises. Et notre bougre fait bien les choses puisque vous trouverez des applications autant pour l'audit réseau que pour la récupération de mots de passe ou pour de la maintenance. Certains sont même traduits en français. Faire une liste complète serait inutile, mais nous avons quand même souhaité vous présenter quelques-uns des meilleurs softs du site...

«CE SITE EST PLEIN DE VIRUS !»

Comme la plupart des logiciels qui se trouvent sur notre CD, les programmes NirSoft auront tendance à faire paniquer votre antivirus. Comme ces outils agissent parfois comme le feraient des malwares, les systèmes de protection les considèrent comme des logiciels malveillants. En utilisant les outils de Nir Sofer, vous ne risquez rien...

Notre sélection de logiciels NirSoft

CE QU'IL VOUS FAUT

NirSoft **NIRSOFT**

OÙ LE TROUVER ? :
www.nirsoft.net

DIFFICULTÉ :

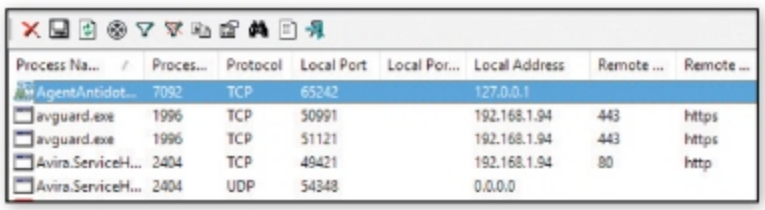
01 PRODUKEY

ProduKey permet de facilement récupérer le numéro de licence de votre Windows, de votre pack Office ou d'autres produits Microsoft. Vous pourrez ainsi réinstaller vos produits sur un autre PC si vous en changez.

02 SNIFFPASS

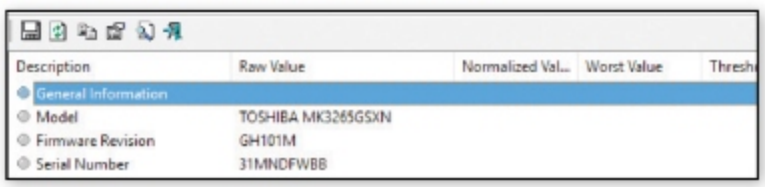
Ce logiciel va «sniffer» votre réseau à la recherche de mots de passe POP3, IMAP4, SMTP, FTP et HTTP. Si vous avez une connexion, mais que vous avez perdu le mot de passe, lancez le logiciel et SniffPass le retrouvera pour vous.

03 CURRPORTS



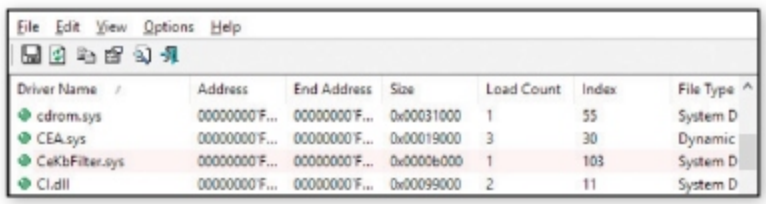
Comme son nom l'indique, CurrPorts est un outil de surveillance réseau qui permet d'afficher les ports UDP et TCP/IP actifs sur un ordinateur local. Cet outil est particulièrement utile pour analyser les connexions qui sont utilisées par vos différents programmes.

04 DISKSMARTVIEW



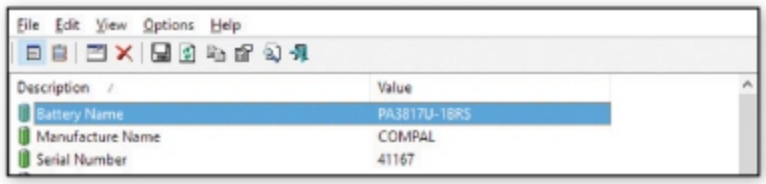
DiskSmartView rassemble toutes les informations SMART (Self-Monitoring, Analysis, and Reporting Technology) de vos disques durs installés et répertorie les informations sur une seule fenêtre. Ces données comprennent le type de micro logiciel, le numéro de série, la température, les taux d'erreur, etc.

05 DRIVERVIEW



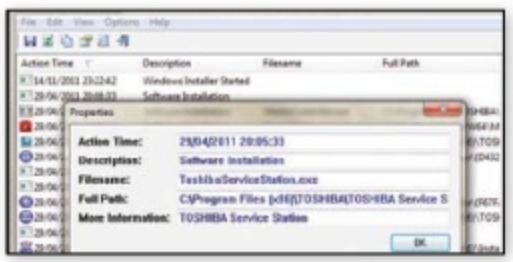
DriverView vous permettra d'y voir un peu plus clair dans vos périphériques, mais contrairement au gestionnaire intégré à Windows, il répertorie tous les pilotes des appareils avec de nombreuses informations: adresse de chargement, type de fichier, description, etc.

06 BATTERYINFOVIEW



BatteryInfoView est un petit utilitaire pour les ordinateurs portables qui affiche différentes informations sur votre batterie: marque, numéro de série, état de l'alimentation, capacité, tension, taux de charge/décharge et des indications sur sa santé.

07 LASTACTIVITYVIEW



LastActivityView est un petit programme à utiliser sur votre machine ou celle de vos enfants. Il permet de surveiller discrètement l'activité: installation de programmes, ouverture d'un fichier, d'un dossier ou d'un logiciel, branchement d'une clé USB, redémarrage, etc.

ET AUSSI...

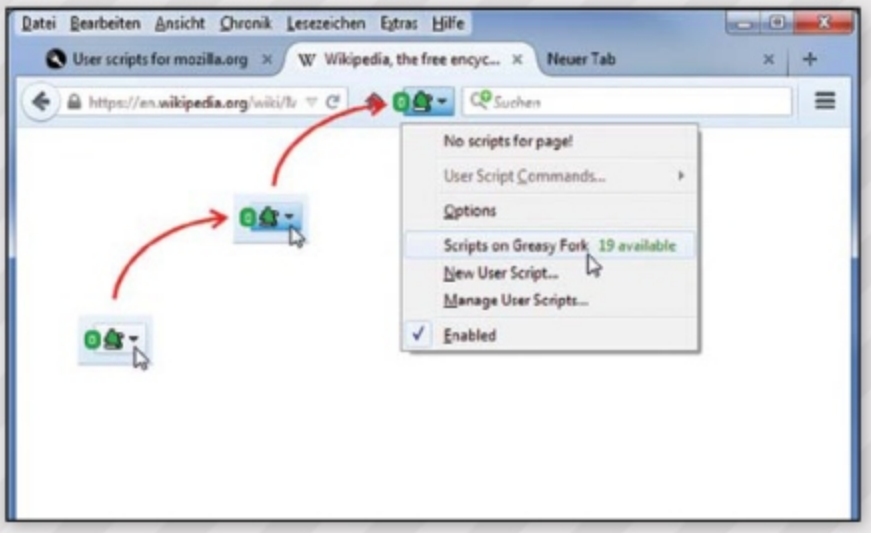
NirSoft propose aussi des outils meilleurs que ceux qui sont intégrés à Windows. Si le gestionnaire de périphérique, le désinstalleur, le journal ou l'observateur d'événements par défaut ne vous conviennent pas, Nir Soft a forcément une alternative: DevManView, My Uninstaller, WinCrashReport, MyEventViewer, etc.

#1 Quels userscripts sont dispos pour tel site

AVEC GREASY FORK

Dans *Pirate Informatique* n°18 et *Les Dossiers du Pirate* n°3 nous vous avions parlé de Greasemonkey. Cette extension permet l'exécution de scripts sur une page Internet pour modifier son affichage ou son fonctionnement (mettre des skins dans Gmail, supprimer les publicités, modifier le comportement de YouTube ou Facebook, télécharger des vidéos de stream, remplir automatiquement des formulaires, etc.) Il y a tellement de scripts qu'il est bien dur se s'y retrouver ou de savoir ce qui pourrait éventuellement vous intéresser. Heureusement, voici Greasy Fork! Cette extension pour Firefox vous indiquera quels sont les scripts disponibles pour le site que vous êtes en train de visiter.

Lien: **https://goo.gl/dslRFt**



#2 Ouvrez n'importe quel fichier

AVEC ROLLMYFILE

C'est typiquement le genre de service qui aurait bien arrangé les affaires de notre rédacteur en chef à la fin des années 90. Avec l'internet de l'époque, il était bien difficile de savoir quel logiciel pouvait ouvrir quel type de fichier. Cette période est révolue pourtant

un service comme rollMyFile a toute sa place dans vos favoris. Ce site connaît plus de 500 types d'extension de fichier et permet de les ouvrir en un clic. Pour cela, il

pioche dans une sélection d'application en ligne. Il est même possible d'éditer certains documents. La version payante à 6€/mois permet de traiter ses fichiers depuis son cloud et de travailler avec plusieurs types de fichiers différents.

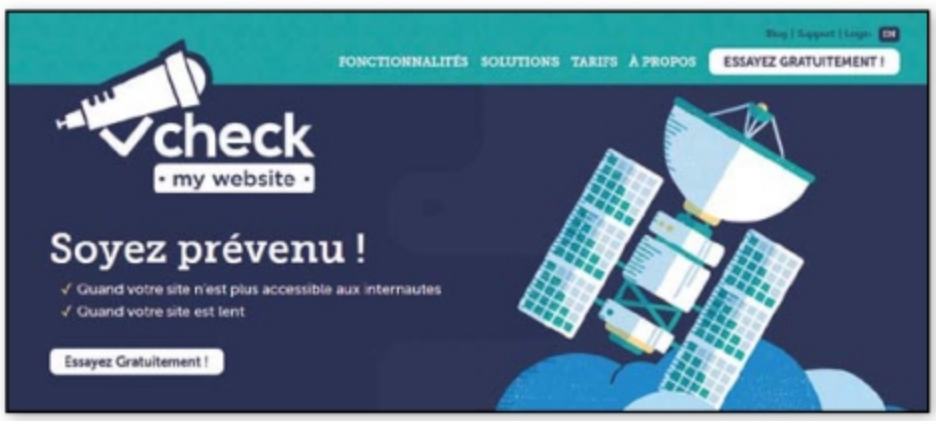
Lien: **www.rollapp.com**

#3 Vérifiez la santé de votre site en temps réel

AVEC CHECK MY WEBSITE

Vous avez un site Internet et vous ne pouvez pas vous permettre qu'il soit offline ou lent ? Check my Website est un service qui va vérifier en temps réel que tout se passe bien. Toutes les minutes, Check my Website va envoyer des requêtes vers votre site depuis plusieurs endroits du globe. Les résultats peuvent être affichés directement depuis votre CMS et dès qu'il y a une alerte vous êtes prévenu par e-mail ou SMS. Le service est gratuit pendant deux semaines et ensuite les tarifs sont très abordables (16€/an pour un site unique).

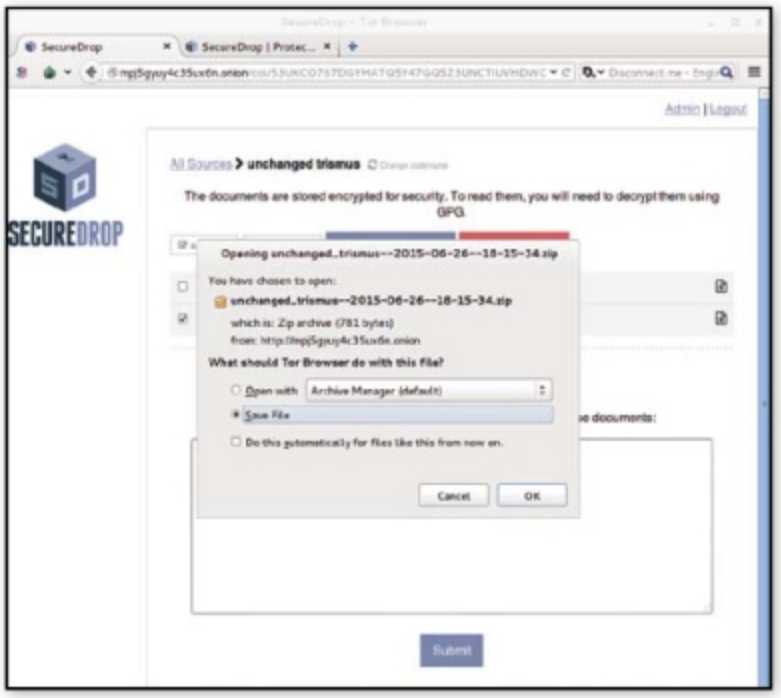
Lien: **https://checkmy.ws**



#4 Devenez lanceur d'alerte

avec SecureDrop

Nous aurions bien fait un article complet sur SecureDrop, mais il faut bien reconnaître que les gens concernés par le projet sont peu nombreux. Imaginons que vous ayez des informations à transmettre à un journaliste, mais que vous voudriez éviter d'avoir affaire avec lui (un journaliste est censé avoir le droit de protéger ses sources, mais dans les faits, il vaut mieux rester prudent). En bon whistleblower, vous devrez vous connecter au site Tor du journal puis laisser un message. En retour, SecureDrop vous donnera une clé permettant



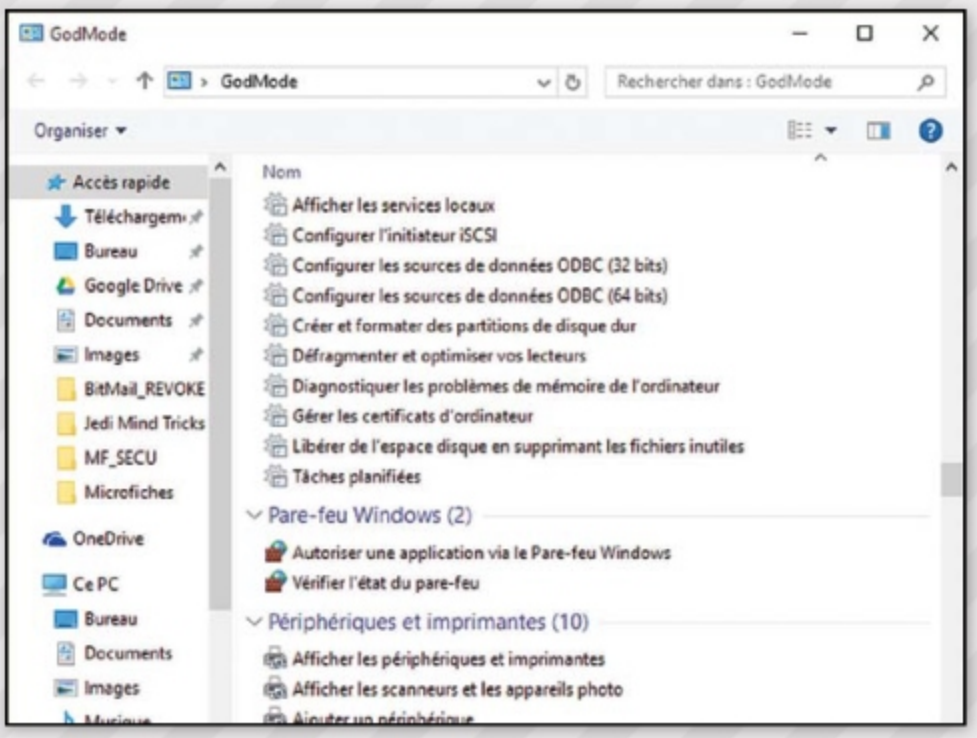
de lire les messages du journaliste. Ce dernier doit se connecter depuis Tor à son compte SecureDrop pour récupérer messages et documents. Pour l'instant seuls des médias anglo-saxons se sont intéressés au projet dont *Gawker Media, The New Yorker, The Guardian, The Washington Post* et une vingtaine d'autres.

Lien: **https://securedrop.org**

#5 Devenez Dieu!

avec Windows 10

Comme Windows 7 et 8, Windows 10 propose aussi une fonctionnalité nommée GodMode (ou «Mode Dieu» en français). Loin d'être une réelle mainmise totale sur le système, ce mode est tout de même très pratique et fait office de «super Panneau de Configuration». Pour y avoir accès, il suffit de créer un nouveau dossier (clic droit puis **Nouveau** et **Dossier**) sur le bureau et de le nommer **GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}**. Double cliquez sur votre nouvelle icône et contemplez vos nouvelles fonctionnalités: ergonomie, affichage, alimentation, réseau, sécurité, etc.



#6 Vérifiez l'intégrité de vos fichiers

avec Fim

Si vous avez un paquet de fichiers à transférer, vous aimeriez sans doute être absolument sûr que les données n'ont pas été endommagées. Fim (File Integrity Manager) va créer un fichier avec une empreinte de chaque document à transférer pour les comparer une fois le processus terminé. Vous saurez donc exactement quels fichiers ont connu des problèmes. Ceux qui le trouvent un peu rugueux peuvent aussi se rabattre sur MD5 Summer.

Lien: **https://github.com/evrignaud/fim**

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3€

Chez votre marchand de journaux

L'INFORMATIQUE FACILE

POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

qBittorrent : LA NOUVELLE STAR DU TORRENT

Vous téléchargez grâce au protocole BitTorrent et vous ne voulez plus de µTorrent ? Il faut reconnaître que ce logiciel n'est plus que l'ombre de ce qu'il était. qBittorrent fait figure de successeur. Léger, multi plate-forme et intégrant des fonctionnalités en pagaille, ce petit client ne quittera plus votre machine.

LEXIQUE

***BITTORRENT :** Protocole P2P inventé par Bram Cohen en 2002. Ce nom fait aussi référence au programme «historique» permettant les téléchargements et à la compagnie qui gère ses intérêts depuis 2006. Le protocole BitTorrent permet le partage de fichier volumineux tout en partageant la bande passante utilisée entre chaque intervenant.

***DHT :** Pour Distributive Hash Table ou table de hashage distribuée en français. Il s'agit d'une version complètement décentralisée de BitTorrent (sans tracker) où chacun a une liste réduite des Torrents dispos sur le réseau? Cela évite de questionner un serveur lors des recherches de pairs.

***PEX ET LSD:** Pour Peer Exchange et Local Peer Discovery. Il s'agit de deux méthodes permettant de récupérer des pairs depuis un pair avec qui on échange beaucoup ou qui est proche géographiquement. Le but est d'accélérer les téléchargements.

Depuis des années, lorsque nous parlions de client BitTorrent, nous recommandions systématiquement Torrent à nos lecteurs. Mais depuis son rachat par la société BitTorrent, notre ancien logiciel fétiche n'a cessé d'accumuler les tares : consommation de ressources excessive, version payante, publicité et un basculement vers le monde du logiciel propriétaire (fermé). Mais, ce qui a complètement signé l'arrêt de mort du logiciel à nos yeux c'est Epic Scale, un programme intégré aux dernières versions de Torrent qui minera du Bitcoin dans votre dos sous prétexte de sauver les bébés phoques et autres mensonges du même acabit.

LE RENOUVEAU DU CLIENT TORRENT

Nous avons donc décidé de changer de crèmerie et d'aller voir du côté de qBittorrent, un logiciel libre, en français, léger et bourré de fonctionnalités très intéressantes. C'est un client que les amoureux des premières versions de Torrent vont adorer. Il intègre un mode anonyme, la possibilité de gérer ses téléchargements à distance depuis une interface Web, un moteur de recherche, un module de création de fichier .torrent, un contrôle de la bande passante et du ratio ainsi qu'une compatibilité avec certaines variations du protocole BiTorrent : camouflage du protocole, DHT, LSD et PeX. Notons aussi qu'il permet de télécharger des Torrents chiffrés avec le protocole I2P (voir *Pirate Informatique* n°25) et de filtrer les IP connectées grâce aux listes de eMule ou PeerGuardian/PeerBlock (voir *Pirate Informatique* n°13 ou *Les Dossiers du Pirate* n°2).

Présentation de qBittorrent

CE QU'IL VOUS FAUT

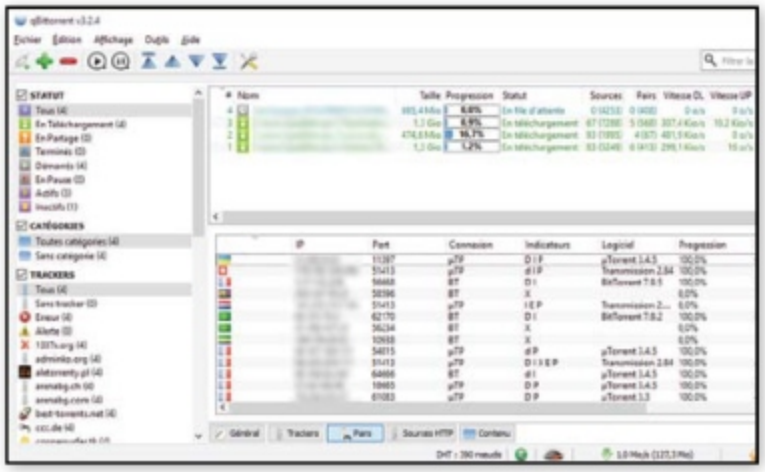
QBITTORRENT

OÙ LE TROUVER ? : **www.qbittorrent.org**

DIFFICULTÉ :

01 DÉJÀ-VU ?

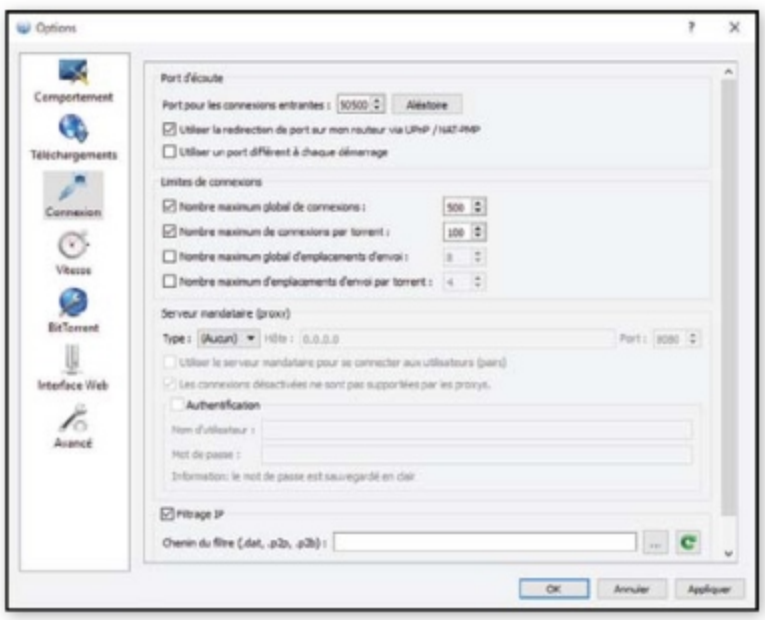
Rien de très original au niveau de l'installation. Pensez juste à cocher la case permettant de créer une exception automatique dans votre pare-feu et de mettre qBittorrent comme logiciel par défaut pour les .torrent et les liens



magnet. L'interface ressemble à un µTorrent 2.2 (une des dernières versions encore potables), pas de surprise à ce niveau-là. Allons dans **Outils**>**Options** pour commencer les réglages...

02 FILTRAGE AVEC IBLOCKLIST.COM

Passons sur les onglets **Comportement** et **Téléchargement** qui gèrent les réglages liés à l'interface pour nous intéresser à **Connexion**. Ici, vous pourrez paramétrer le port d'écoute, les **Limites de connexion**, un



éventuel proxy et le filtrage d'IP. Pour cette dernière option, sachez que les fichiers .dat, .p2p et .p2b sont compatibles avec qBittorrent. Vous pourrez donc empêcher les IP «espionnes» de se connecter chez vous. Allez sur **www.iblocklist.com** pour trouver des listes.

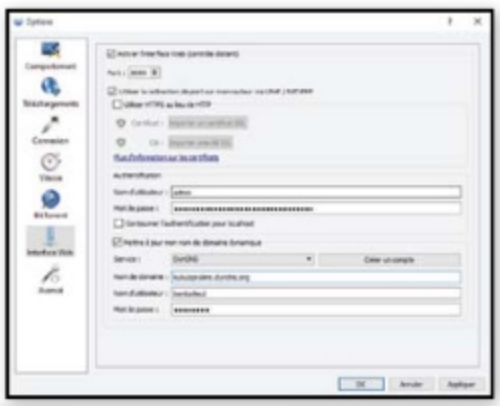
03 ET ENCORE DES OPTIONS...

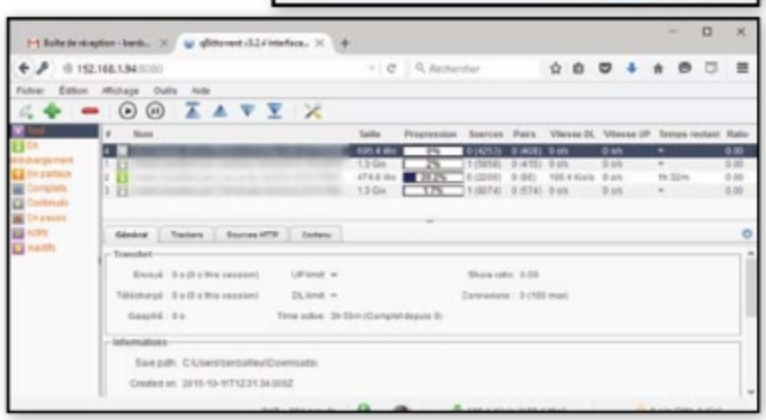
Dans **Vitesse,** vous pourrez gérer votre bande passante avec des limites d'upload et de download ainsi qu'un mini planificateur pour ne pas trop pomper le débit lorsque vous travaillez sur votre PC dans la journée par exemple. Dans **BitTorrent**, vous activerez ou non le DHT, le PeX, le

chiffrement et le **mode Anonyme**. Ce dernier masque le Peer-ID de votre empreinte sur le réseau. Attention, cette option n'est pas acceptée par certains trackers et incompatible avec le DHT. Par contre, si vous utilisez I2P, il faudra l'activer.

04 L'INTERFACE WEB

Enfin, comme son grand frère, qBittorrent propose un mode **Interface Web** pour gérer ses Torrents lorsque vous n'êtes pas chez vous. Activez ce mode, choisissez des identifiants et utilisez un compte DynDNS depuis le site No-IP pour y accéder depuis l'extérieur (voir *Pirate Informatique* n°23). Depuis votre navigateur, entrez votre nom de domaine dans la barre d'adresse puis vos identifiants. Une belle interface tout en Ajax et offrant les mêmes options que le client devrait alors s'ouvrir...





FOOTBALL, TENNIS, BASKET, RUGBY : SOPCAST SUR MOBILES

Si vous êtes lecteur de longue date vous connaissez sûrement Sopcast, ce logiciel chinois qui permet d'afficher des flux vidéo du monde entier. Et bien, sachez qu'une version pour Android est désormais de la partie et qu'elle fonctionne très bien...

Les retransmissions des rencontres sportives sur Internet ont le vent en poupe ! Sopcast est un logiciel très astucieux qui permet de profiter de chaînes de télévision via un réseau P2P. Il suffit de trouver des liens au format sop:// sur des sites spécialisés et de les faire fonctionner avec le logiciel. Ces flux sont en fait mis à disposition par de sympathiques internautes qui reçoivent plusieurs chaînes et qui vont les distribuer via ce réseau. Des versions pour Windows, MacOS et Linux existent, mais pour ce pas-à-pas nous allons essayer la version Android...

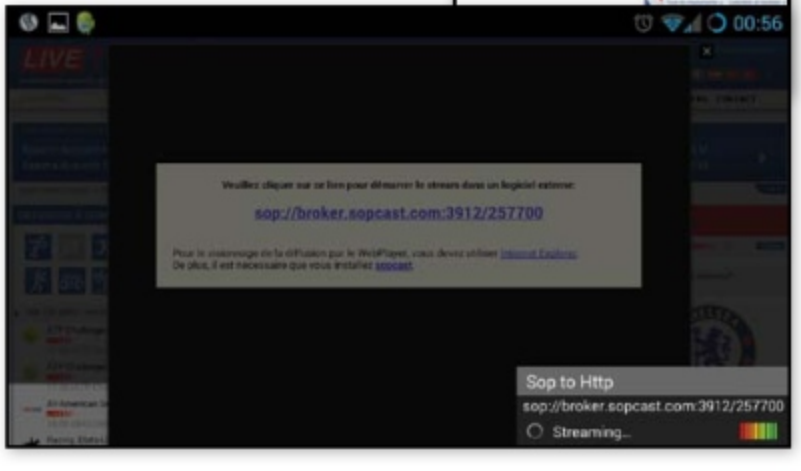
PAS À PAS

Sop to Http en 3 étapes

SOP TO HTTP (SOPCAST)
OÙ LE TROUVER ? : **https://goo.gl/DDV6rt**
DIFFICULTÉ :

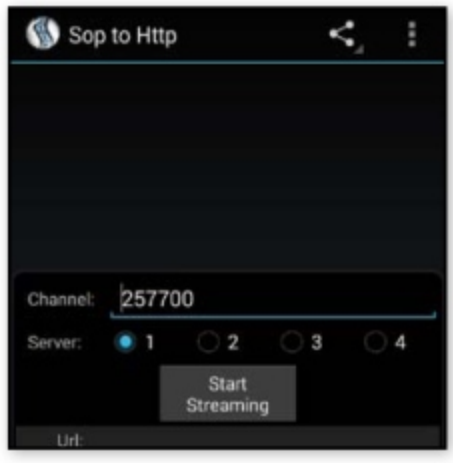
01 TROUVEZ DES LIENS

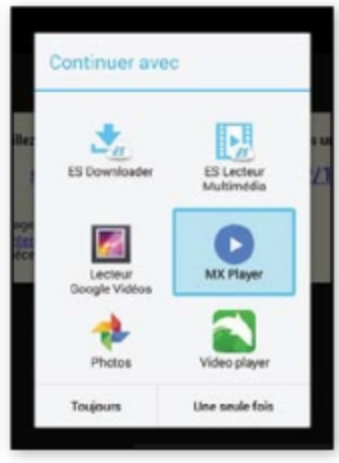
Pour trouver des liens **sop://**, nous avons l'habitude d'utiliser le site **http://livetv.sx/fr**. Même s'il est russe, ce dernier propose des liens vers les retransmissions de match qui intéresseront forcément les utilisateurs français ou francophones. Choisissez votre sport, votre match et cliquez sur **Diffusion vidéo**. Vous trouverez des **liens pour navigateurs web** et en dessous des **liens pour logiciels**. Ce sont ces derniers qui nous intéressent.



02 L'APPLI

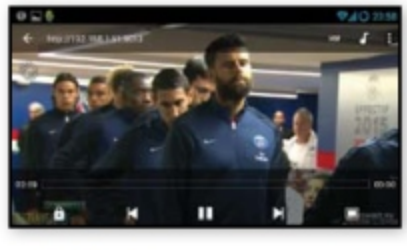
Dans cette liste vous trouverez des liens **sop://,** mais aussi des liens AceStream (un autre programme de retransmission P2P) avec la langue des commentaires et le débit. Pour une connexion Internet normale, vous pouvez aller jusqu'à 2000 kb/s. Cliquez sur la petite icône **Play** puis sur le lien pour que l'application Sopcast prenne la relève. Faites **Start Streaming** et attendez que la vidéo commence à se mettre en tampon.

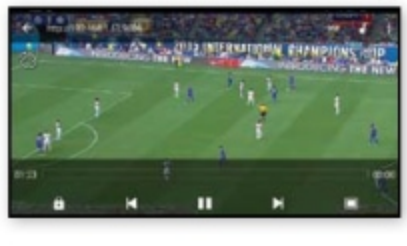




03 LA RETRANSMISSION

La première fois que vous allez lancer une vidéo, Sopcast vous demandera de choisir votre lecteur vidéo. Pour ce travail, nous vous conseillons MX Player. Comme il s'agit de P2P, plus il y a d'utilisateurs et plus la qualité sera au rendez-vous. Bien sûr, l'appli fonctionne sur smartphone, mais aussi sur tablette via WiFi ou la 3/4G. Si un lien ne fonctionne pas, essayez-en un autre ou tentez un des autres serveurs (juste avant le bouton **Start Streaming**).





LE POPCORN TIME DE LA MUSIQUE ?

Popcorn Time fait trembler l'industrie du cinéma et les diffuseurs de contenu de type Netflix ? Il n'en fallait pas plus pour que les créateurs du logiciel Aurous tente un buzz en lançant une version musicale de Popcorn Time. Pari réussi ?

Vous avez sans doute déjà entendu parler de Popcorn Time ? Ce logiciel basé sur la technologie BitTorrent et permettant de visionner films et série TV comme s'il s'agissait de streaming fait des émules. Cette fois-ci, il ne s'agit pas d'un énième fork ou portage, mais bien d'un logiciel de contenu musical qui utilise les mêmes ficelles. Les mêmes ficelles ? Pas vraiment. Il faudra encore attendre pour une véritable plate-forme musicale complètement décentralisée. Sur Aurous, la technologie BitTorrent ne sert qu'à la recherche et il est possible de passer outre. Le programme se base en effet sur des sites de stream russes illégaux bien sûr, le P2P passe au second plan. Encore en version alpha, le logiciel plante souvent, mais l'interface est plutôt réussie et il est possible d'ajouter son propre contenu depuis ses bibliothèques en attendant l'intégration de playlists venant d'autres services. Pour l'instant, seules les versions desktop sont disponibles (Windows, Mac et Linux), mais on parle de versions mobiles très prochainement...

PAS À PAS

Comment fonctionne Aurous ?

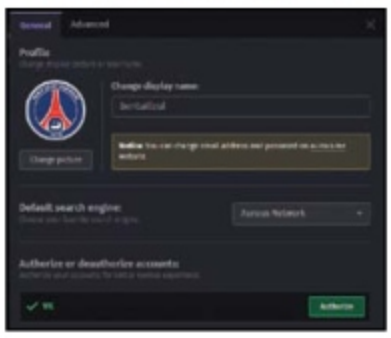
CE QU'IL VOUS FAUT

AUROUS

OÙ LE TROUVER ? : **https://aurous.me**

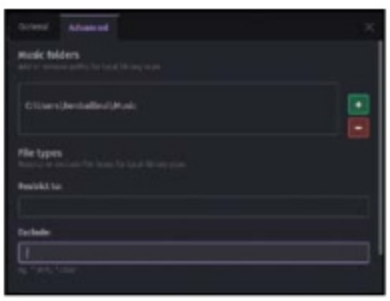
DIFFICULTÉ :

01 PREMIER «KONTAKT»



Dès le lancement, faites un tour dans les **Paramètres** (l'engrenage en haut à gauche) pour entrer votre pseudo, un avatar et choisir votre moteur de recherche par défaut : Aurous (recherche grâce à des listes BitTorrent, MP3WithMe ou VKontakte (VK), un réseau social russophone. Notez d'ailleurs que vous pourrez partager sur ce site si vous êtes titulaire d'un compte, camarade !

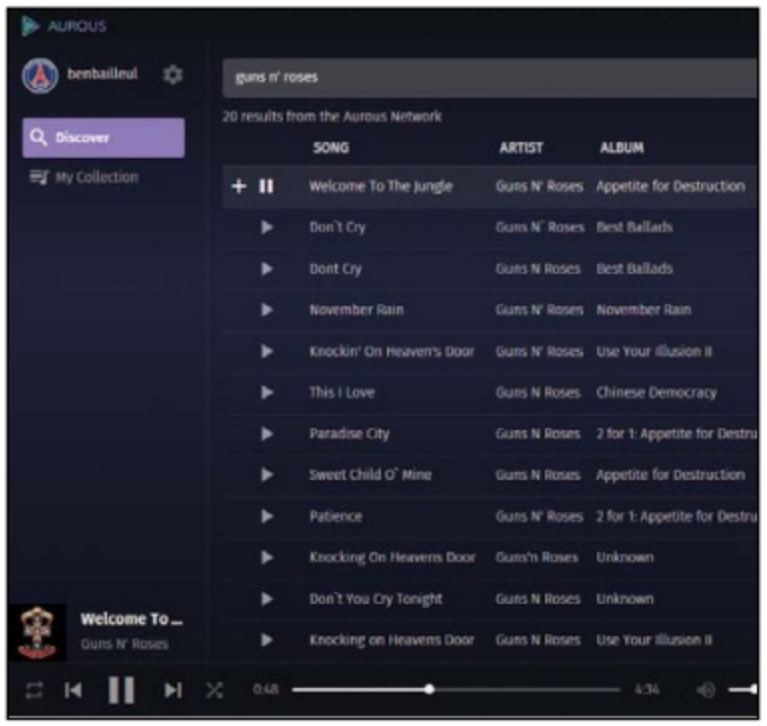
02 VOS PRÉFÉRENCES



Dans **Advance**, il est possible de pointer vers vos bibliothèques pour partager vos morceaux et plus bas vous pourrez spécifier vos préférences en matière de format de fichiers. Le lossless n'est pas encore de la partie au moment où nous écrivons ces lignes tout comme la sauvegarde et l'import de playlist. Il faut dire que c'est une version alpha 0.1 : tout est à faire, mais les développeurs ont l'air réactifs et répondent sur Twitter.

03 L'INTERFACE

L'interface est très jolie, mais il vaut mieux s'armer de patience, car cela plante souvent. On trouve toutes les fonctions basiques, mais pourquoi n'est-il pas encore possible de créer ses playlists comme on peut le voir sur la capture d'écran du site ? Même si on est encore loin d'un «Spotify killer», le logiciel s'avère tout de même prometteur... À vous de vous faire une idée.

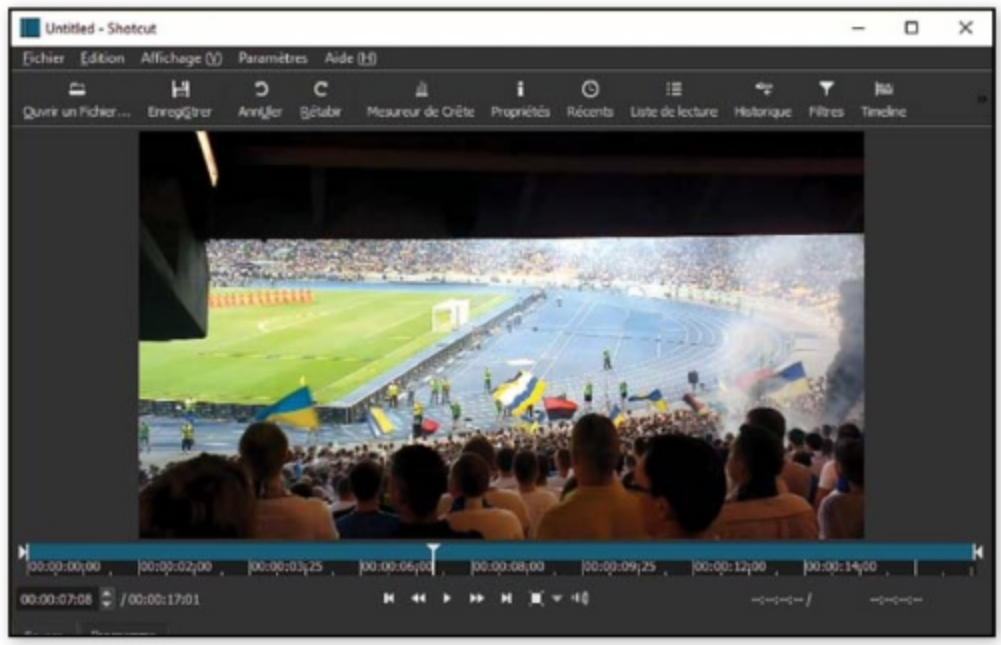


#1 Un éditeur vidéo gratuit

AVEC SHOTCUT

Si vous aimez encoder, traiter ou convertir vos vidéos personnelles, Shotcut est fait pour vous. Non seulement il est gratuit, mais il propose une quantité phénoménale de fonctionnalité. Que vous vouliez ajouter des filtres, corriger le contraste, la luminosité ou les couleurs, désentrelacer, muxer ou démuxer, c'est le programme idéal. Avec sa compatibilité Ffmpg, il reconnaît la plupart des fichiers y compris les nouveaux standards 4K. Il est tellement complet qu'il est un peu complexe à prendre en main, mais vous trouverez des liens vers des tutos en vidéo sur le site.

Lien: **www.shotcut.org**



#2 Stockez 500 Go gratuitement

AVEC GIGA

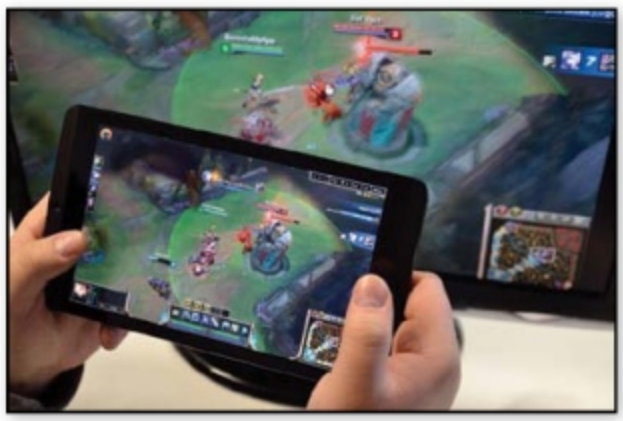
Record battu! Mega.co.nz proposait 50 Go de stockage, mais Giga.gg (le successeur de GigaTribe) décuple cet espace. Bien sûr c'est gratuit, mais vous serez limité à un trafic de 2 Go/mois en mode«Turbo». Ce dernier permet la lecture en stream de vos contenus et un téléchargement à pleine vitesse. Vous pouvez inviter vos amis à télécharger dans votre espace et vice-versa. Cerise sur le gâteau, tout est chiffré, vous ne risquez donc pas de retrouver vos précieuses photos sur le Net. La version payante à 6€/mois vous donne 10 To d'espace et un mode «Turbo» illimité.

Lien: **https://giga.gg**

#3 Jouez à vos jeux PC sur votre mobile

AVEC REMOTR

Si vous ne possédez pas de Nvidia Shield, il existe un moyen de streamer les jeux de votre PC directement sur votre appareil Android ou iOS. Cette solution s'appelle Remotr et elle est téléchargeable gratuitement sur le Play Store. Contrairement à l'application préinstallée sur les appareils Nvidia, Remotr permet la configuration de boutons virtuels, au lieu de brancher une manette. Une bonne machine (aussi bien côté PC qu'appareil mobile Android) ainsi qu'une bonne connexion Internet sont nécessaires pour une expérience optimale. L'application qui ravira les personnes souhaitant continuer à jouer, mais qui ont l'habitude de faire plusieurs choses à la fois.

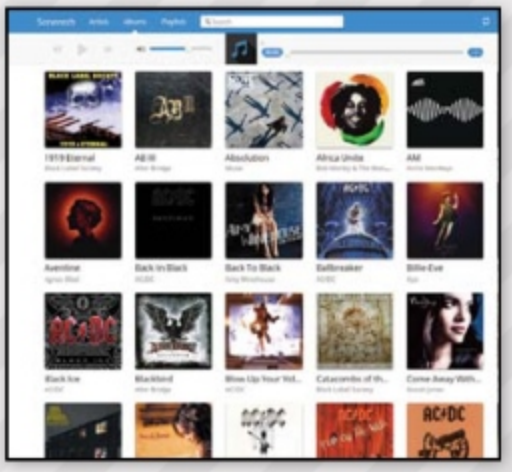


Lien: **http://remotrapp.com**

#4 Votre musique partout où vous le souhaitez

AVEC SONEREZH

Si vous disposez d'un espace d'hébergement Web (PHP+SQL) avec votre FAI ou si votre NAS permet d'héberger un site, voici Sonerezh. Cette solution logicielle permet d'héberger votre musique et d'y avoir accès depuis



l'ensemble de vos appareils (et d'inviter vos amis bien sûr). L'interface est plutôt jolie et vous pourrez alors vous passer d'uploader vos MP3, FLAC ou OGG sur Google Music ou un autre service de ce genre. Une notice de déploiement détaillée en français est disponible sur le site...

Lien: **www.sonerezh.bzh**

#5 Découvrez si une photo est truquée

AVEC FORENSICALLY

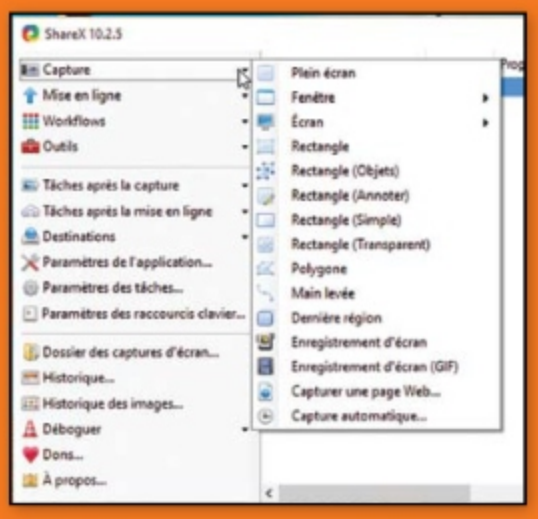
Forensically est un site qui propose de savoir si une photo a été truquée ou si des éléments ont été ajoutés et modifiés. Il suffit d'uploader votre fichier et d'utiliser les différents menus comme **Error Level Analysis** ou **Clone Detection** pour voir les irrégularités. Même retravaillé par un virtuose, vous découvrirez le pot aux roses à chaque fois...

Lien: **http://goo.gl/FU8Ibk**

#6 Des captures sur mesure

AVEC SHAREX

Si la touche **Imp.Écran** montre ses limites, vous aimeriez peut-être installer un vrai logiciel de capture d'écran. ShareX convient pour des captures simples comme pour les cas les plus complexes. Vous pouvez capturer les fenêtres, l'écran entier, mais aussi une zone à main levée (sous plusieurs formes). Depuis



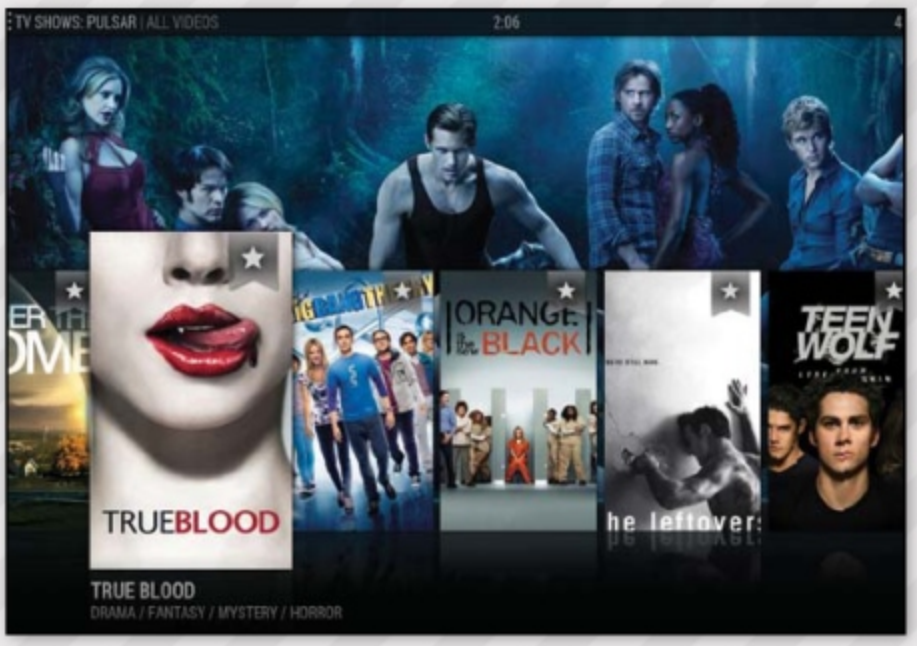
l'interface, vous pouvez imprimer, envoyer sur Twitter, mettre en ligne (site, cloud) ou capturer une page Web entière. ShareX propose aussi des options de capture vidéo (GIF, x264 ou Xvid). Il y a tellement d'options que nous n'en avons toujours pas fait le tour...

Lien: **http://getsharex.com**

#7 Films & séries à la demande

AVEC PULSAR

Si vous êtes un habitué de nos publications, vous connaissez sans doute Kodi (ex-XBMC), un des Media Center les plus populaires. Disponible sur toutes les plates-formes (Windows, Mac, Linux, etc.) y compris les plus surprenantes, Kodi centralise vos fichiers multimédias pour les afficher sur le téléviseur du salon. C'est donc avec joie que nous avons donc découvert Pulsar, un plug-in pour Kodi qui permet de faire exactement la même chose que Popcorn Time mais depuis son canapé! Comme il ne figure pas encore dans la liste des plug-ins officiels, il faudra l'installer



depuis une archive .zip (suivez notre lien). Le contenu n'est pas aussi riche que pour les autres clones et la rapidité dépendra beaucoup de la puissance de la machine qui fait tourner Kodi. C'est un plug-in à surveiller de près!

Lien: **https://goo.gl/PEml02**

X-MATÉRIELS

> Yubikey Standard de Yubico

Yubikey est un dispositif de sécurisation qui prend la forme d'une clé USB. Cette version Standard est disponible en deux formats : une normale et une version Nano de taille très réduite (trop ?). Antichoc, étanche et fonctionnant sans pile, cette clé génère un mot de passe aléatoire de 32 caractères (appelé OTP pour One Time Password) à chaque pression sur le petit bouton en son centre. Cette chaîne est ensuite chiffrée à l'aide d'une clé AES 128 bits et envoyée sur un serveur de validation (chez Yubico ou le vôtre). Un autre mode de validation (statique) permet de générer le même sésame complexe à chaque fois. C'est à vous de choisir la méthode d'identification. Vous n'aurez plus à vous creuser la tête pour trouver vos mots de passe ou pour vous connecter à un site ou un service en ligne. Notons enfin que Yubico propose aussi des modèles plus avancés comme la Edge ou la Neo qui intègrent des fonctionnalités supplémentaires : un mode NFC (sans contact), une compatibilité avec OpenPGP ou l'algorithme FIDO U2F, qui n'est utilisé que par Google et Dropbox à l'heure actuelle.

Prix : **25$ (23 €)** **www.yubico.com**

VideoGhost,
Captures d'écran à votre insu

Vous connaissez certainement ces keylogger matériels qui se branchent entre le PC et le clavier pour enregistrer les frappes à l'insu de vos enfants ? Le VideoGhost fonctionne un peu de la même manière sauf que cet appareil capture ce qui s'affiche à l'écran de votre «victime». Disponible au format DVI, HDMI et VGA ce petit câble passera inaperçu derrière une tour. Il suffit de le brancher entre le PC et l'écran et de l'alimenter avec un port USB libre. À vous ensuite de régler l'intervalle de capture, le chiffrement (ou pas), la taille des captures et le taux de compression Jpeg. Le VideoGhost permet de stocker 4 Go de données. Seul hic, il faudra avoir accès à la machine pour récupérer les images. Pendant que les gosses sont à l'école ?

Prix : **130 €** **www.keelog.com**

America, The ear listens,
Les murs ont des oreilles

Ce petit gadget permet de facilement écouter les sons et les conversations à travers des murs de 20 cm ! Il suffit de le caler contre une cloison, un plafond ou un plancher (béton, bois, verre, etc.) pour ne rien rater de ce qui se passe de l'autre côté. L'amplificateur est très puissant alors évitez de le mettre à fond au risque de vous faire mal aux oreilles. La batterie rechargeable vous autorise une autonomie de quelques heures. Notons la possibilité d'ajouter un dispositif d'enregistrement depuis le port jack. Attention, n'utilisez pas cet appareil pour espionner vos voisins par exemple, vous pourriez tomber sous le coup de la loi.

Prix : **32 €**

http://goo.gl/2P2xSo

Emish X800,
Une SmartTVBox puissante et abordable

Si vous n'avez pas de SmartTV la solution est d'investir dans une clé de type Chromecast ou plus sympa, de s'équiper d'une SmartTVBox. Ce genre de boîtier permet de récupérer tous les fichiers multimédias de la maison pour pouvoir en profiter sur son téléviseur. Le seul problème, c'est que ces appareils manquent parfois de puissance (WiFi limité à quelques mètres, fichier lourd, pas pris en charge, etc.) Le Emish X800 ne connaît pas ces déboires. Équipée de la dernière version d'Android 5.1, d'un processeur 8 cœurs et d'1 Go de RAM, cette petite merveille lit les derniers types de fichiers à la mode (x264/265, MKV, FLAC, etc.) sans problème et sans ramer, même en Ultra HD ! Idéal pour installer Kodi, ce X800 est aussi compatible Bluetooth et propose 8 Go de stockage pour dépanner.

Prix : **60 €** **www.dx.com**

NOTRE TEST EXCLUSIF

La Yubikey Standard de Yubico, Des mots de passe à la demande

La Yubikey est une solution de sécurisation idéale à condition de bien savoir s'en servir. Qu'il s'agisse de gérer un portefeuille de mots de passe ou de s'identifier sur ses sites préférés (Webmail, magasin en ligne, Facebook, etc.), cet appareil aux allures de gadget montre tout son talent...

#1 PREMIER CONTACT

Nous avons acheté la Yubikey Standard sur le site officiel et l'appareil est arrivé une semaine plus tard dans une lettre toute simple. Pas top, mais la clé USB est antichoc selon le fabricant donc... Dans le pli, on trouve aussi une petite pochette où glisser la clé. Comme la Yubikey est prise en charge comme un clavier, vous n'avez pas besoin de pilote, il suffit de l'insérer dans votre PC (Windows et Linux) ou votre Mac.

ET EN CAS DE VOL ?

En cas de perte ou de vol de votre Yubikey, il faudra composer avec les différents services. Sur LastPass par exemple, il est possible de supprimer l'association de votre compte au Yubikey en les contactant directement. Si vous utilisez le mode statique, il faudra copier votre mot de passe quelque part. Attention au format du clavier, nous vous suggérons d'appuyer sur le bouton dans un éditeur de texte pour voir le mot de passe en toutes lettres.

#2 DEUX SLOTS POUR QUATRE MÉTHODES

Pour paramétrer sa clé, il va falloir installer le Yubikey **Personalization Tool (https://goo.gl/hMjz2j)**. Chaque Yubikey dispose de plusieurs méthodes d'identifications (4 pour notre version «Standard») mais vous ne disposez que de deux «slots», ce qui veut dire que vous ne pourrez utiliser que deux méthodes. Le slot 1 s'activera lorsque vous appuierez sur le bouton brièvement (entre 0,3 et 1,5 seconde) tandis que l'authentification correspondant au slot 2 s'activera lorsque vous appuierez au moins 2 secondes. Dans notre cas, nous allons paramétrer le slot 1 sur le mode statique et le 2 sur le mode OTP.

#3 LES DIFFÉRENCES

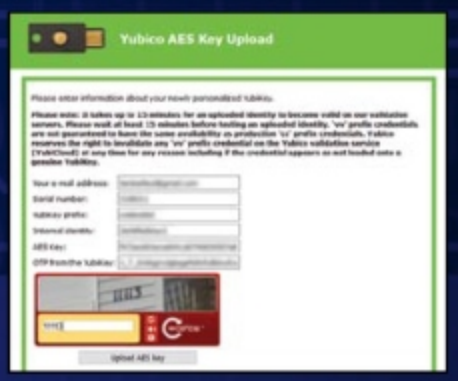
Le mode OTP permet de s'authentifier avec les services associés comme LastPass ou Tutanota (pour bientôt !) tandis que le mode statique donnera toujours le même mot de passe de 32 caractères. Même en utilisant uniquement des lettres minuscules, il faudrait des millions d'années pour cracker votre sésame. Si vous n'utilisez pas LastPass ou un autre service compatible avec l'OTP, optez pour le mode statique !

#4 LE MODE STATIQUE: TOUT TERRAIN

Allez dans **Static Password**, puis **Quick** et cliquez sur **Configuration Slot 1**. Choisissez un type de clavier et entrez un mot de passe (38 caractères maximum). Plus haut, vous pouvez choisir de protéger l'accès à ce mode de configuration (pour éviter qu'un voleur ne reprogramme la clé). Faites **Write Configuration** et validez (attention, si vous avez déjà paramétré l'OTP sur le **Slot1**, changez pour le second). Notez que le mode **Advance** permet en plus de gérer encore plus de paramètres de chiffrement. Voilà c'est fait, votre mot de passe statique est enregistré dans la clé.

#5 LE MODE OTP: UNIQUEMENT AVEC LES SERVICES COMPATIBLES

Pour le mode OTP, allez sur le premier onglet, faites **Quick** et cliquez sur **Configuration Slot 2.** Ici, vous n'avez rien à faire puisque les paramètres sont générés aléatoirement. Faites **Write Configuration** puis **Upload to Yubico**. Remplissez les champs, appuyez que le bouton pendant 3 secondes



depuis le champ **OTP from the Yubikey** et validez. Vous pourrez ensuite tester l'authentification sur une page Web spéciale. Avec l'OTP, un mot de passe généré à partir de votre clé privée sera envoyée au serveur de Yubico à chaque authentification et ce dernier validera ou non ce mot de passe avec la clé publique que vous aurez envoyée.

CD OFFERT

LE PACKAGE DU PIRATE

Tous les logiciels INDISPENSABLES

100% GRATUIT

LE GUIDE PRATIQUE

100% MICRO-FICHES, TRUCS & ASTUCES

Sécurisation

ANTI-FRAUDE

Adblock

P2P

DNS

KALI LINUX 2

VPN

Mots de passe

RASPBERRY PI

BEL/LUX : 6 € - DOM : 6,10 € - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – MAR : 50 mad - TUN : 9,8 tnd

L 12730 - 27 - F: 4,90 € - RD