+ OFFERT SUR LE CD : LE GUIDE COMPLET DE L'ANONYMAT

LES CAHIERS DU HACKER

# PIRATE [INFORMATIQUE] // 33

PIRATE [INFORMATIQUE]

## GUIDE 100% PRATIQUE

## 200% PIRATE

- Les meilleurs outils et astuces des hackers

+ OPENVPN Le GUIDE COMPLET du meilleur VPN GRATUIT

+DE 60 FICHES PRATIQUES AVEC CD GRATUIT


**MOTS DE PASSE**
HYDRA CRACKE LES MOTS DE PASSE DU WEB

**PROTECTION**
RANSOMFREE VOUS DÉBARRASSE DES RANSOMWARES

**MULTIMÉDIA**
TOUTES LES CHAÎNES ENFIN GRATUITES SUR PC ET TV

0,00€

# SOMMAIRE

## PROTECTION/ANONYMAT







## HACKING






## MULTIMÉDIA




43

46

**+ NOTRE TEST EXCLUSIF**

### 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 malwares, 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°33 - Mai / Juillet 2017**

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

**Directeur de la publication :**
David Côme

**Axl :** Benoît Bailleul

**Slash & Duff :**
Yann Peyrot & Thomas Povéda

**Dizzy & Melissa :** Sergueï Afanasiuk & Stéphanie Compain

**Correctrice :**
Marie-Line Bailleul

**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
Parution : 4 numéros par an.




## ÉDITO

### BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Dans ce numéro nous avons choisi de donner la parole à différents acteurs français de la sécurité informatique pour leur poser nos questions sur ce qu'ils pensent de l'actualité (Vault #7, etc.) et de la surveillance en général. Les réponses sont franches et surprenantes ! Nous avons aussi décidé de faire un sujet complet sur le logiciel OpenVPN et sur le service VPN qui nous semble le plus sûr à ce jour : IPredator. Un article référence. Vous aimerez aussi sans doute le dernier volet de notre série sur les systèmes alternatifs puisqu'après Tails et Qubes OS nous avons mis en lumière Kodachi, un OS anonyme proposant une tunnellisation complète avec un VPN et Tor. Nous continuons aussi la présentation des outils de Kali Linux avec le très dangereux xHydra. Ce logiciel propose tout simplement de cracker des mots de passe en ligne sans utiliser de hash. À n'utiliser qu'à but pédagogique donc. Enfin nous avons trouvé une petite perle : MediCat. Il s'agit en fait du successeur de Hiren's Boot CD, bien connu des bidouilleurs.

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

## MACRON SUR LE CHIFFREMENT : SANS DÉCODEUR ON NE COMPREND RIEN !

Celui que tout le monde veut nous vendre comme le futur Président (et qui le sera peut-être au moment où vous lirez ces lignes) s'est illustré par sa méconnaissance des méthodes de chiffrement. Suite à l'attaque du 22 mars à Londres où les crétins habituels ont utilisé WhatsApp pour communiquer, Emmanuel Macron a fustigé les grands groupes d'Internet qui auraient refusé jusqu'à présent de communiquer leur clef de chiffrement ou de donner accès à leur contenu (sans doute avait-il en tête l'affaire Apple contre le FBI). Bien sûr, s'il est élu, blabla, s'en sera fini de ces histoires.Il prévoit aussi de «*réquisitionner leurs services cryptés*». C'est bien sûr oublier que tant que ces services sont basés à l'étranger, il ne peut légalement rien faire, mais qu'en plus cela ne fonctionne pas du tout comme ça. Il n'existe pas de sésame permettant d'ouvrir toutes les portes et même pas de sésame du tout si le chiffrement est de bout en bout avec les clés stockées localement sur l'ordinateur des utilisateurs. Mais on n'est plus à une approximation près pour le «candidat du numérique».

## ALLO TONTON ? POURQUOI TU TOUSSES ?

Avocat, écrivain et homme politique de son État, Gilbert Collard n'est par contre pas très à l'aise avec les nouvelles technologies. Après avoir twitté par erreur certains de ses propres mots de passe (nous lui conseillons d'ailleurs la lecture de notre dernier numéro des *Dossiers du Pirate* «spécial smartphone», encore en kiosques), il s'est récemment illustré en annonçant sur Radio Classique «être sur écoute». Bien sûr qu'il est sur écoute Gilbert ! Par contre son exemple en a fait rire plus d'un puisqu'en lieu de preuve il nous raconte que son téléphone lui dit «répétez ce que vous venez de dire». Même en imaginant que les petits gars de nos services secrets sont des Max la Menace, on les imagine mal demander à Maître Collard de se répéter. Vous l'aurez compris, Gilbert a fait connaissance avec l'assistant vocal de son smartphone, Siri ou OK Google. Lui qui connaît si bien les « *voix médiatiques tout à fait compatibles avec les aéroports*» n'a pas reconnu celle d'un...robot.

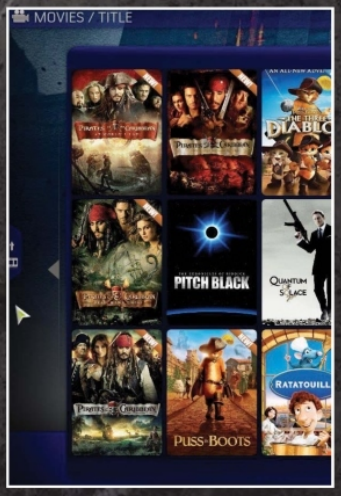
**«Allo? C'est Gilbert ! Passez-moi le 22 à Asnières ! Comment ça biiiiip ?»**

# L'IMPORTANCE DES MOTS DE PASSE PAR NOS AMIS EUGEN ERHAN & TUDOR MUSCALU


FREDO & PIDJIN - WWW.PIDJIN.NET

# KODI VEUT REDORER SON BLASON

Kodi a l'intention d'en finir avec son image sulfureuse. Il faut dire que ce media center (Windows, MacOS, Android, Raspberry Pi, etc.) est souvent associé au piratage de contenu : films, séries, retransmissions sportives, etc. Il ne s'agit pas du fait de l'éditeur, mais des nombreuses extensions qui le permettent. En effet, comme le code est libre, n'importe qui peut faire ce qu'il veut avec. Au lieu d'interdire et de faire la guerre aux développeurs indépendants, Kodi a décidé de proposer du contenu légal et payant. On leur souhaite bonne chance, mais il faut rappeler que d'autres s'y sont essayés sans rencontrer le succès : Vuze, BitTorrent, etc.




# LA CIA FAIT SON TRAVAIL ET ÇA SURPREND TOUT LE MONDE !

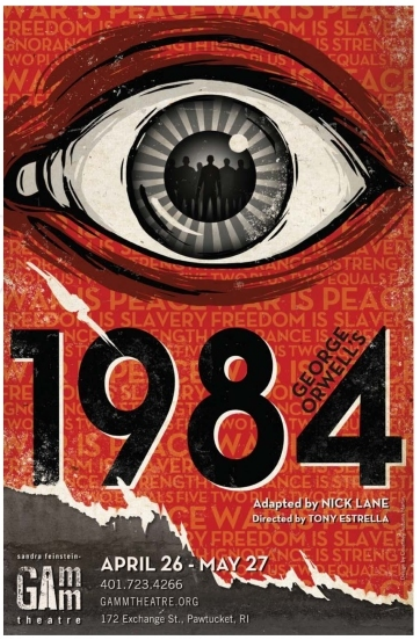
**Alors que le soufflé «Snowden» est retombé auprès du grand public et que les nouveaux maîtres de la nov'langue rangent ces révélations dans la case «théorie du complot», voici que Wikileaks en remet une couche avec la publication de documents prouvant que la CIA dispose de moyens d'espionnage très avancés. Voyons de quoi il s'agit et pourquoi ça ne surprend pas la rédaction de *Pirate Informatique*...**

Depuis qu'il est confiné dans l'ambassade d'Équateur à Londres, Julian Assange fait plus parler de lui que sa création : Wikileaks. Et pourtant, ce site vient dernièrement de frapper un grand coup en mettant en ligne 1 Go de documents datés de 2013 à 2016 et qui proviendraient du pôle high-tech de la CIA. Une sacrée collection qui, selon le site, ne représenterait que 1 % des documents en sa possession. On peut donc compter sur plusieurs autres «fournées» dans un avenir proche. Comme vous avez pu l'entendre ou le lire ailleurs, il s'agit de documents détaillant comment les hackers de l'Oncle Sam développent des techniques pour infiltrer tout ce qui se connecte à Internet. On apprend donc que la CIA

tente de contourner les antivirus pour infecter des ordinateurs et des téléphones portables de toutes marques. Pourquoi tenter de cracker les protocoles chiffrés utilisés par Signal, WhatsApp ou Telegram lorsqu'il suffit de récupérer les messages avec une sorte de keylogger avant même qu'ils ne soient chiffrés ? On arrive carrément dans le roman d'anticipation lorsqu'on apprend que les services secrets américains peuvent mettre sur écoute les possesseurs de certains types de téléviseurs. Si vous avez déjà vu ou lu *1984* cela vous fera sans doute sourire (ou pas). Vous vivez dans une cave et votre PC n'est relié à aucun réseau ? Pas de problème puisque la CIA sait comment mettre un malware sur un DVD «vierge» qui ira contaminer tout ce que vous graverez dessus. Ce sont pas loin de 500 programmes qui ont été décrits dans ces fichiers même si pour des raisons évidentes, Wikileaks n'a pas publié les codes et garde au chaud d'autres révélations pour supposément laisser le temps aux éditeurs et fabricants et colmater les failles.

## On ne reproche pas aux balayeurs de balayer...

Mais est-ce que les informations contenues dans ces documents sont si choquantes que cela ? Quel est le travail de la CIA au juste ? La protection des États-Unis contre leurs ennemis. Là où les révélations de Snowden montraient que la NSA espionnait tout le monde - y compris les amis des USA - on apprend ici que la CIA fait simplement son travail. En effet, je n'aime pas que mes conversations téléphoniques ou électroniques soient captées et stockées, mais nous parlons ici d'attaques ciblées. Cela fait certes très peur d'entendre que si la CIA peut conduire à distance votre voiture dans un ravin si elle vous a dans le nez, mais cela demande de gros moyens et dans la plupart des cas, un accès physique aux appareils. Bref, ce n'est pas parce que vous avez installé Tor ou parlé à votre cousin pro-Poutine au téléphone que la CIA va envoyer un espion mettre un mouchard dans votre iPhone 7. Mais ce qui fait vraiment peur c'est qu'on apprend que la CIA est très gourmande de failles *0day* qu'elle achète sur le darknet (comme Sergueï, le *black hat* de Biélorussie) puis les stocke dans un placard pour s'en servir un jour. C'est effrayant et débile, car au lieu d'avertir les personnes ou services concernés, l'agence laisse des trous béants au risque de léser ses propres concitoyens. Car ces failles seront forcément utilisées par des gens malintentionnés un jour ou l'autre... Et bien sûr, la CIA prétend ne pas espionner les citoyens américains, mais c'est aussi ce que disait la NSA avant 2012. Pour nous, les «*non-citizen*», cela ne change rien d'autant qu'il est connu que la CIA opère sur le sol européen depuis le consulat américain à Francfort. Mais que fait la *Polizei* ?




## Bons baisers de Russie ?

Les autorités américaines déploient de gros moyens pour trouver qui a bien pu livrer ces documents, mais il est probable qu'on ne trouve jamais le ou les coupables. C'est aussi pour cela que la CIA et le FBI ont commencé une campagne de dénigrement de WIkileaks. Certes l'image du site s'est un peu détériorée avec de récents scoops un peu réchauffés ou des publications pas vraiment indispensables (comme la vidéo du camion lors de l'attentat de Nice), mais certains démocrates américains vont carrément dénoncer des accointances avec la Russie depuis que, selon eux, Hillary Clinton a perdu les élections à cause de l'affaire des e-mails de leur parti. Ambiance guerre froide. De son côté Wikileaks accuse à demi-mot la CIA de commanditer des opérations sous faux Drapeau en se faisant passer pour des hackers russes...

# HACKTUALITÉS

# LES EXPERTS NOUS RÉPONDENT

**Parce qu'il n'y a pas qu'Edward Snowden qui milite contre la surveillance de masse en apportant des solutions de sécurité... ils sont quelques-uns en France, à se battre pour la préservation de vos données personnelles. Chercheurs ou entrepreneurs, mais surtout experts... nous vous présentons ici les acteurs de la sécurité au travers de questions d'actualités.**


**Mounir Idrassi**

A commencé sa carrière professionnelle chez un fabricant de cartes à puce (Oberthur Technologies) où il a travaillé sur différentes problématiques autour de la cryptographie et la sécurité informatiques. Créateur de l'entreprise IDRIX spécialisée dans le conseil et le développement de logiciels autour de la carte à puce. À l'origine de VeraCrypt (2013), l'héritier de TrueCrypt pour le chiffrement de données, il planche sur l'amélioration et l'apport de nouvelles fonctionnalités à ce dernier afin de lui offrir une meilleure intégration dans les entreprises.

**Laurent Brault**

Diplômé des grandes écoles de commerce et de Gestion (HEC) Laurent est un spécialiste en gestion de projet IT en France et à l'international. Il fonde sa société de conseil en sécurité informatique LBR Conseil en 2007 qui devient MDK Solutions en 2012. Il travaille sur le développement de 3 nouveaux produits autour de la KryptKey, la clef USB facilitant le chiffrement de tout ce qu'elle stocke : une nouvelle KryptKey allégée, une version Pro permettant la sauvegarde automatique et un tout nouveau modèle. En parallèle, sa société développe un nouveau produit mystère, qualifié d'innovant et de surprenant.

## Jean-Pierre Lesueur

Président de la société PHROZEN. À l'origine du RAT DarkComet utilisé par plus d'un million de personnes à travers le monde en seulement quatre ans (arrêté en 2012 pour cause ormation (Winja, RunPE Detector, etc.) Il travaille également sur Phrozen Keylogger, soft qui promet d'être le meilleur outil de surveillance pour Microsoft Windows.

## Éric Filiol

Scientifique de formation (mathématiques et informatique), Éric a passé 22 ans dans l'armée (infanterie/ troupes de marine). Il dirige à présent un laboratoire de recherche en sécurité qui adopte prioritairement la vision de l'attaquant pour justement anticiper les risques. Il s'attelle depuis plus de 20 ans à la cryptanalyse des systèmes de chiffrement symétriques. Son laboratoire publiera en fin d'année une analyse sur le réseau Tor. De plus, il travaille sur GostCrypt. Fork de TrueCrypt. Le projet est en pleine refonte : nouvelle version avec une nouvelle interface, un code sécurisé et de nouveaux algorithmes.

**Suite aux révélations de WikiLeaks concernant le piratage par la CIA des appareils connectés (pour les transformer en outils d'espionnage) en exploitant des failles zero-day. Comment faire à l'heure du tout connecté, pour garder sa vie un peu «privée» ?**

**J.P.L :** Les mots « vie privée » et « tout connecté » ne sont pas compatibles. Dès lors que vous soumettez à un tiers une information, vous vous exposez au risque d'une interception de cette dernière. Les pirates ou les services gouvernementaux peuvent la récupérer en exploitant une faille ou une mauvaise implémentation d'un protocole de chiffrement.

**M.I :** Aujourd'hui, on est dans une situation catastrophique pour la protection de la vie privée, car les grands acteurs de l'informatique ont imposé un modèle à l'antipode de la protection de la vie privée. Néanmoins, il commence à y avoir des alternatives proposant un meilleur respect de la vie privée, même si cela reste limité.

**L.B :** L'explosion du ItoT permet l'émergence de nouveaux usages... cela ouvre aussi la voie à l'exploitation « occulte » des données. Aucune surprise à constater que la CIA est en 1ère ligne sur cette voie. Mais de nombreuses grosses sociétés font de même (banques, assurances...). Comment se protéger ? La méthode la plus efficace serait de ne pas avoir/utiliser des objets connectés. Il faut donc à minima limiter leur utilisation et leur capacité.

**E.F :** Il faut relativiser la portée technique de ce leak. Les techniques et approches opérationnelles utilisées sont classiques et déjà anciennes. En revanche, ce qui est intéressant c'est l'usage des vulnérabilités et autres 0-days. Cela montre que l'on peut avoir la technologie de protection de l'information que l'on veut,mais si on la met en œuvre sur des matériels fournis par l'adversaire (OS, matériels...), il est illusoire d'imaginer être protégé.

**Que pensez-vous des messageries sécurisées de type Signal, Telegram ? Sont-elles des solutions viables pour récupérer un peu le contrôle sur nos vies privées et sur les fichiers que nous échangeons ?**

**J.P.L :** «Signal» et «Telegram» renforcent incontestablement notre vie privée, mais comme nous l'avons vu avec la fuite de Vault7, nous ne sommes pas à l'abri de failles ou de bugs permettant d'abaisser leurs niveaux de sécurité et finalement de nous exposer tout autant à une fuite d'informations utilisables par un gouvernement ou des pirates.

**M.I :** Pour moi, les dangers sur la vie privée viennent d'abord des terminaux (smartphone, ordinateur). En ce qui concerne les messageries sécurisées, c'est la meilleure solution aujourd'hui pour avoir un peu de contrôle, mais je ne recommande pas Signal ou Telegram car ils obligent à partager le numéro de téléphone et le carnet d'adresses. Je recommande plutôt Wire qui utilise le même système de chiffrement que Signal, mais qui ne requiert ni numéro ni carnet d'adresses.

**L.B :** La sécurité repose sur la confiance que l'on peut accorder à la société qui la délivre. En supposant que Signal et Telegram ne donnent pas accès aux flux de données échangés qu'ils gèrent, le service proposé ne protège que la phase d'échange. Il existe des services de gestion de chiffrement d'email, développés par des sociétés françaises, pour échanger des photos/vidéos en toute sécurité.

**E.F :** Dans le principe oui comme toute solution de chiffrement, mais le problème se situe ailleurs. Ces applis sécurisées doivent être vues comme des portes blindées. Mais à elles seules elles ne sont pas suffisantes. Pour prolonger l'analogie, si cette porte blindée est installée sur un mur en carton, il suffit de passer par le mur. Or l'existence persistante (voire entretenue à mon avis) des vulnérabilités permet justement de s'assurer que le mur sera toujours moins solide que la porte.

**Avez-vous en tête des solutions contre la surveillance de masse ?**

**J.P.L :** Préférez par ordre de préférence croissant : XMPP + OTR, Telegram, Signal pour communiquer avec vos amis ou collègues. Utilisez PGP (Pretty Good Privacy) autant que possible pour

# HACKTUALITÉS

chiffrer vos e-mails avec une clef de taille minimum de 4096 bits. Surfez couvert au moyen d' un bon VPN (Virtual Private Network) tel que Ipredator que je recommande fortement.

**M.I :** La décentralisation est la clef contre la surveillance de masse. Les solutions techniques à base de P2P ou blockchain existent et elles ont prouvé leur efficacité. On peut citer par exemple Tox ou Bitmessage. Néanmoins, elles souffrent souvent de problèmes de complexité et de manque de souplesse en environnement mobile. Ceci réduit le nombre de leurs utilisateurs.

**L.B :** Le fort développement du BigData et des nouvelles technologies (ItoT,...) a amplifié la surveillance. Une grande majorité des gens n'a pas conscience de la masse d'informations collectées, ni de la façon dont ces données sont obtenues. Il est illusoire de penser pouvoir contrôler ces collectes et l'utilisation qui en sont faites. Il faut au moins sensibiliser.

**E.F :** Techniquement utilisez systématiquement le chiffrement (données, mails...). Évitez de céder aux sirènes technologiques. On vit très bien sans Facebook et autres réseaux sociaux. Fuyez les objets connectés et tout ce qui est smart (on vit aussi très bien sans). Il faut se dire que « smart » et « connectés » sont devenus synonymes de surveillance. Redevenir citoyen et cesser de n'être que des consommateurs.

**LA VIE PRIVÉE DES JEUNES GÉNÉRATIONS EST DE PLUS EN PLUS EXPOSÉE (RÉSEAUX SOCIAUX, APPLIS, ETC.), POUR LEUR APPRENDRE À SE PROTÉGER, FAUT-IL INCULQUER LA NOTION DE VIE PRIVÉE À L'ÉCOLE ?**

**J.P.L :** Il serait en effet important de voir les nouvelles générations être sensibilisées dès le plus jeune âge à l'utilisation de l'outil informatique ainsi qu'aux services auxquels ils nous rattachent. D'autant plus que l'informatique touche une population de plus en plus jeune et par conséquent à faible maturité, ce qui l'expose aux risques liés aux nouvelles technologies.

**M.I :** Il est essentiel de leur apprendre les dangers liés à cette surexposition et de leur inculquer l'importance de protéger leur vie numérique. Les jeunes sont particulièrement vulnérables aux fausses applis et aux différentes attaques (comme le phishing) et je pense que c'est le devoir des autorités d'inclure dans les programmes scolaires la notion de protection de la vie numérique.

**L.B :** Ils se rendent rarement compte de la façon dont les données sont collectées et encore moins de leur possible exploitation . Il faudrait leur expliquer tous les aspects du BigData, tout ce qui permet au « bon » BigData de se développer, et comment participer à ce développement.Il faut également leur expliquer ses côtés « cachés » permettant au « mauvais » BigData de prospérer.

**E.F :** Sans vie privée, c'est-à-dire la possibilité de faire des bons ou mauvais choix, nous subirons la dictature de la transparence (sauf pour les hommes politiques qui n'ont pas oublié de s'organiser quelques exemptions). Cela veut dire que très vite nos choix seront normés. Nous aurons perdu alors notre liberté. La vie privée est constitutive de notre liberté.

# NOUVEAU !


**Par l'équipe de *Pirate Informatique* !**

*L'officiel PC*
**RASPBERRY PI**
Idées & Projets Clés en Main

**GUIDE COMPLET**

**CHEZ VOTRE MARCHAND DE JOURNAUX**

# IPREDATOR + OPENVPN, LE COMBO GAGNANT !

**Depuis le temps que vous nous le demandiez, le voici ! Cet article a pour but de présenter OpenVPN et de passer à la pratique sur PC et mobile. Mais comme OpenVPN ne se suffit pas à lui même, nous avons choisi de faire le test avec le service IPredator basé en Suède. Bien sûr, vous êtes libre de choisir votre prestataire, la mise en place se fait à peu près de la même manière.**

Espionnage de votre gouvernement ou de la NSA, piratage de vos données personnelles, infection de virus... Surfer sur Internet n'est pas sans danger, surtout avec la multiplication des points d'accès WiFi où il est compliqué de vérifier la sécurité. Une solution pour y remédier : passer par un VPN, ou Virtual Private Network. Le principe est simple : une fois le VPN activé, les données envoyées quand vous serez sur Internet passeront par un «tunnel» où elles seront chiffrées, rendant impossible l'espionnage ou l'interception de vos données. Vous aurez même le droit à une IP dans un autre pays pour brouiller les pistes. À part quelques rares exceptions, les VPN sont devenus des services commerciaux payants et même si dans notre numéro 27 nous avons vu comment auto-héberger un VPN à la maison avec un Raspberry Pi, tout le monde n'a pas de Rasberry Pi ou la volonté de faire un tel montage. Miser sur un service payant c'est aussi avoir moins de risques d'avoir affaire à des charlatans ou des incompétents.

## POURQUOI CHOISIR IPREDATOR ?

Pour cette démonstration nous avons choisi IPredator, car même s'il se situe dans un pays qui oblige à conserver les données, l'équipe a volontairement diversifié les zones géographiques pour chaque pièce du puzzle : conservation des données, propriété du service, du serveur, du réseau, etc. Le but est de rendre toute tentative de harcèlement juridique difficile, voire impossible. L'IP

réelle du client est utilisée le temps de la connexion et c'est tout. Bien sûr, il faut les croire sur parole pour ce dernier détail, mais après tout, les personnes à l'origine du projet sont les 3 enfants terribles de Pirate Bay : Gottfrid Svartholm, Fredrik Neij et Peter Sunde. On peut tomber plus mal comme caution. Le problème des VPN payants c'est...qu'il faut les payer ! Et l'argent laisse des traces. IPredator se plie en quatre pour proposer le plus de moyens de paiement possibles dont certains sont anonymes : carte de crédit prépayée (il suffit de l'acheter avec du liquide), BitCoin (même si le BitCoin n'est pas anonyme à la base, il est possible de passer par Tor et de réduire les risques).

## POURQUOI CHOISIR OPENVPN ?

Le protocole PPTP est disponible sur IPredator, mais il est fortement déconseillé, car considéré comme cassé. En effet, même s'il est disponible sans installation supplémentaire sous Windows, son chiffrement de 128 bits est considéré comme faible à présent. À l'inverse, OpenVPN propose un chiffrement minimum de 256 bits (avec un maximum de 2048 bits chez IPredator). Rien ne laisse penser dans les révélations de Snowden qu'OpenVPN a été affaibli ou corrompu par la NSA (surtout couplé avec Tor). Il est également considéré comme immunisé aux attaques de la NSA grâce à ses échanges de clés éphémères et à l'utilisation de systèmes de chiffrement modernes gourmand en ressource (ce qui est problématique avec l'autonomie réduite de nos appareils mobiles) et est un peu plus compliqué à mettre en place. Heureusement, Viscosity (un «fork» d'OpenVPN pour PC) simplifie les choses en proposant une interface intuitive et la gestion du fichier .ovpn contenant vos informations personnelles pour accéder au «tunnel». Le logiciel est gratuit 30 jours puis coûte 8,50 € à l'achat. Avec les 6 €/mois du service IPredator, cela fait un petit budget à prévoir au début de l'aventure, mais c'est le prix de la tranquillité. Sur mobile, le client OpenVPN for Android est gratuit et vous pouvez bien sûr connecter 2 appareils en même temps en étant abonné. Il ne s'agit pas d'une limitation d'IPredator, mais d'OpenVPN.

## POURQUOI UTILISER UN VPN ?

- Éviter l'espionnage et les attaques (cela va des services secrets aux pirates en passant par HADOPI)
- Protéger son emplacement
- Se connecter en toute sécurité sur un point d'accès WiFi inconnu
- Rester anonyme sur Internet
- Contourner la géolocalisation de certains sites (avoir le Netflix US en France par exemple même s'il faudra en plus utiliser Tor, car IPredator ne propose qu'une IP suédoise que vous pouvez faire «rebondir» avec Tor)
- Contourner le bridage de certains sites ou services si un jour la neutralité du Net n'était pas respectée


**Attention lorsque vous allez choisir votre mot de passe ! Même si IPredator ne bronchera pas, les caractères spéciaux sont parfois problématiques avec Viscosity. Nous avons été bloqués plusieurs heures avant de comprendre que le problème venait du caractère «ç» que nous avions placé dans notre sésame...**

## LES SERVICES ANNEXES D'IPREDATOR

En plus du VPN, IPredator ne vous lâche pas dans la nature et propose d'autres services compris dans le prix (et comme ils nous versent 20 000 €/mois pour en parler, on va bien insister là-dessus) :

- Un proxy
- Un nœud de sortie Tor
- Un service de messagerie instantanée Jabber (avec OTR)
- Un service permettant de voir si votre VPN est bien étanche
- Un service d'e-mail anonyme
- Et encore d'autres options que nous nous ferons un plaisir de détailler si vous vous manifestez

Lien : **https://ipredator.se/page/services**

PAS À PAS

# Période d'essai et inscription

CE QU'IL VOUS FAUT

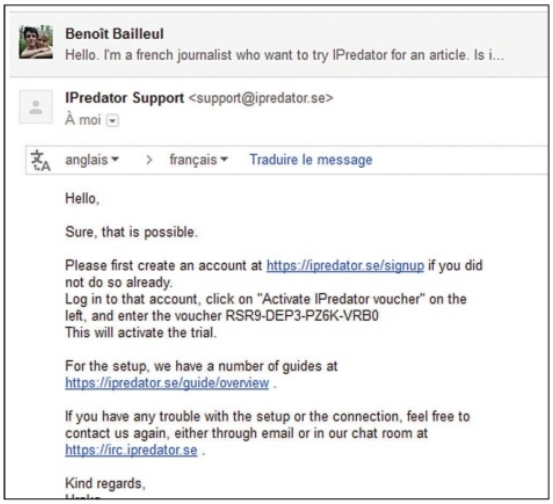
**IPREDATOR**

OÙ LE TROUVER ? :
**https://ipredator.se**

DIFFICULTÉ :

## 01 TROIS JOURS D'ESSAI

Il est apparemment impossible de payer directement pour un mois ou plus, il faudra d'abord demander une période d'essai de 72 heures (sans doute font-ils cela pour éviter de rembourser les n00bs qui n'arriveront pas à faire fonctionner le VPN). Envoyez une demande en anglais à cette adresse : **support@ipredator.se**. Pas besoin de faire du Shakespeare, aidez-vous de Google Traduction. Au bout de trois heures nous avons reçu notre code pour une période d'essai. Pas de carte bancaire à sortir donc...



**Benoît Bailleul**
Hello. I'm a french journalist who want to try IPredator for an article. Is i...

**IPredator Support** <support@ipredator.se>
À moi

anglais › français Traduire le message

Hello,

Sure, that is possible.

Please first create an account at https://ipredator.se/signup if you did not do so already.
Log in to that account, click on "Activate IPredator voucher" on the left, and enter the voucher RSR9-DEP3-PZ6K-VRB0
This will activate the trial.

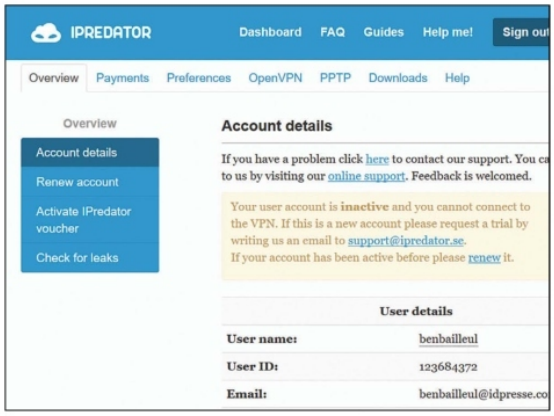
For the setup, we have a number of guides at https://ipredator.se/guide/overview .

If you have any trouble with the setup or the connection, feel free to contact us again, either through email or in our chat room at https://irc.ipredator.se .

Kind regards,

## 02 VOTRE COMPTE

Ouvrez un compte, identifiez-vous et sur la gauche, cliquez sur **Activate IPredator voucher** et entrez le code pour activer votre compte. Vous serez alors dirigé




vers le **Dashboard** d'où vous aurez accès à vos données, vos fichiers de configuration, etc. Lorsque votre période d'essai sera terminée, c'est dans **Renew Account** qu'il faudra aller pour payer et **Check for Leak** permet de voir si votre VPN est bien étanche lorsqu'il sera installé. En haut, **Guides** vous propose des tutos pour tous les appareils compatibles.

PAS À PAS

# Sous Windows 10 avec Viscosity

CE QU'IL VOUS FAUT

**VISCOSITY (OPTIONNEL)**

OÙ LE TROUVER ? :
**www.sparklabs.com/viscosity**

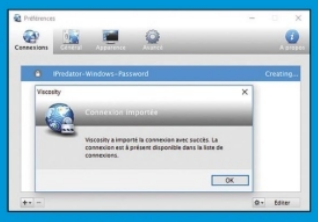
DIFFICULTÉ :

## 01 UNE OFFRE UNIQUE POUR TOUS LES SYSTÈMES


Sous Windows, on a le choix entre le client OpenVPN de base ou le client Viscosity, payant, mais plus simple et disposant d'une interface graphique et d'un très bon système d'import/export de configuration. Heureusement Viscosity dispose d'une version d'essai de 30 jours. À vous de voir ensuite si ce dernier vaut les 9 $ (8,50 €) que l'éditeur vous réclamera. Si vous pensez le contraire, le client historique est à peine plus compliqué et vous trouverez de l'aide dans **Guides**. Notez que IPredator fonctionne sous Linux, iOS, MacOS, etc.

## 02 VOTRE FICHIER .OVPN PERSONNEL

Téléchargez Viscosity, installez-le et dans votre **Dashboard**, téléchargez aussi le fichier **IPredator-Windows-Password.ovpn**. Lancez Viscosity puis dans la zone de notification, faites un clic droit dans l'icône correspondant au client et choisissez **Préférences**. Dans cette nouvelle fenêtre, faites **+** puis **Importer connexion > À partir du fichier** puis trouvez le fichier **.ovpn**. Vous devriez voir **Connexion importée** si tout se passe bien.



PAS À PAS

# Sur Android avec OpenVPN

**CE QU'IL VOUS FAUT**

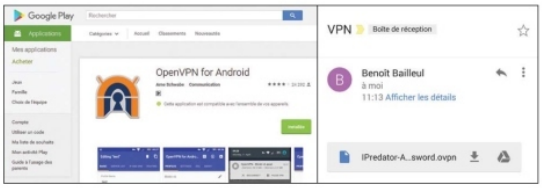
**OPENVPN**

OÙ LE TROUVER ? :
**https://goo.gl/mS7k3g**

DIFFICULTÉ :

## 01 VOTRE FICHIER .OVPN PERSONNEL

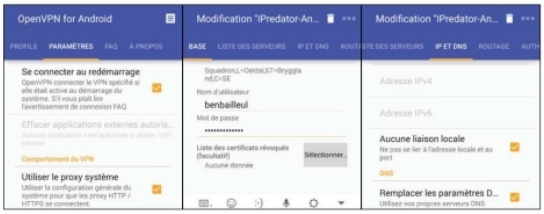
Pour Android, pas besoin d'avoir un appareil rooté. Installez **OpenVPN for Android** (celui-là et pas un autre !) et téléchargez aussi le fichier **IPredator-Android-NAT-Password.ovpn**




depuis **Dashboard**>**Download**>**Configuration File**. Envoyez ce fichier sur votre mobile (par e-mail, Bluetooth, câble USB ou carte SD) puis ouvrez l'application OpenVPN for Android.

## 02 QUELQUES RÉGLAGES...

Ouvrez l'onglet **Paramètres** et cochez toutes les cases sauf la dernière. Dans **Profil**, cliquez dans les trois petits points en haut à droite et faites **Importer un profil depuis un fichier .ovpn**. Retrouvez votre fichier dans le smartphone et cliquez sur l'icône jaune en forme de disquette (comment ça, *c'est quoi une disquette* ?). Dans **Base**, entrez les identifiants que vous avez utilisés pour l'inscription. Dans **IP et DNS**, cochez **Aucune liaison locale** et **Remplacer les Paramètres DNS**. Tapez **ipredator.se** en suffixe, **194.132.32.23** et **46.246.46.46** dans les DNS primaire et secondaire.

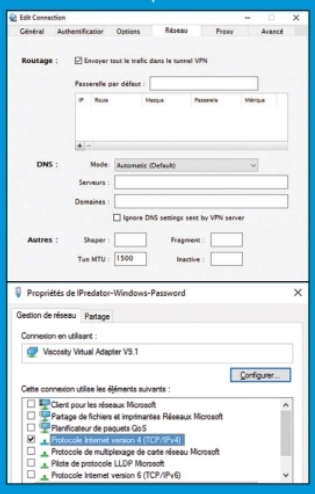



## 03 CONNEXION, VÉRIFICATION ET RÉSULTAT

Enfin, dans **Profils**, cliquez sur **IPredator** et lancez le VPN. Si tout se passe bien vous devriez voir une petite clé ou le symbole VPN du système Android en haut avec le débit entrant et sortant dans votre zone de notification (le volet qui se déroule à partir du haut). Vérifiez que tout est en ordre et qu'il n'y a pas de fuite avec cette URL : **https://check.ipredator.se**. Et n'oubliez pas de passer par Orbot, la version mobile de Tor (voir *Pirate Informatique* n°30 ou les *Dossiers du Pirate* n°11 encore en kiosques). Bravo, vous êtes anonyme !


## 03 QUELQUES RÉGLAGES...

Sélectionnez maintenant **Éditer** et allez dans l'onglet **Réseau** pour cocher la case **Envoyer tout le trafic dans le tunnel VPN**. Vous n'avez pas besoin de faire autre chose. Cliquez sur **Sauvegarder**. Maintenant il va falloir désactiver des services dans la connexion en passant par Windows. Ouvrez le menu **Démarrer**, allez dans **Paramètres** > **Réseau et Internet** > **VPN** > **Modifier les options d'adaptateur**. Effectuez un clic droit sur **IPredator** et sélectionnez **Propriétés**. Décochez toutes les cases sauf **Protocole Internet version 4 (TCP/IPv4)**. Validez avec **OK**. Dans la zone de notification (en bas à droite) faites un clic droit dans l'icône de Viscosity, cliquez sur **Détails** et laissez cette fenêtre ouverte.




## 04 CONNEXION, VÉRIFICATION ET RÉSULTAT

Toujours dans la zone de notification cliquez sur **Connecter IPredator**. Il ne vous reste qu'à rentrer les identifiants que vous avez utilisés pour l'inscription et vous pourrez voir dans la fenêtre **Détails** que vous êtes connecté. En faisant un test de bande passante, nous sommes passés de 10,15 à 7,62 Mbit/s en téléchargement (et de 725 à 622 Kbit/s en upload). La différence est imperceptible avec un navigateur ou en téléchargement Torrent. Par contre le ping est passé de 28 à 227 : OpenVPN n'est pas vraiment l'ami des gamers. Vérifiez que tout est en ordre et qu'il n'y a pas de fuite avec cette URL : **https://check.ipredator.se**. Et n'oubliez pas de passer par Tor en plus pour brouiller les pistes et disposer d'autres «pays de complaisance» !

# LES DOSSIERS DU Pirate

## DES DOSSIERS THÉMATIQUES COMPLETS

**À DÉCOUVRIR EN KIOSQUES**

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES


Actuellement

#Guide pratique

**GUIDE POUR SMARTPHONE & TABLETTE**

# SÉCURISER VOS ACHATS EN LIGNE AVEC QWANT


**L'application mobile Qwant n'est pas qu'un moteur de recherche anonyme. Avec l'intégration du navigateur Liberty et du système de « Vault », ou coffre-fort, elle permet d'acheter en ligne en toute sécurité.**

Début 2017, Qwant, moteur de recherche anonyme qui veut faire oublier le « tout Google » (93 % des recherches Web en France) part à l'assaut du mobile avec une application dédiée. En plus de la recherche, elle embarque un navigateur sécurisé, Liberty, et un système de « Vault » pour sécuriser les achats en ligne. Le principe de ces coffres-forts est simple : vous enregistrez vos informations personnelles et de paiement, celles-ci sont ensuite chiffrées et stockées sur l'appareil, pas sur un serveur externe. Au moment de payer, et uniquement à ce moment-là, les informations sont transmises à la boutique. Est-ce que ça change quelque chose ? Tournez la page et Éric Léandri, co-fondateur de Qwant, vous répond (*spoiler alert:* oui).

## UNE ERGONOMIE À REVOIR

L'idée est intéressante, mais la réalisation n'est pas encore au rendez-vous. À l'heure où nous écrivons ces lignes, la navigation sur Liberty est confuse et assez saccadée, malgré une bonne connexion, les pages chargées ne sont pas forcément les bonnes (on appuie sur un site, et c'est le précédent qui s'affiche), tandis que le plein écran est impossible en lecture vidéo. Bien sûr, ces imperfections vont sans doute être corrigées à l'heure où vous lirez ces lignes… Le système de Vault, lui, est simple à mettre en place, une fois qu'on a compris où chercher. Et à partir de là, rien à dire : enregistrement des identifiants et des mots de passe (en local, on le rappelle) puis remplissage automatique fonctionnent sans faille.

## LEXIQUE

***OPEN SOURCE :** Licence sous laquelle est distribué le code source d'un programme, que chacun est alors libre de consulter et modifier. Le code peut être publié après ou pendant le développement. Dans ce dernier cas, l'idée est souvent de mener à bien un projet collaboratif, où plusieurs développeurs participent en même temps.

PAS À PAS

# Créer et alimenter un Vault

CE QU'IL VOUS FAUT

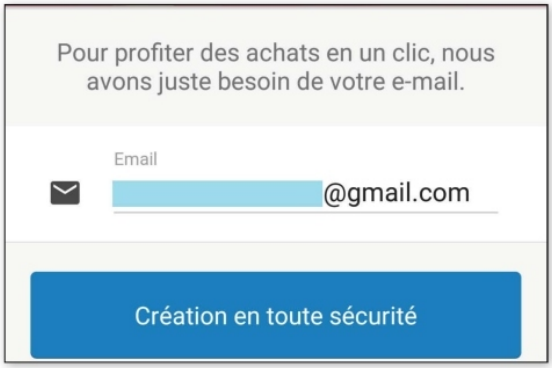
**QWANT**

OÙ LE TROUVER ? : **https://goo.gl/XYLCly**

DIFFICULTÉ :

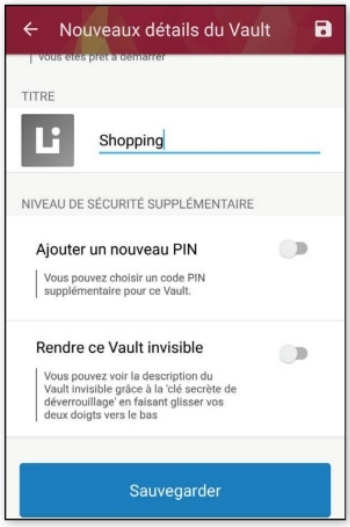
## 01 CRÉER UN COMPTE

Pour utiliser toutes les capacités de Liberty et des Vaults, notamment le paiement en un clic sécurisé, il faut créer un compte. Touchez l'icône de Liberty en bas à droite et faites **Suivant** jusqu'à tomber sur **Inscrivez-vous** et suivez la démarche. Il faudra également définir un code PIN, à utiliser pour l'accès/modification des Vaults et informations de paiement.




## 02 CRÉER UN VAULT

La création du compte terminée, vous atterrissez sur la **TapMap**, une grille contenant vos favoris et vos Vaults. Touchez le «+» **> Nouveau Vault > Accessories** (par exemple, cela n'a pas d'importance puisque vous allez le modifier). Changez le **Titre** et, si vous le souhaitez, ajoutez un **Niveau de sécurité supplémentaire**. Validez avec **Sauvegarder**.



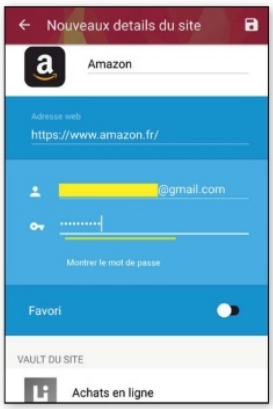

# *Interview de Eric Léandri*

## Co-Founder & CEO QWANT

### POURQUOI LANCER UNE APPLICATION?

C'est malheureusement une obligation. Les navigateurs mobiles installés par défaut (Chrome et Safari) ne permettent pas de mettre Qwant en moteur de recherche. Vous avez juste le choix entre quatre américains. Seul Firefox, avec qui nous avons conclu un partenariat, le permet. Le problème, c'est que Firefox n'est pas très répandu sur mobile, et que, quand bien même, les gens changent très rarement leur moteur de recherche par défaut.
Nous savions aussi que les applications ne sont quasiment jamais utilisées pour la recherche Internet. Pour cela, vous ouvrez votre navigateur et vous cherchez, vous ne vous servez pas de l'application Google prévue pour ça.
L'application Qwant devait donc proposer quelque chose de nouveau, d'où les trois fonctions : recherche

## 03 AJOUTER UN SITE



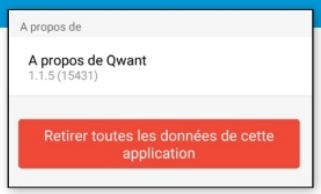

Revenez sur la **TapMap** pour toucher le «+» puis **Nouveau site**. Cherchez dans la liste s'il n'est pas déjà répertorié avec la loupe en haut à droite. Sinon, il faudra le créer manuellement. Entrez l'Adresse Web, vos identifiants et touchez le Vault du site pour l'inclure dans celui de votre choix. Validez avec **Sauvegarder**. En accédant à ce site via Liberty, les identifiants sont désormais automatiquement renseignés.

## 04 AJOUTER UNE CARTE DE PAIEMENT

Il est possible d'enregistrer une carte de paiement directement dans Liberty pour sécuriser les achats en ligne. Dans le navigateur Liberty, ouvrez le menu hamburger et allez dans **Portefeuille**. Touchez le «+» et autorisez l'accès à l'appareil photo pour prendre la carte en photo et remplir automatiquement les informations demandées, ou refusez et entrez-les manuellement.


## SUPPRIMER SON COMPTE

L'application intègre une solution très simple pour effacer toutes les informations enregistrées dans Qwant. Une fois dans le menu hamburger de Liberty, allez dans les Paramètres, descendez et touchez **Retirer toutes les données de cette application**. Votre compte est totalement supprimé en quelques secondes. Un système que l'on aimerait voir plus souvent !




simple sécurisée, choix parmi des applications partenaires respectueuses de la vie privée et navigateur Liberty, lui aussi sécurisé.

### Pourquoi intégrer le Vault? Comment ça fonctionne?

Nous pensions qu'il fallait proposer une solution de shopping en ligne sécurisé. Aujourd'hui, vous êtes pisté pendant votre achat, parce que vos informations sont stockées ailleurs que dans votre appareil. Les prix et les disponibilités peuvent donc changer alors qu'ils ne devraient pas. Grâce au système de Vault, vos recherches sur les sites marchands, vos informations personnelles et de paiement... Tout est chiffré et stocké en local sur votre mobile. Autrement dit : le site marchand n'a accès aux informations pour finaliser la vente qu'au tout dernier moment.

Pour faire une comparaison avec la vraie vie, imaginez que vous vouliez acheter un sac. Actuellement, la boutique sait que vous avez une carte de paiement « Platinium », et va vous dire qu'il ne reste plus qu'un exemplaire du modèle que vous voulez, au double du prix. Et si vous avez une carte basique, elle va plutôt vous proposer un crédit pour payer en dix fois. Avec le Vault, ce n'est plus possible. De plus, le déchiffrement des données avant leur envoi au marchand est dépendant de votre carte SIM et d'un code de votre choix. Si vous bloquez votre carte SIM après un vol ou une perte, plus personne ne peut utiliser ou avoir accès aux données.

### Comment permettre à ce système d'être adopté par le plus grand nombre?

Le problème technique actuel, c'est que le navigateur Liberty intégré à l'application est très sécurisé. C'est bien sûr une bonne chose, mais il bloque aussi ce que les utilisateurs aiment sur d'autres navigateurs : la personnalisation de l'interface, la gestion des favoris... En bref, les extensions auxquelles ils sont habitués. Notre but est donc d'ouvrir l'API de Vault pour pouvoir intégrer le système à n'importe quel navigateur mobile, sous forme d'extension. On a d'ailleurs commencé les tests. Pour arriver à faire adopter la sécurité, il faut donner à l'utilisateur quelque chose de simple.

### À terme, Qwant doit devenir Open Source?

Vers le mois de juin, nous publierons le code du « front » *[l'interface que voit l'utilisateur, ndlr]* de la version Web de Qwant. Pour moi, l'Open Source, c'est une belle finalité. Il faut d'abord que l'outil fonctionne, qu'il apporte quelque chose de qualité, sinon ça ne sert à rien d'ouvrir le code. Nous publierons aussi le code de l'extension quand elle sera prête.

# ENFIN UNE SOLUTION CONTRE LES RANSOMWARES !

**Dans nos numéros 26 et 31, nous vous mettions en garde contre les ransomwares, ces virus qui prennent en otage vos données les plus chères. Même si les éditeurs antivirus mettent le paquet pour contrer cette nouvelle menace, il existe une nouvelle solution efficace pour contrer les ransomwares avant même qu'ils ne passent à l'action...**

## LEXIQUE

***RANSOMWARE :**
C'est un malware qui sera introduit par un ver informatique. Le ransomware va cibler les types de fichiers ayant une valeur sentimentale ou pratique (photo, vidéo, DOC, XLS, etc.) et les chiffrer avec une double clé très solide. Au bout de quelques minutes, vos fichiers deviennent inaccessibles et un message s'affiche sur votre écran. Ce dernier vous invite à payer une somme d'argent pour récupérer la clé privée ayant servi au chiffrement et ainsi retrouver vos données.

Les ransomwares (ou «rançongiciels» dans la langue de Kev Adams) prennent en otage vos données en les chiffrant. Tout commence par un malware de type «ver» qui va charger un programme malicieux. Le renouveau du ransomware a débuté fin 2013 avec CryptoLocker, mais depuis l'année dernière, ce type de malware a le vent en poupe et on ne compte plus les variantes et versions alternatives. Une fois infecté, c'est fichu même s'il existe un espoir (voir notre encadré). Autant alors se protéger avec RansomFree. L'action de ce logiciel est basée sur l'analyse de 40 ransomwares et leurs variantes connues. Les développeurs ont réussi à comprendre le comportement de ces saletés. Dès que le schéma est détecté, RansomFree va bloquer le processus de chiffrement et protéger vos données. Vous pourrez choisir d'éliminer la menace ou de laisser faire. En effet, les faux positifs sont possibles. Nous avons essayé de déclencher l'alerte avec les logiciels VeraCypt et AxCrypt mais rien ne s'est passé. Il a fallu écrire un script Python dédié pour réveiller la bête.

PAS À PAS

# RansomFree : mode d'emploi

**CE QU'IL VOUS FAUT**

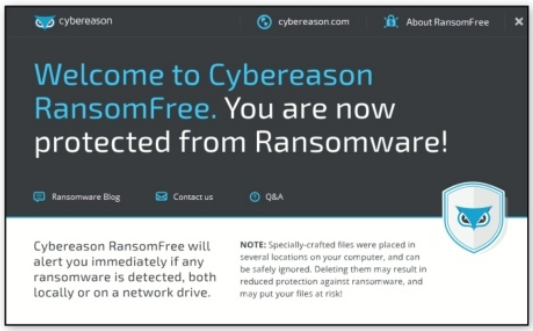
**RANSOMFREE**

OÙ LE TROUVER ? :
**https://ransomfree.cybereason.com**

DIFFICULTÉ :

## 01 RIEN À FAIRE !

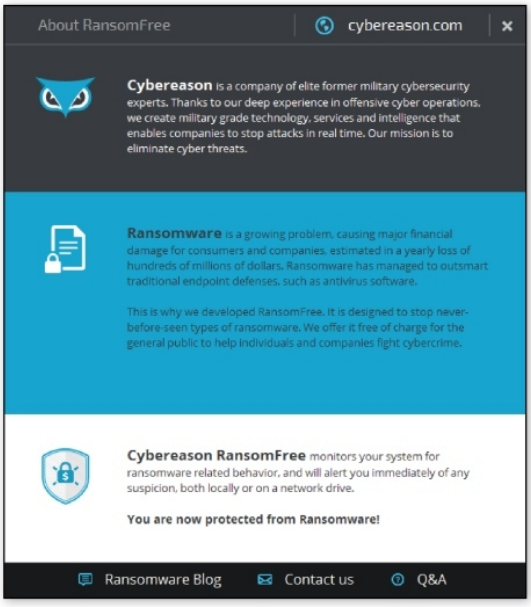
Dès l'installation, RansomFree va disséminer des fichiers leurres aux quatre coins de votre disque dur. Si un ransomware




tente de chiffrer vos données, il ira aussi s'attaquer à ces fichiers et déclenchera l'alerte. Vous n'avez rien à faire ni aucun réglage à effectuer.

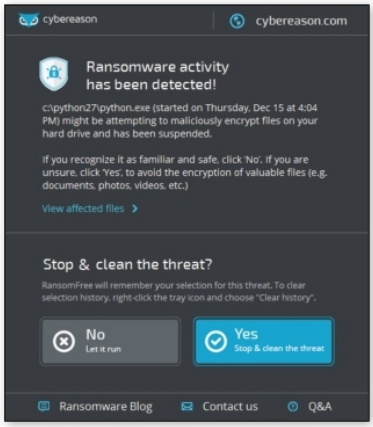
## 02 AU DÉMARAGE

RansomFree fonctionnera aussi si un disque dur réseau est attaqué. Notez que le logiciel sera actif au démarrage de Windows (pour les Mac, utilisez RansomWhere) même s'il ne figure pas dans la liste du **Gestionnaire des tâches**.



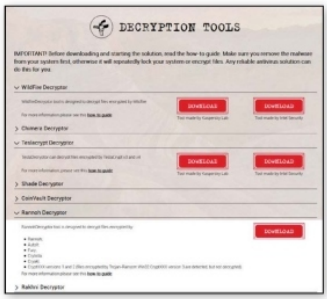

## 03 ALERTE !

En cas d'alerte, le processus incriminé est suspendu. Vous pouvez voir la liste des fichiers attaqués (**View affected files**), choisir de laisser faire (**No, Let it run**) ou au contraire bloquer définitivement le processus et faire le ménage (**Yes, Stop & clean the threat**).




## UN ESPOIR : LE CRYPTO SHERIFF

Depuis la dernière fois où nous vous avions parlé des ransomwares, un nouveau shérif est en ville. Alors il ne fait pas très peur (à cause de son embonpoint et de son pistolet à eau sans doute), mais il a le mérite d'exister et vous permettra, si vous avez de la chance, de trouver une solution à votre problème de ransomware. En effet, le site No More Ransom centralise tout ce qu'il faut savoir sur ces malwares au niveau de la prévention, mais il dispose aussi d'un service de détection en ligne (pour savoir de quel mal vous avez hérité) et de plusieurs outils de désencryption. Ce sont plus de 25 ransomwares qui peuvent être éradiqués avec ces outils : Wildfire, Teslacrypt (v3 et v4), Shade (extensions .xtbl, .ytbl, .breaking_bad et .heisenberg), CoinVault (et BitCryptor), Rannoh (ainsi que Fury, CryptXXX, Crybola, etc.), Rakhni (plus Chimera, Rotor). Bien sûr, dès qu'une solution est disponible elle est mise en ligne gratuitement. Cela vaut la peine d'essayer non ?




Lien : **www.nomoreransom.org**

# RICOCHET : LA MESSAGERIE SÉCURISÉE

**Grâce à l'utilisation du réseau Tor, Ricochet garantit un anonymat total pendant les conversations, au prix de quelques limitations.**

## LEXIQUE

***TOR :**
The Onion Router (Tor) est un réseau mondial décentralisé. Composé de serveurs appelés « nœuds », son but est d'anonymiser ses utilisateurs. Pour cela, la seule connexion à Tor ne suffit pas, et tout un tas d'outils sont mis à disposition par l'équipe en charge du projet, dont un navigateur basé sur Firefox, Tor Browser.

***CHIFFREMENT BOUT À BOUT :**
Les messages que vous envoyez à votre destinataire sont chiffrés sur votre PC avant d'être envoyés sur le réseau. Comme le serveur lui, ne fait rien d'autre que relayer le message chiffré, les risques liés à une éventuelle interception sont réduits.

Les messageries sécurisées, voilà l'outil à la mode chez les adeptes d'anonymat. Pas pour leur nouveauté (certaines ont plus de deux ans), mais pour l'abondance de nouvelles têtes : Telegram, Signal (voir *Pirate Informatique* n°31), OTR (n°25), Tor Messenger (n°30), etc. Parmi elles, c'est le projet Ricochet qui a retenu notre attention même si nous l'avions déjà abordé dans le comparatif sur les messageries instantanées du *Pirate Informatique* n°29). Avec elle, impossible, pour l'instant, d'envoyer des fichiers, passer des appels vocaux ou visio, d'entamer une discussion à plusieurs, voire de retrouver facilement ses contacts sur une autre machine. Ne froncez pas les sourcils : malgré ses limitations, Ricochet est l'une des messageries les plus sécurisées qu'il soit.

### TOR À LA MANŒUVRE

Ricochet est open source et tire pleinement parti du réseau Tor. En vous inscrivant, le programme vous attribue un identifiant unique et aléatoire. C'est lui que vous devez communiquer à l'interlocuteur pour qu'il vous ajoute à ses contacts, sachant que la connexion est validée par un mot de passe aléatoire et éphémère (Ricochet s'en charge, vous n'avez pas à le rentrer). Votre liste de contacts n'est pas partagée, et les conversations sont bien sûr chiffrées de bout en bout. En clair, si votre FAI vous espionne, il saura que vous utilisez Tor, mais c'est tout, pas même que vous êtes en train de discuter. Ricochet est extrêmement simple à mettre en place, toutes les opérations se passant en coulisse. On espère que Special, le développeur à l'origine du projet, continuera à travailler dessus pour y ajouter plus de fonctions.

PAS À PAS

# Discuter via le réseau TOR avec Ricochet

CE QU'IL VOUS FAUT

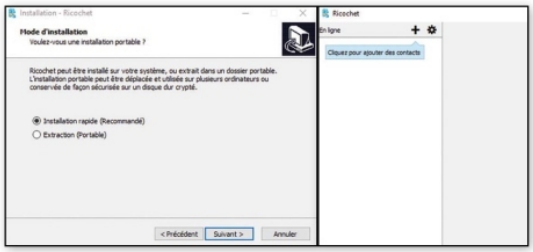
**RICOCHET**

OÙ LE TROUVER ? : **https://ricochet.im**

DIFFICULTÉ :

## 01 CONFIGURER

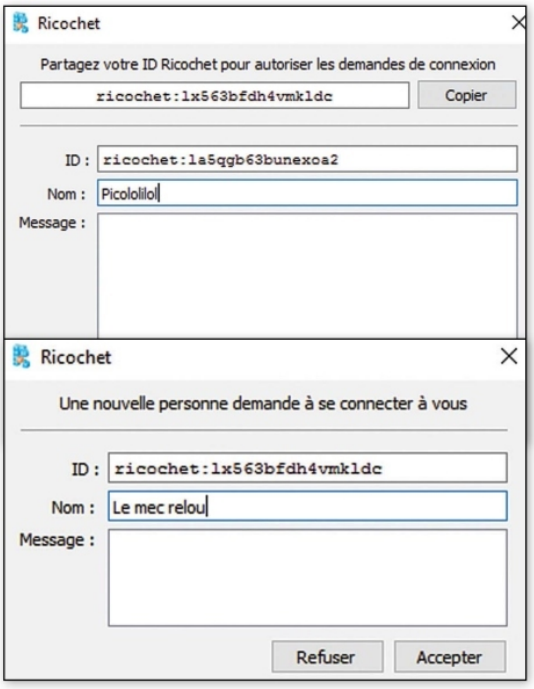
Téléchargez la version de Ricochet compatible avec votre système d'exploitation. Passez les slides de présentation du




logiciel pour faire votre choix entre la version classique (un dossier d'installation est créé sur l'un de vos disques) ou la version portable (que vous placez sur une clef USB par exemple). Faites **Connexion** pour rejoindre le réseau Tor.

## 02 AJOUTER UN CONTACT

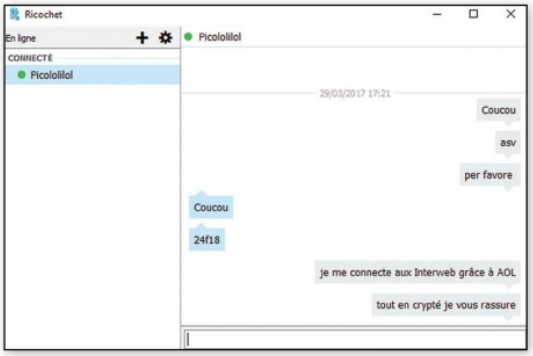
Cliquez sur le **+** en haut de l'interface principale. Deux possibilités: vous copiez votre **ID ricochet** puis vous le partagez avec votre destinataire via un autre moyen de communication. Ce dernier n'aura plus qu'à le rentrer via




le même menu, en remplissant l'**ID** puis en renseignant votre **Nom**. Si vous l'ajoutez de votre côté, récupérez son **ID** puis renseignez-le depuis le même menu. Notez qu'il doit **Accepter** l'invitation dans le pop-up qui s'ouvre de son côté.

## 03 DISCUTER

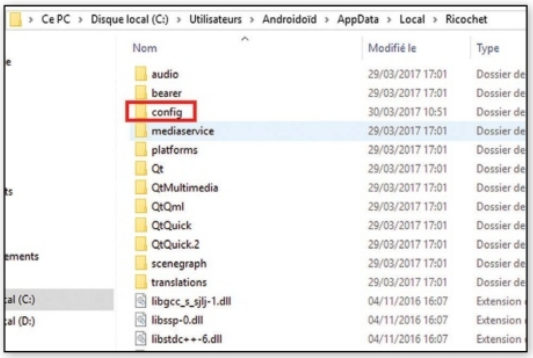
S'agissant d'un service de messagerie instantanée basique, mais ultra sécurisée, Ricochet se limite au strict minimum en termes de fonctionnalités. Tapez vos messages puis envoyez-




les à l'aide de la touche **Entrée**. Vous partagez facilement, via copier coller, des URL. Pas de partage de photos. Notez que si vous envoyez un message à un destinataire non connecté, il ne le recevra pas.

## 04 RETROUVER SES CONTACTS

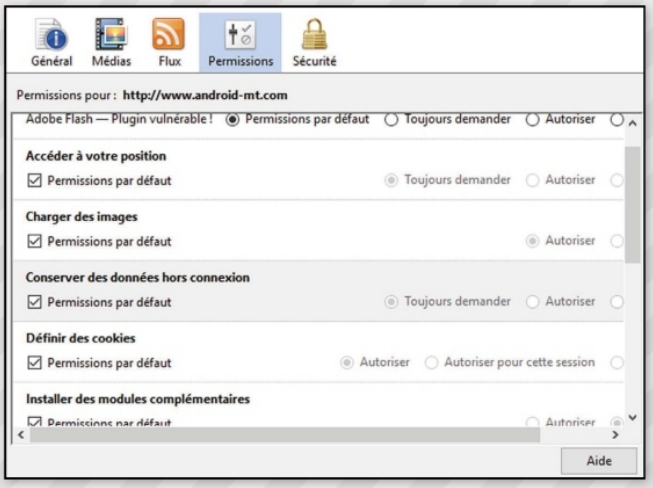
Commencez par afficher les dossiers cachés dans Windows. Suivez le chemin menant au dossier d'installation de Richochet (par défaut: **C:\Utilisateurs\»Votre nom d'utilisateur»\AppData\Local\Ricochet**). Copiez le dossier **config** qu'il contient pour le coller dans le dossier d'installation de Ricochet, sur votre autre ordinateur. Lancez le logiciel pour retrouver les mêmes contacts.



## #1 Gérer les permissions demandées par les sites

AVEC FIREFOX

Le navigateur «sécurité et vie privée friendly» Firefox embarque un outil permettant de contrôler et de retirer les permissions que s'adjugent certains sites. Accès à votre micro, à votre Webcam, notifications sonores... depuis Firefox, cliquez sur le petit **i** à gauche de l'URL du site à contrôler.



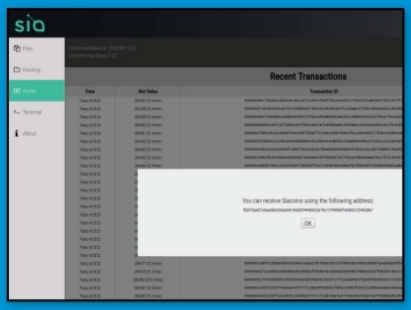

Cliquez sur la flèche de droite et choisissez **Plus d'informations**. Explorez ensuite l'onglet **Permissions** pour décocher et **Bloquer** les permissions que vous jugez suspectes et/ou abusives. Notez que certaines permissions sont nécessaires au bon fonctionnement d'un site.

Lien: **https://goo.gl/3qNmL**

## #2 Un Cloud privé et décentralisé

AVEC SIA

Dans le monde du stockage en ligne, le service Sia veut se démarquer. Open Source, il conserve vos données chiffrées sur un réseau décentralisé, basé sur un blockchain («technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle»). Un blockchain fonctionne avec de la monnaie virtuelle. Il faudra donc gagner des «Siacoins» pour payer le service, équivalent à 2 $ par mois pour 1 To de stockage. Assez complexe à mettre en place, mais c'est le prix à payer pour un Cloud véritablement anonyme et sécurisé. Un tuto dans le prochain numéro?

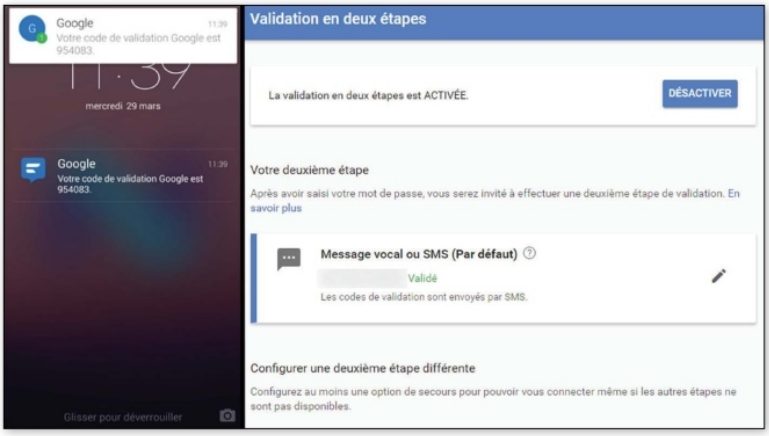



Lien : **http://sia.tech/fr**

## #3 S'authentifier en deux étapes

AVEC GOOGLE

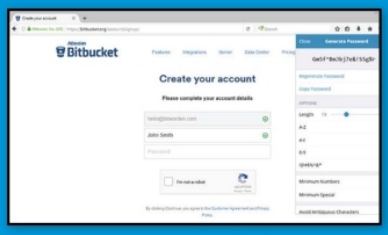
Si vous possédez un mobile Android, BlackBerry ou iPhone vous avez la possibilité d'apporter un niveau de sécurité supplémentaire à votre compte Google. Lors de votre connexion à ce dernier, une fois le mot de passe renseigné, un code unique vous est envoyé par SMS, en le rentrant, vous accédez à votre compte. Pour profiter de cette sécurité permettant d'éviter le vol de votre compte, suivez le lien présenté plus bas puis connectez-vous. Faites **Démarrer** et renseignez le numéro du téléphone à associer. Entrez ensuite le code que vous recevez par SMS. Finalisez l'opération avec **Activer**. La validation en deux étapes est maintenant opérationnelle. N'ayez crainte, ce mode ne s'active que lorsque vous faites des changements critiques à votre compte: mot de passe, association, paiement, etc.




Lien: **https://goo.gl/Q2YrDo**

## #4 Rapatrier tous ses mots de passe dans un gestionnaire Open Source

AVEC BITWARDEN



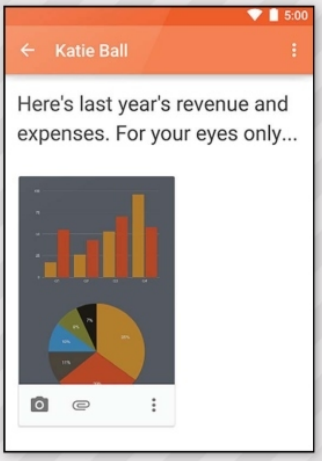

Parce que vous savez très bien qu'un mot de passe fort et différent pour chaque service est une étape nécessaire vers la sécurité, vous avez opté pour un gestionnaire de mot de passe. Mais parce que ce dernier ne vous plaît plus, vous aimeriez en changer, sans devoir tout refaire. Bitwarden est un gestionnaire Open Source qui permet de rapatrier simplement vos mots de passe en provenance de 1Password, Chrome, LastPass ou autre. Une application mobile est également de la partie, le tout gratuitement.

Lien: **https://bitwarden.com**

## #5 Une messagerie auto-destructible

AVEC CONFIDE

Encore une messagerie sécurisée? Oui, mais Confide a la particularité de détruire chaque message ou fichier échangé sitôt lu, sur les appareils bien sûr, mais aussi sur les serveurs. Pas de transfert ou de copie possible, et pas de capture d'écran non plus: vous obtiendrez juste un fond gris. Disponible sur PC, Mac, Android et iOS, Confide propose une



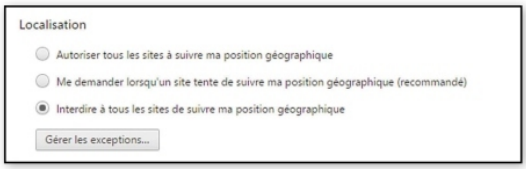

interface très claire pour vous permettre de vous focaliser sur l'essentiel: discuter du plan de domination mondiale des Reptiliens Illuminati.

Lien: **https://getconfide.com**

## #6 Bloquer les demandes de localisation dans les navigateurs

AVEC CHROME, FIREFOX ET EDGE

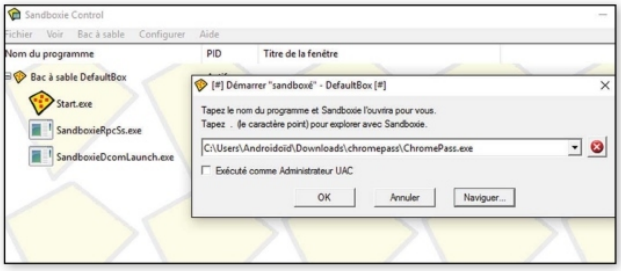
Les navigateurs demandent parfois votre localisation. Ça peut se comprendre sur Google Maps (et encore), mais dans la majorité des cas, c'est une indiscrétion inutile. Dans Chrome, allez dans les **Paramètres**, cliquez sur **Afficher les paramètres avancés** puis sur **Paramètres de contenu** (sous **Confidentialité**) et cochez **Interdire à tous les sites de suivre ma position géographique**.




Sous Firefox, tapez **about:config** dans la barre d'adresse, passez l'avertissement, tapez **geo.enabled** et double-cliquez sur la valeur pour qu'elle bascule sur **false**. Enfin, si vous utilisez Edge (on ne juge pas), allez dans les **Paramètres du PC > Confidentialité > Localisation** et décochez **Microsoft Edge** sous **Choisir les applications autorisées à utiliser votre emplacement exact**.

## #7 Tester un logiciel douteux avant de l'installer

AVEC SANDBOXIE




L'usage d'une sandbox est intéressant dans le cadre où vous souhaitez tester un logiciel, car vous doutez de son authenticité. Pour éviter d'endommager votre bécane, installez le programme Sandboxie en suivant notre lien. Lancez ensuite un soft puis suivez **Bac à sable > DefaultBox > Exécuter «sandboxé» > Exécuter un programme > Naviguer**. Dans l'explorateur qui s'ouvre, pointez vers le logiciel à tester puis validez avec **OK**. Si le cadre brille en jaune durant l'installation dans la sandbox, cela signifie que le programme est de confiance. En rouge, ce dernier est potentiellement dangereux.

Lien: **www.sandboxie.com**

# KODACHI, UN SYSTÈME QUI TRANCHE AVEC LES AUTRES

**Basé sur la distribution Debian, Kodachi tire son nom d'un type de sabre japonais. C'est un système misant sur l'anonymat, la sécurité et la mobilité. Disponible uniquement en mode Live CD (sur DVD ou clé USB), cet OS comprend quantité d'outils pour masquer son identité et son emplacement : Tor, chiffrement, VPN, etc. Attention, Kodachi ne s'adresse pas forcément aux experts...**

## LEXIQUE

***FORENSIC :**
IL s'agit d'investigation numérique pratiquée de manière légale ou non. Kodachi est «anti-forensic» car cette distribution permet de minimiser ou de masquer les activités que vous entreprenez sur l'ordinateur que vous utilisez.

Présentée comme une distribution sécurisée, antiforensic et anonyme, Linux Kodachi se pose en alternative à Tails (*Pirate Informatique* n°30) en étant plus facile à installer et pas uniquement destinée aux journalistes et aux activistes. Il est même surprenant de voir le système se connecter tout seul à un VPN, tout en passant par Tor et en chiffrant les DNS dès qu'elle se connecte à un point d'accès. Outre ces mesures de sécurité, Kodachi intègre des outils pour protéger sa localisation et son identité dont certains sont de vieilles connaissances pour nos lecteurs : Tor (*Pirate Informatique* n°23), la messagerie Pidgin (*n°25*), VeraCrypt (*n°25*), KeePass, etc.

### CE SYSTÈME S'AUTODÉTRUIRA DANS...

La section Panic Room permet quant à elle d'effacer la mémoire vive, de verrouiller la session, de renouveler son adresse


**Dans la catégorie des systèmes Linux complets qui misent sur l'anonymat, Kodachi se pose en concurrent de Tails...**

### Si vous avez raté des numéros...

Si les systèmes étanches et sécurisés vous intéressent, sachez que nous avons dédié 6 pages à Tails dans notre numéro 30 et encore un article sur Qubes OS dans notre numéro 31. Comme nous sommes super sympas, retrouvez ces articles complets au format PDF dans notre CD au cas où vous auriez raté un ou plusieurs épisodes !

MAC, de détruire les données sur les parties du disque dur non utilisées ou carrément d'autodétruire le système ! Cette dernière option est d'ailleurs très efficace : votre serviteur a perdu toutes ses captures d'écran en faisant un essai... Kodachi propose aussi des logiciels «normaux» pour éviter d'avoir à ajouter quoi que ce soit. Du téléchargement Torrent (Transmission), un portefeuille Bitcoin (Electrum), un client FTP (FileZilla), un filtreur d'IP (PeerGuardian), LibreOffice, VLC, Gimp, Komodo, etc. Le but de Kodachi est de proposer un système «jetable», mais vous pouvez aussi choisir de l'installer sur votre PC. Pour ce faire, vous pourriez être intéressé par notre article sur le dual boot dans notre précédent numéro.

## PERSONNE N'EST À 100 % ANONYME SUR INTERNET

Attention, comme pour Tails, il faut bien avoir en tête que le risque zéro n'existe pas et que personne ne peut se targuer d'être complètement anonyme sur Internet. Quelle utilisation voulez-vous faire de Kodachi ? S'il s'agit de se connecter sans laisser de trace depuis un autre lieu que votre domicile, c'est parfait. Par contre, gardez en tête que la société éditrice Eagle Eye, qui fournit aussi l'accès VPN, garde forcément une trace des connexions. Le combo Tor + VPN ne change pas la donne puisqu'il faut une adresse IP pour se connecter à Tor et que si Eagle Eye a décidé de vous trahir, elle peut le faire. La solution consiste alors à paramétrer votre propre service de VPN (voir notre pas à pas et l'article sur OpenVPN).

PAS À PAS

# Présentation de Kodachi

CE QU'IL VOUS FAUT

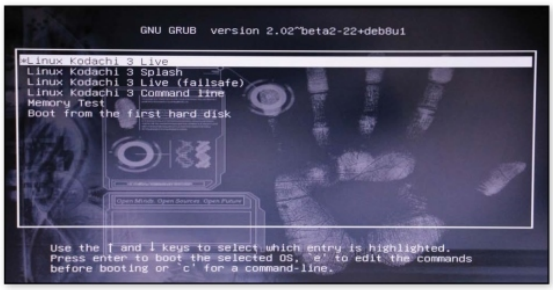
**LINUX KODACHI3**

OÙ LE TROUVER ? :
**www.digi77.com/linux-kodachi**

DIFFICULTÉ :

## 01 LE BOOT

Comme pour tous les système de type Live CD qui se chargent dans la RAM, il faudra juste graver l'ISO sur un DVD (ou placer le fichier sur une clé USB avec Rufus par exemple) et faire booter le PC sur le bon périphérique. On peut aussi envisager l'utilisation



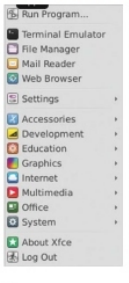

d'une machine virtuelle avec VMware. Dans le menu de boot, choisissez le mode **Live** et attendez que le bureau s'affiche.

## 02 PREMIER CONTACT

La première chose à faire sera d'aller dans la barre d'outils en haut pour ajouter le français comme langue par défaut (clic droit dans **US** puis **Preferences** et onglet **Input Method**). Ajoutez aussi votre réseau local dans l'assistant de connexion juste à côté. Dès qu'il sera authentifié, Kodachi va commencer à activer le VPN, le chiffrement de DNS et la connexion à Tor. Pendant qu'il fait tout ça, découvrez l'interface...


## 03 L'INTERFACE

Si vous ne trouvez pas votre bonheur dans les raccourcis du bas, faites un tour dans le menu **Apps**. C'est notamment ici que vous trouverez les programmes «généralistes» comme VLC, Audacity, LibreOffice, etc.

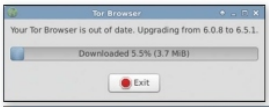


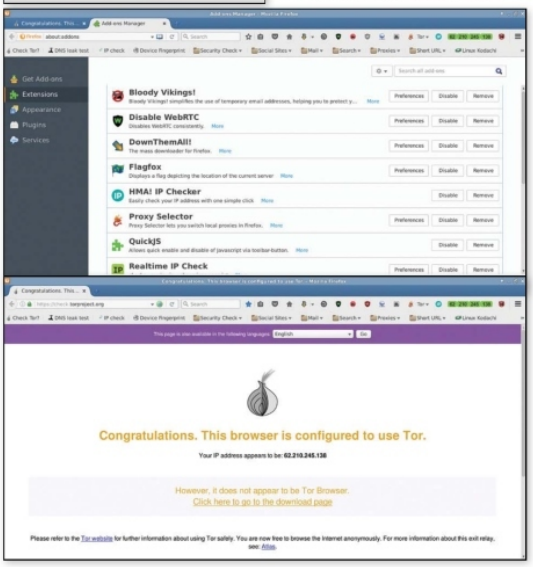

Raccourcis vers les applis et les options les plus importantes

Fond d'écran interactif avec un affichage en temps réel de données telles que l'utilisation du CPU, de la RAM et des port. Analyse du trafic, connexion à Tor, VPN et activation de DNSCrypt.

## 01 LA CONNEXION AVEC TOR

Normalement, vous n'avez rien à faire pour être anonyme avec Kodachi, mais nous allons nous en assurer. La distribution embarque le Tor Browser et un autre navigateur (Kodachi Browser) qui utilise aussi Tor pour se connecter. Cliquez sur le premier pour mettre à jour Tor et, une fois terminé, faites un tour dans le second. Vous devriez voir votre IP d'emprunt

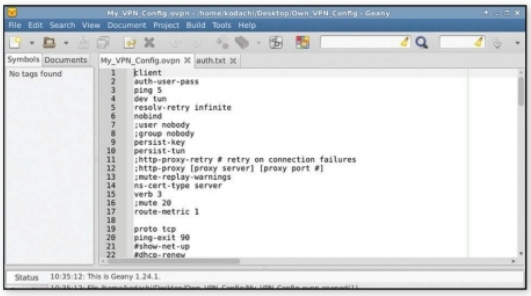



avec un message de confirmation. L'avantage du navigateur de Kodachi c'est le nombre de plugins préinstallés pour brouiller les pistes : adresse e-mail temporaire, agent de connexion permettant de masquer votre configuration, anti-pub, anti-tracker, proxy, etc.

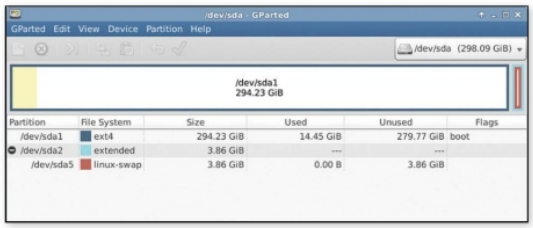
## 05 VOTRE PROPRE VPN

Vous n'avez pas confiance dans le service de VPN proposé par Kodachi ? Il est possible d'utiliser le vôtre ! Sur votre bureau, ouvrez le dossier **Own_VPN_Config**, collez les paramètres de votre fournisseur dans le fichier **My_VPN_Config.ovpn** (ou remplacez-le) et vos identifiants dans le fichier **auth.txt**. Sauvegardez, allez dans la barre de lancement rapide en bas et choisissez **Start your own VPN** dans **VPN Tools**.

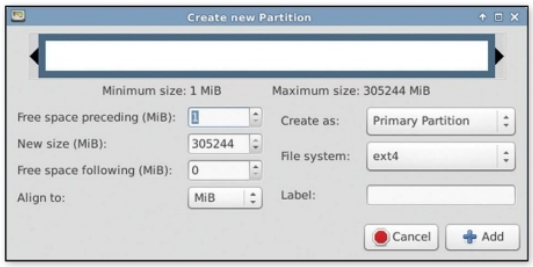



## 06 UNE INSTALLATION SUR DISQUE DUR ?

Kodachi n'est pas pensé pour cela, mais il est tout de même possible d'installer la distribution. Après avoir booté sur le DVD ou la clé USB, allez dans le menu **Apps** puis faites **System**



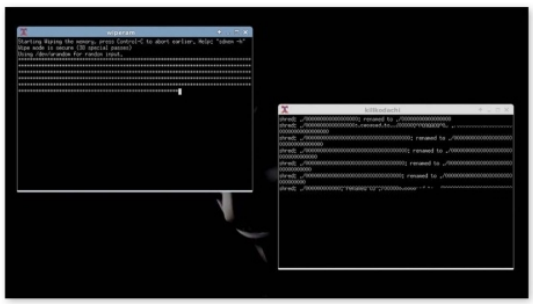

> **Refracta Installer** > **Use su**. Entrez le mot de passe (par défaut **r@@t00**) puis choisissez **Simple installation** > **Run GParted** > **Device** > **Create partition Table** > **Apply** > **Partition** > **New** > **Add** > **Apply All Operations** > **Close**. Attention de ne pas écraser une précédente installation. Fermez




Gparted et sélectionnez la partition que vous avez créée. Faites ensuite **Proceed with the installation** et paramétrez vos identifiants.

## 07 TOUT EFFACER !

Avec Tails, il suffit de retirer la clé USB du PC pour effacer la RAM et le contenu du bureau. Dans Kodachi, il faudra aller dans la partie **Panic Room** où vous pourrez faire **Wipe the RAM** ou **Wipe RAM then Shutdown**. Le processus est plus long que dans Tails. Si vous utilisez Kodachi depuis longtemps et que vous voulez absolument tout effacer sans laisser de trace, faites **Destroy Kodachi**. Vous perdrez absolument toutes les données !



# 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.*

# KALI LINUX : HAIL HYDRA !

**Hydra c'est bien sûr une organisation ennemie jurée de Captain America, mais c'est aussi un redoutable logiciel qui peut cracker du mot de passe en ligne sur une cinquantaine de protocoles ou bases de données : Telnet, FTP, HTTP, HTTPS, IRC, VNC, SSH, SMTP, MySQL, XMPP, IMAP, etc. Pour cela, il nous faudra compter sur un dictionnaire de mots de passe et d'un peu de chance...**

Nous vous mettons souvent en garde sur l'importance du choix de vos mots de passe et ce n'est pas pour rien ! Avec très peu de connaissances en informatique, un pirate à la petite semaine pourrait faire de votre vie un enfer (usurpation d'identité, défaçage de votre site, vol de données, etc.) Car on utilise des mots de passe tellement souvent sur Internet que certains utilisateurs font l'erreur de choisir le même partout. C'est bien sûr une chose à éviter, car il suffit qu'un seul de vos comptes se fasse pirater pour que les autres ne tombent comme des dominos. De même, n'utilisez pas de mots de passe permettant de deviner les autres (kiki75, kikiPaname, TheKiKidu75, etc.) ou faciles à deviner.

## NE VOUS CROYEZ PAS À L'ABRI !

Car avec les réseaux sociaux il est facile de connaître des éléments sur vous : date de naissance de vos enfants, séries, sports ou parti politique préférés, mot de passe qui veuille dire quelque chose, même avec une alternance et des chiffres à la fin. Par exemple **SoNgOkU92** ou **BELmondo76** sont peu sûrs (voir nos articles sur John The Ripper). Alternez capitales, minuscules, chiffres et caractères spéciaux. **Rgè7°l^$Hj562Nugfù** vous semble alambiqué ? Certes, mais il est sûr selon le site **https://howsecureismypassword.net** : testez les vôtres ! Il sera bien sûr difficile de mémoriser ces types de mots de passe, mais au lieu de les écrire sur un Post-It (attention aux cambriolages !), faites confiance à un porte-feuille comme Xecret ou Enpass (voir notre précédent numéro) : la plupart du temps, vous n'aurez même pas à les retaper ! À la différence de nos précédentes démonstrations sur les mots de passe, Hydra fonctionne en ligne. Alors que nous devions auparavant avoir un hash en main pour tenter de cracker le mot de passe correspondant, ce n'est pas le cas ici. Hydra va directement envoyer des requêtes vers un serveur cible. Voyons comment se présente xHydra, son interface graphique...


**Notre mot de passe Rgè7°l^$Hj562Nugfù est très solide, mais pas invincible pour autant. Même s'il faudrait des siècles à un logiciel pour le cracker, vous n'êtes pas à l'abri d'une faille de sécurité qui pourrait le rendre visible, d'un keylogger ou d'une attaque encore inconnue à ce jour... D'où la nécessité de les changer régulièrement.**

etc. Si vous pensez que **MélenchonPSG9698** est solide, vous avez tort... Mais ce qui nous intéresse ici c'est la méthode par dictionnaire puisqu'Hydra l'utilise principalement. Ne prenez donc jamais un

## 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.

***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.

PAS À PAS

# xHydra sous Kali 2

CE QU'IL VOUS FAUT

KALI LINUX

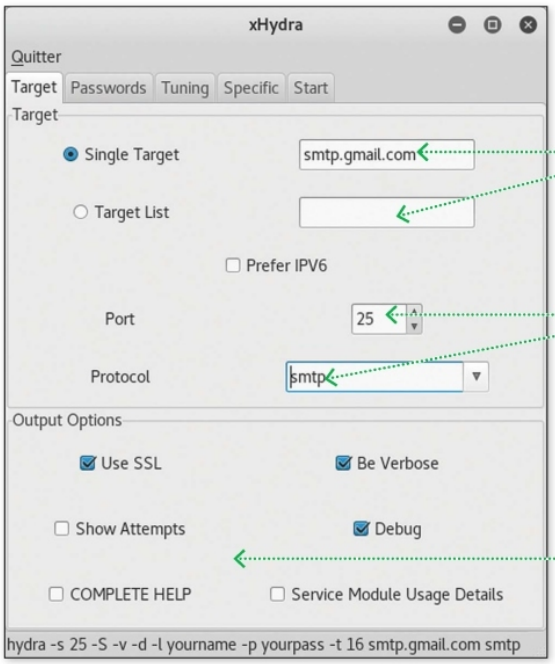
OÙ LE TROUVER ? : **www.kali.org**

DIFFICULTÉ :

## 01 XHYDRA DANS KALI LINUX

Nous ne reviendrons pas sur la mise en place de Kali Linux puisque nous avons vu dans notre n°27 que vous pouviez l'installer, l'utiliser depuis un Live CD, une virtualisation ou même un Raspberry Pi. xHydra est l'interface graphique du logiciel Hydra et vous la trouverez dans le menu **Applications > Attaques de Mots de Passe > Les Attaques en Ligne > hydra-gtk**.


## 02 ONGLET TARGET (CIBLE)




Dans ce champ vous devrez taper l'adresse IP ou l'URL de la cible. Si vous avez plusieurs cibles, vous pouvez en faire une liste au format TXT ou LST et spécifier l'emplacement ici. La case en dessous permet d'utiliser des adresses IPv6

Ici vous devez spécifier le protocole et le port d'écoute. Chaque protocole a un ou plusieurs ports d'écoute habituels (21 pour le FTP, 22 pour le SSH, 193 pour IRC, etc.) Pour être sûr que vous ne donnez pas des coups d'épée dans l'eau, vous pouvez scanner les ports d'une cible avec le logiciel Nmap, inclus aussi dans Kali.

Utilisation du protocole SSL pour les serveurs qui l'utilisent plus d'autres options permettant d'avoir des détails sur les tentatives, un mode Debug, etc.

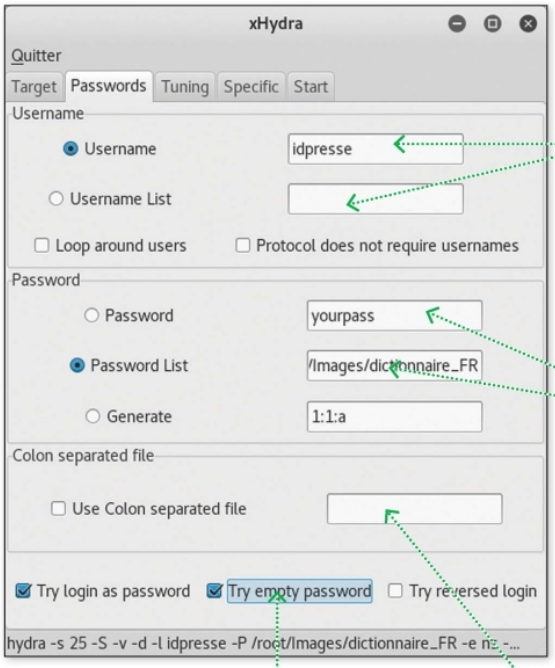
## DES VERSIONS POUR TOUT LE MONDE !

SI vous n'avez pas envie d'installer ou d'utiliser Kali Linux, il existe aussi une version Windows appelée THC-Hydra que vous trouverez ici : **www.thc.org/thc-hydra**. Attention, votre navigateur et votre antivirus ne vont pas aimer... Sinon, vous pouvez aussi tenter de l'installer sur un appareil Android rooté. Attention, la manipulation est un peu complexe : **https://goo.gl/bKJyGu**.

## ATTENTION !

La démonstration suivante a pour but de tester vos mots de passe ou de persuader un ami à prendre au sérieux la notion de sécurité informatique (avec son autorisation bien sûr). Dans le cas contraire, vous pourriez tomber sous le coup de l'article 323-1 du code pénal, lequel dispose que *«Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 € d'amende.»*

## 03 ONGLET PASSWORD




Nom d'utilisateur de la cible, comme pour le précédents onglet, vous pouvez dresser la liste des Username potentiels... Cochez la première case si vous désirez que la liste revienne sur elle même en cas d'échec et cochez la deuxième si vous n'avez pas besoin de nom d'utilisateur.

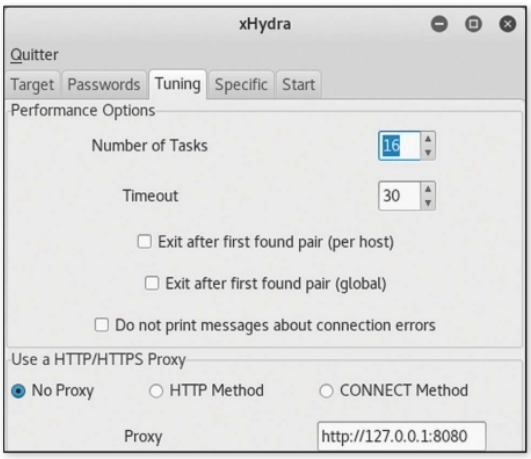
Si vous avez votre mot de passe mais que vous cherchez votre identifiant, entrez le sésame dans le premier champ. Si vous avez l'identifiant mais pas le mot de passe, vous pouvez spécifier une liste de mots de passe que l'on appelle dictionnaire au format TXT ou LST. Les dictionnaires de bonne qualité sont rares ou payants. Vous pourrez trouver quelques exemples ici dans plusieurs langues (wordlists) : **http://www.openwall.com/mirrors**. Vous pouvez aussi essayer le générateur de mots Crisis dont nous vous parlerons dans le prochain numéro : **https://goo.gl/iwr90e**. Generate sert à la méthode brute force mais reste très anecdotique dans cette interface. Préférez la version ligne de commande pour cette option.

Cases à cocher pour essayer d'utiliser l'identifiant comme mot de passe, un mot de passe vide ou inverser le mot de passe et l'identifiant. Cochez les trois car il ne faut jamais sous-estimer la bêtise des gens...

Pour les fichiers avec des données séparées par des points virgules (les fichiers doivent normalement revenir à la ligne à chaque mot pour être pris en compte.

## 04 ONGLETS TUNING & SPECIFIC

Les deux onglets suivants permettent moult autres réglages ou paramétrages : nombre de threads, comportement à adopter en cas de succès (continuer sur d'autres tâches ou s'arrêter), utilisation d'un proxy, etc.

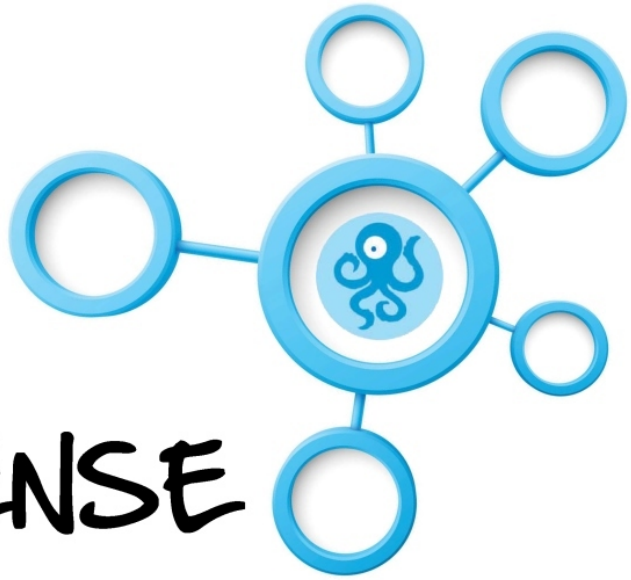



## 05 ONGLET START

Bien sûr, le dernier onglet va démarrer le processus. Cliquez sur **Start** en bas lorsque vous êtes sûr de vos réglages. Notez que le logiciel va mémoriser les résultats ou les échecs et si un bug se manifeste, vous n'aurez pas à tout refaire. Notez que tout en bas, vous verrez l'équivalent de vos paramétrages et de vos actions en ligne de commandes. Vous pourrez donc à terme comprendre comment fonctionne la syntaxe d'Hydra. Dans notre exemple, nous avons fait chou blanc. Forcément, nous avons essayé de pirater le compte Gmail du rédacteur en chef !

# OONI

# SOIT QUI MAL Y PENSE



**Nous vous parlons souvent de censure et de filtrage sur Internet, mais tout cela reste bien obscur. Comment savoir si le réseau des réseaux est «bancal» lorsque vous vous y connectez. Chez vous, au travail ou à l'étranger voyons comment directement tester votre connexion avec les applications mobiles ooniprobe...**

Disponibles sur Raspberry Pi, MacOS et Linux (**https://ooni.torproject.org//install**), les logiciels OONI débarquent sur appareils mobiles Android et iOS sous le nom d'ooniprobe. Lancé par les responsables du projet Tor, OONI (Open Observatory of Network Interference) propose trois tests permettant de faire le point sur les performances de votre réseau et sur l'éventuelle censure de votre connexion à Internet. En France, à part quelques sites de djihadistes, la censure est discrète même si on fait aussi la chasse aux sites de téléchargement (coucou T411 !). Dans d'autres pays, on fait moins dans la dentelle avec des sites d'informations bloqués, les protocoles de messageries instantanées, les bridges de Tor, certains proxys, etc. Pas besoin non plus de sortir du pays pour voir sa connexion Internet manipulée. Avec ces applis, vous allez savoir si votre réseau d'entreprise, votre hôtel ou votre bibliothèque brident les connexions.

## UNE FORMIDABLE SOURCE D'INFORMATION... PARFOIS UN PEU TROMPEUSE

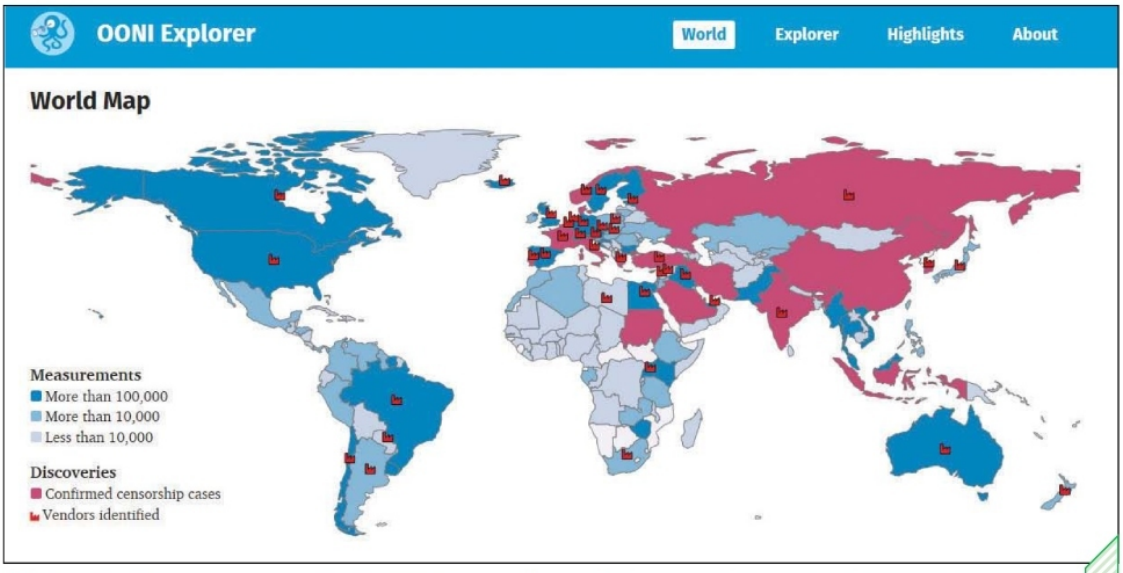
Toutes les données recueillies par ooniprobe sont analysées et réunies pour dresser un bilan mondial de la censure. Ces données sont parfois à prendre avec des pincettes, car certains pays sont plus testés que d'autres, par méconnaissance du projet ou peut-être aussi un peu à cause de la répression... C'est avec surprise qu'on apprend que la Biélorussie filtre moins de choses que la France. Quand on regarde de plus près, la dernière dictature d'Europe n'a connu que 1200 mesures tandis que la France en est à plus de 2 millions. Avec en plus Trident Media Guard qui scrute les méchants pirates, le pays des droits de l'Homme est dans le rouge alors que tout va bien à Loukachenko-land !

## LEXIQUE

***NEUTRALITÉ DU NET :** Surveiller que la Neutralité du Net est bien respectée c'est être sûr que tout le monde dispose de la même connexion et des mêmes chances. Aimeriez-vous qu' un Internet ou un forfait plus cher permettent aux gens fortunés de télécharger plus vite ou d'être prioritaires sur certains contenus ? En tant que webmaster, aimeriez-vous que les vidéos qui s'affichent sur votre site soient de moins bonne qualité parce que vous ne vous appelez pas Google ou Microsoft ?

## ATTENTION !

Les tests menés par les logiciels OONI permettent de détecter certains signes de censure, de surveillance et de manipulation du trafic. Or, vous pourriez être inquiété dans certains pays pour avoir utilisé ces tests : amende, surveillance de votre trafic, mise sur liste noire, voire même emprisonnement. On ne plaisante pas avec ce qui est considéré comme de l'espionnage en Corée du Nord, Chine, Soudan et autres. Soyez prudent.



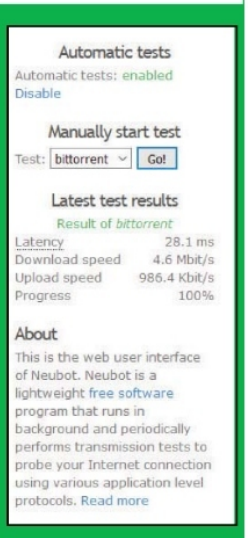

Les résultats obtenus par l'ensemble des logiciels OONI sont centralisés sur le site avec des renseignements détaillés pour chaque pays. Comme nous pouvons le voir, la France n'est pas au top et c'est surtout à cause des mesures de surveillance HADOPI/Trident Media Guard (vendors sur la carte).


Lorsqu'on clique sur un pays, on peut voir le nombre de sites bloqués sur le nombre de ceux qui ont été testés. C'est aussi un peu trompeur, car certains sites bannis ne sont peut-être pas dans la liste. Il est possible de contacter OONI pour les ajouter. En Chine on apprend que sont bloqués les sites de news de Google, DuckDuckGo, OpenVPN, Reporter Sans Frontière, Amnesty International, Dalailama.com, Twitter, Tor Project, etc.

## NEUBOT, POUR SURVEILLER LA NEUTRALITÉ DU NET

Vous en voulez encore ? Le site MesurementLab propose des outils à utiliser sous Windows dont Neubot (car le service en ligne Glasnost a fermé ses portes en février dernier). Il s'agit d'un logiciel open source qui effectue périodiquement des tests de transmission avec des serveurs de test pour s'assurer que la neutralité du Net est bien respectée. Le programme enregistre les résultats de transmission de différents protocoles et les données peuvent être analysées en fonction de l'emplacement géographique et du FAI.

**www.measurementlab.net**



PAS À PAS

# Comment maîtriser ooniprobe ?

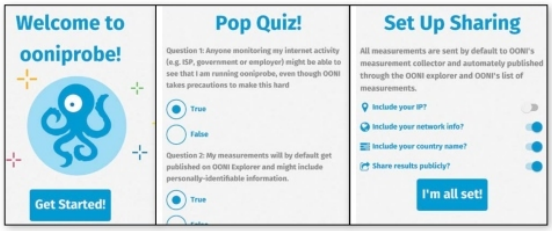
**CE QU'IL VOUS FAUT**

**OONIPROBE**

OÙ LE TROUVER ? : **https://goo.gl/DqJeyw (Android); https://goo.gl/i4XfiV (iOS)**

DIFFICULTÉ :

## 01 PREMIER CONTACT

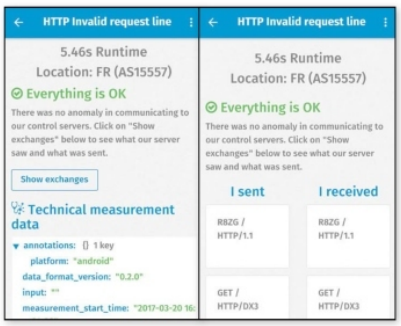



Lors du premier lancement, ooniprobe vous proposera un petit quiz pour voir si vous avez bien compris les dangers de l'appli. La première question vous demandera si vous êtes conscient que des gouvernements ou votre employeur peuvent être au courant que vous utilisez l'appli tandis que la deuxième vous demandera si vous savez que vos données peuvent être publiées sur le site officiel. Heureusement, sur la page suivante vous pouvez faire en sorte de partager vos informations et les résultats de vos tests sans pour autant communiquer votre IP (ce qui vous ne vous rend pas 100% anonyme pour autant).

## 02 TEST DE CONNECTIVITÉ

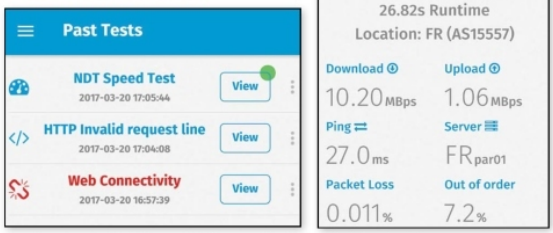

Vous pourrez ensuite lancer les différents tests. **Web Connectivity** tente de se connecter à plusieurs sites préenregistrés dans le but de voir s'ils sont bloqués et à quel niveau : DNS ou Deep Packet Inspection (analyse détaillée des paquets de données pour en déterminer le protocole, etc.) Pour voir les résultats, il suffit de cliquer sur les trois barres horizontales et de faire **Past Test**. Si vous avez un doute sur un site, le plus simple est d'essayer de s'y connecter avec Tor...

## 03 CONTRE LES «MIDDLE BOXES»




Attention, l'utilisation du second test **HTTP Invalid Request Line** peut être considérée comme une manœuvre offensive de hacking dans certains pays. Il s'agit de détecter l'utilisation de proxys sur certains sites pour surveiller les connexions ou manipuler le trafic. Comme bien souvent, rien à signaler avec un FAI français, mais ailleurs... Attention, ce n'est pas parce qu'un site utilise un proxy qu'il est forcément louche. En cas de réponse positive, allez faire un tour dans les journaux.

## 04 TEST DE CONNEXION




Le dernier test Network Diagnostic Test n'a rien de bien sorcier, il s'agit de données basiques concernant votre connexion : débit, ping, paquets perdus, etc. Le reste n'intéressera que les ingénieurs réseau. Notez que, même s'il est beaucoup plus simple de faire ces tests d'un smartphone, la version «desktop» propose des options plus avancées : vérification du réseau Tor ou du bon fonctionnement des messageries WhatsApp ou Facebook Messenger. Nous y reviendrons si vous le désirez...


**Comme vous pouvez le voir, les tests sont très détaillés et les résultats peuvent être gardés en mémoire pour les comparer ultérieurement...**

# NOS GUIDES WINDOWS 100% PRATIQUES

## POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3€


## Chez votre marchand de journaux

# MEDICAT : LA TROUSSE À OUTILS UNIVERSELLE

**Problème de fichier Windows, d'infection, de RAM, de disque dur, de partition ou de mot de passe ? Plus besoin d'avoir toute une collection de Live DVD sur vous lorsque vous partez réparer l'ordi de tata Lydie ou celui de Kévin (votre cousin de 13 ans qui se prend pour un hacker). MediCat propose une compilation d'outils fréquemment mis à jour...**

Nous avons souvent parlé de Hiren's Boot CD (notamment dans Les *Dossiers du Pirate* n°7), mais malheureusement, ce Live CD proposant une trousse à outils extrêmement complète n'est plus mis à jour et commence à se faire vieux. Pour remplacer cette compilation, nous vous proposons de découvrir MediCat (MediKit, MediCat, vous saisissez?). Cette compilation permet de faire la chasse aux virus, de restaurer un Windows bancal, de sauvegarder des données en cas de problème physique ou de mettre un peu d'ordre dans vos partitions.

## DES VERSIONS ENTRE 1,5 ET 7,5 GO

MediCat comprend aussi des outils de diagnostic en tout genre, plusieurs logiciels pour récupérer vos mots de passe (dont ceux de Windows et de certaines distributions Linux). Idéal pour les altruistes qui n'hésitent pas à se déplacer pour réparer l'ordi d'un ami, MediCat est indispensable. La version la plus «lourde» peut aisément prendre place sur une vieille clé USB de 8Go, raison de plus pour la garder tout le temps avec soi.

**SUR NOTRE CD**

**SI VOUS AVEZ RATÉ DES NUMÉROS...**

Retrouvez sur notre CD les anciens articles au format PDF mentionnés dans ces pages : Hiren's Boot CD, Kon-Boot, Offline NT Password & Registry Editor et TestDisk !

## BIOS UEFI ?

Certains fabricants de cartes mères intègrent depuis quelques années un BIOS sécurisé et un peu pénible appelé UEFI ou EFI. Ce BIOS spécial est un peu difficile à prendre en main et vous donnera du fil à retordre si vous souhaitez «booter» depuis un CD, un DVD. Dans ce cas, il faudra désactiver l'option Secure Boot et activer le Boot Legacy (ou CSM si cette dernière est présente). Pour les clés USB, le logiciel Rufus (voir notre pas-à-pas) vous facilite un peu la tâche même si cela ne fonctionne pas encore à 100%. Pour en savoir plus et apprendre comment s'en sortir avec ces BIOS, voici un article très intéressant : **http://goo.gl/KSDTS5**

PAS À PAS

# Utilisation de MediCat

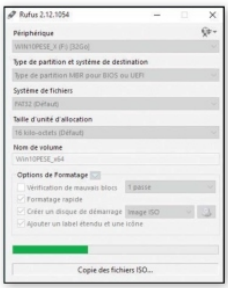
**CE QU'IL VOUS FAUT**

**MEDICAT**
OÙ LE TROUVER ? : **https://goo.gl/3imeh8**

**RUFUS**
OÙ LE TROUVER ? : **https://rufus.akeo.ie**

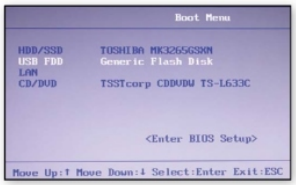
DIFFICULTÉ :

## 01 L'IMAGE ISO




Choisissez la version que vous voulez sur le Google Drive ou Mega. Nous vous conseillons la plus lourde sauf si vous n'avez pas de graveur de DVD double densité (et pas de clé USB). Notez qu'il faudra rassembler les fichiers (**medicat.16.10.stable.7z.001, medicat.16.10.stable.7z.002**, etc.) avec 7-Zip en ouvrant le premier. Gravez celte image ou ouvrez Rufus, laissez **MBR pour BIOS ou UEFI, FAT32** comme système de fichier et choisissez Image ISO dans le dernier menu déroulant. Dans la case à droite, renseignez l'emplacement de l'image. Faites Démarrer mais attention, votre antivirus va sans doute se réveiller. Désactivez-le pendant cette phase.

## 02 «BOOTER» DEPUIS UN PÉRIPHÉRIQUE




Pour booter sur le lecteur DVD ou sur un port USB, il faudra juste demander à votre PC de le faire. Faites **Suppr, F1, F2** ou **F8** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier votre lecteur optique ou l'USB. Pour les BIOS UEFI, consultez notre encadré à ce sujet...

## 03 LE MENU PRINCIPAL


Vous devriez voir l'interface principale avec **Continue Booting The PC** (pour booter normalement sur le disque dur une fois que vous aurez terminé), **Boot Other Harddisk Partitions** pour choisir sur quelle partition booter (au cas où vous auriez plusieurs OS sur lesquels démarrer) et **64-Bits Windows Recovery** pour retrouver un Windows stable. Ensuite nous avons **Diagnostic Utilities** avec **Hardware Detection Tool** (pour identifier les périphériques et mieux choisir ses pilotes), **MemTest, TestDisk** (pour réparer la table des partitions ou faire une image miroir de son disque dur, voir *Pirate Informatique* n°32) et le classique **Ultimate Boot CD**.

## 04 ANTIVIRUS ET ACCÈS WINDOWS

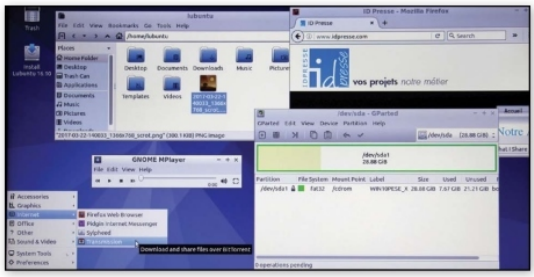


En cas d'infection, c'est **Scan for Viruses** qu'il faudra sélectionner. Cette option va afficher l'antivirus Comodo. Depuis cette interface vous pourrez bien sûr lancer des scans, mais aussi accéder à Internet et à des outils rudimentaires (navigateur, capture d'écran, etc.) **Remove User Account Password** vous donne accès à des outils que nous avons déjà abordés, dont **Offline NT Password & Registry Editor** (*Les Dossiers du Pirate* n°10) et **Kon-Boot** (*Pirate Informatique* n°28) qui permettent de retrouver un accès à Windows si vous avez oublié votre mot de passe de session. Ces logiciels ne fonctionnent qu'avec le mot de passe local et pas du tout avec le nouveau type de mot de passe Compte Microsoft.

## 05 DEUX OS EN PRIME

Là où Hiren's Boot CD donnait l'accès à un Windows XP «light», MediCat propose un **Mini Windows 10** et **Lubuntu**. Le premier

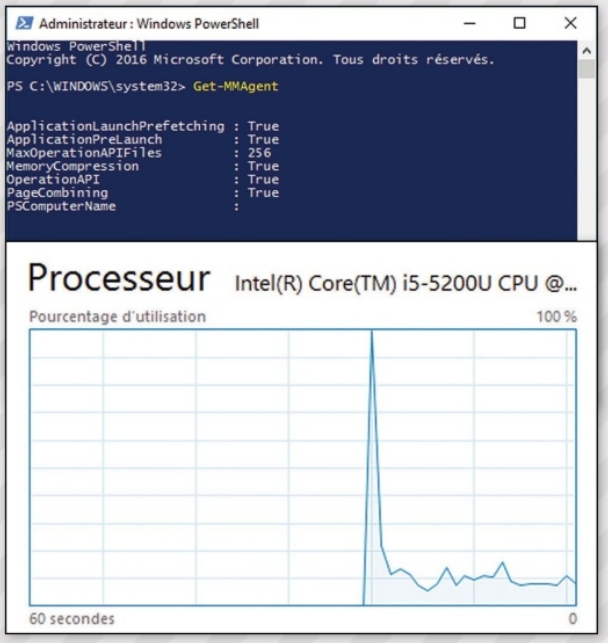
vous donne un véritable petit Windows pour récupérer ce qui peut l'être, accéder au réseau, gérer vos périphériques, monter des disques durs et tout ce qu'on peut faire avec un véritable OS graphique. Il comprend aussi la collection de logiciels de **PortablesApps.com** pour réparer, sauvegarder, etc. Lubuntu fera la même chose pour les linuxiens puisqu'il s'agit d'un Ubuntu «light» avec à peu près les mêmes options, mais pour les systèmes au manchot. **MediCat FreeDOS** n'a quant à lui que très peu d'intérêt puisqu'il s'agira d'aller dépanner les anciens systèmes ou de fonctionner sur de très modestes configurations.



## #1 Un CPU moins sollicité

### AVEC LE POWERSHELL DE WINDOWS

Si vous avez souvent des pics d'occupation de processeur inexpliqués sur votre ordinateur sous Windows 10, cela vient peut-être de l'option de compression de la mémoire virtuelle. En effet, avec certains appareils un peu légers au niveau performance, cette compression optionnelle se prend parfois les pieds dans les pédales. Lancez le **PowerShell** de Windows en **mode Administrateur** (lancez une recherche dans la barre et faites un clic droit) puis tapez **Get-MMAgent**. Vous devriez voir **True** en face de la ligne **MemoryCompression**. Pour retirer cette option, faites **Disable-MMAgent -m**. Si vous voulez revenir en arrière, il faudra taper **Enable-MMAgent -m**.

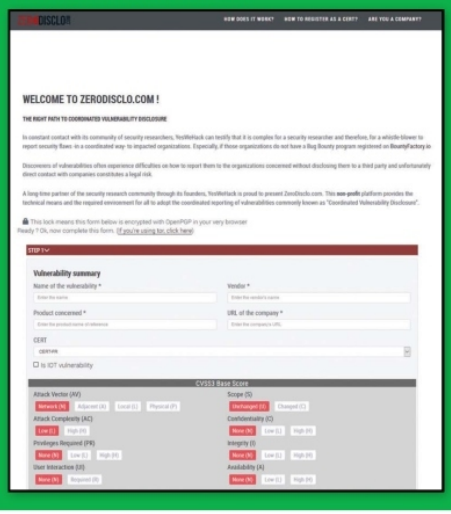



## #2 Dévoiler une faille en toute sécurité

### AVEC ZERODISCLO

Dans notre n°30 nous vous avions parlé du protocole d'alerte Zataz de notre confrère Damien Bancal. Ce protocole permet de mettre au courant un site d'une faille, d'une vulnérabilité, d'un piratage ou une fuite de données pour qu'elle soit colmatée avant qu'elle ne soit exploitée. La plate-forme ZeroDisclo.com co-créée par Korben propose quelque chose de similaire. Accessible directement ou via le réseau Tor, le site permet de signaler une vulnérabilité à différents CERTs (des centres d'alerte et de réaction aux attaques informatiques) depuis un formulaire en ligne. Bien sûr tout est sécurisé et chiffré pour permettre aux bons samaritains de dévoiler une faille sans risquer la case tribunal...

Lien: **https://zerodisclo.com**

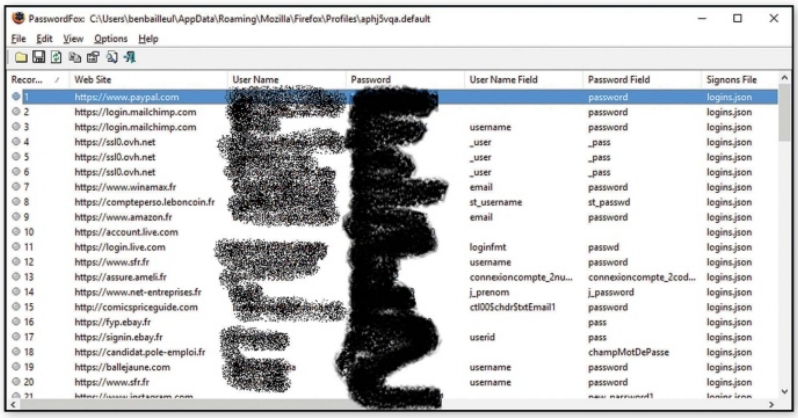



## #3 Récupérer les mots de passe de vos navigateurs

### AVEC LES OUTILS NIRSOFT

Besoin de récupérer les identifiants/mots de passe de vos navigateurs? C'est facile avec les outils de Nir Sofer! Ce programmeur très consciencieux propose des logiciels sains : la plupart de ses produits ne nécessiteront aucune installation et pourront se loger sur une clé USB sans laisser de traces dans la base de registre de votre ordinateur. Avec PasswordFox, ChromePass et IE PassView (jusqu'à la version 8) vous pourrez récupérer vos sésames pour les transférer ou les sauvegarder en cas de problème.

Lien: **www.nirsoft.net/password_recovery_tools.html**

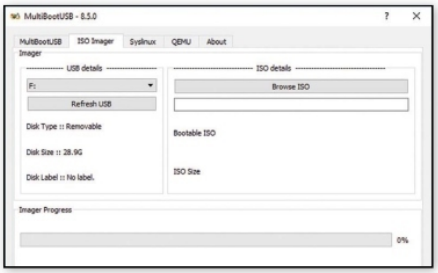


## #4 Une clé USB multiboot

AVEC MULTIBOOTUSB

Comme Rufus, MultiBootUSB permet de placer différentes distributions Linux sur une clé USB tant que celle-ci dispose d'espace disponible. Vous pourrez donc transporter partout des systèmes alternatifs (Kodachi, Tails), des outils de réparation (MediCat, etc.) ou des distributions expérimentales. Si votre matériel n'est pas reconnu comme un périphérique bootable par le BIOS, vous pourrez installer le boot loader Syslinux pour y remédier. Le logiciel est disponible sous Windows et Linux...

Lien: **http://multibootusb.org**




## #5 Audit réseau sur mobile

AVEC ANMAP

ANmap est un outil Android que vous pouvez utiliser sur un réseau ou un site pour déterminer les ports disponibles, les services, les versions du système d'exploitation, les types de filtres/pare-feux, etc. Un outil d'autant plus efficace qu'il s'installe très facilement sur un mobile rooté. Comment avoir l'IP d'un site que vous voulez tester? Faites **tracert www.idpresse.com** dans un terminal par exemple!

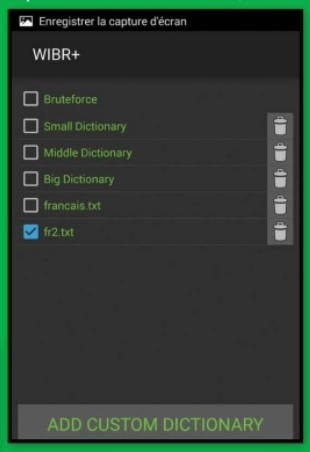
Lien: **https://tinyurl.com/mydfuge**


## #6 Crack de mots de passe WiFi

AVEC WIBR+

Cracker un mot de passe consiste à le deviner en utilisant des outils informatiques et son cerveau (eh oui, il faut les deux). Il existe de nombreux outils sur PC (Windows et Linux) que nous vous présentons parfois dans *Pirate Informatique* et les *Dossiers du Pirate*, mais pour cette fois, nous parlerons de Wibr+, une appli bannie du Google Play Store. Cette dernière propose de casser le mot de passe d'un réseau WiFi pour y pénétrer. Bien sûr nous présentons cette appli pour tester votre propre réseau et aussi pour vous montrer comment s'y prennent les pirates pour accéder à votre réseau et l'utiliser pour réaliser tout un tas de méfaits (téléchargement illégal, attaque DDoS, etc.) Très complète pour une appli mobile, Wibr+ propose 2 types d'attaques: dictionnaire et brute force. Si son fonctionnement vous intéresse, nous avons fait un sujet complet dans les *Dossiers du Pirate* n°11 spécial mobiles, encore en kiosques...

Lien: **http://auradesign.cz/android/wibrplus.apk**





## #7 Un pot de miel pour les hackers

AVEC HONEYDRIVE

Un honeypot («pot de miel» dans la langue de Kanye West) est un procédé de défense contre les hackers. Il s'agit d'un programme, d'un serveur ou d'un site qui va tenter d'attirer les brigands pour les identifier ou les neutraliser. Cela vous donne envie d'essayer? Pour cela, nous vous conseillons HoneyDrive qui est une distribution Linux proposant quantité de honeypots préinstallés et préconfigurés pour faire joujou. Si vous êtes suffisamment nombreux à vous manifester, nous ferons un petit tuto dans le prochain numéro: benbailleul@idpresse.com

Lien: **http://bruteforcelab.com/honeydrive**

N°5 en kiosques
NOUVEAU !

# Le GUIDE
## non officiel de l'utilisateur WINDOWS 10


# 100% PRATIQUE

**ATTENTION !**

Le but de cet article n'est pas de vous montrer comment regarder la L1 ou Canal+ sans payer (même si c'est possible, vous l'aurez deviné). Il s'agit avant tout de profiter de chaînes étrangères pour les expatriés et les bilingues ou de profiter des chaînes françaises lorsque vous êtes en voyage par exemple. Eh oui, vous payez la redevance, mais les IP de nombreuses chaînes françaises sont bloquées à l'étranger...

# DES MILLIERS DE CHAÎNES GRATUITES !


**Dans *Pirate Informatique n°26*, nous avions fait la découverte de PVR IPTV Simple Client, un plugin pour le media center Kodi disponible sur presque tous les supports (voir notre article dans Pirate Informatique n°24 cette fois). Or, l'installation n'est pas très aisée. Que vous ayez un media center ou un PC, nous avons trouvé plus simple...**

Nous vous parlons souvent de P2P lorsqu'il s'agit de visionner des chaînes de télévision sans bourse délier, mais il existe aussi le stream direct avec des listes de chaînes compilées dans un fichier «playlist» au format M3U. Il suffit de trouver ces listes en les téléchargeant ou de se les confectionner soi-même en ajoutant des liens dans un fichier texte que vous renommerez : par exemple liste_france.m3u.


## UN SYSTÈME LUCRATIF POUR DES PETITS MALINS...

Ce type de diffusion est possible grâce à certains utilisateurs qui proposent de partager leurs flux personnels avec les internautes ou de véritables brigands du Net qui eux proposent contre de l'argent des listes mises à jour (car comme toutes les choses illégales sur Internet, les ayants droit font la chasse à ce genre de pratique). Nous ne parlerons pas ici de cet aspect , car il ne s'agit pas de partage, mais le plus souvent d'arnaques déguisées (voir notre encadré). Au final cette solution à la fois disponible sur media center (Android, TV connectée, et n'importe quel appareil compatible avec Kodi ou un logiciel IPTV) ou PC via VLC Media Player est très sympa pour les étrangers, les polyglottes, les expatriés ou les personnes en vacances. On trouve en effet très facilement des chaînes chinoises, roumaines, russes, ukrainiennes, allemandes, turques, anglaises et bien sûr françaises !

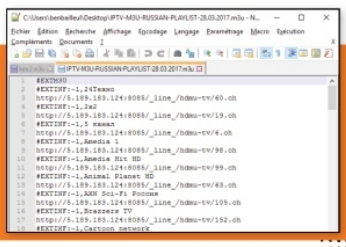
**Si je regarde la Champion's League sur une chaîne publique russe ou ukrainienne, suis-je un pirate ? Vous avez 4 heures...**

## LEXIQUE

***IPTV :**
Il s'agit juste d'un moyen d'avoir la télévision par Internet à la manière des box TV louées par vos FAI sauf qu'il s'agit d'un moyen détourné, mais gratuit d'obtenir des chaînes étrangères depuis un appareil connecté au téléviseur, un PC ou une smart TV.

## STRUCTURE D'UN FICHIER .M3U

Pour avoir des chaînes, il faudra télécharger ou se «fabriquer» une liste au format M3U (les formats M3U8 et le XSPF sont envisageables). Il est possible d'ouvrir ce type de fichiers avec le bloc-note de Windows ou Notepad++ par exemple. À l'intérieur il s'agit juste d'une liste avec une adresse IP par chaîne. Vous pouvez les scinder, les modifier, placer un fichier M3U localement ou mettre un lien vers un site. Lorsque vous avez fini, n'oubliez pas de changer le .txt en .m3u. Pour cela, il faudra afficher les extensions de fichiers. Faites un tour sur Google pour savoir comment faire avec votre système.



PAS À PAS

# IPTV : pour mobile et media center Android

CE QU'IL VOUS FAUT

IPTV

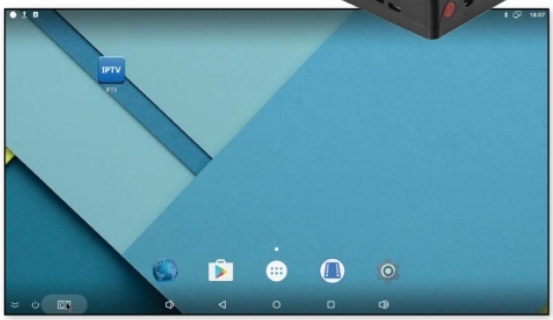
IPTV

OÙ LE TROUVER ? :
**https://goo.gl/Cl1GJ6**

DIFFICULTÉ :

## 01 LE MATÉRIEL

L'appli IPTV est disponible sur les appareils Android, mais il est possible d'utiliser un programme similaire sur certaines smart TV avec un uploader de liste MU3



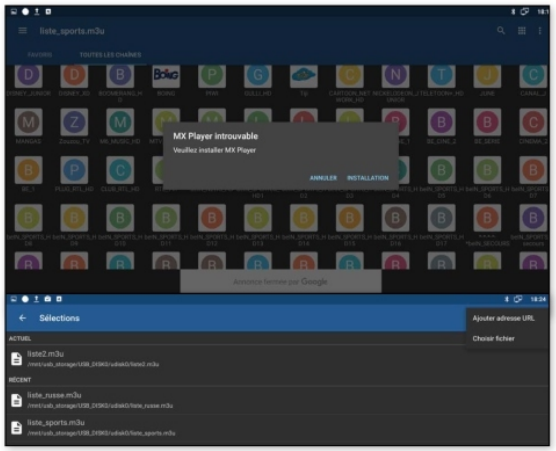

(regardez nos microfiches à la fin ou allez voir ici : **https://goo.gl/1dGGo8**). Nous avons pour notre part testé l'appli depuis un smartphone, une tablette et sur le boîtier media center Android que nous avions testé dans *Pirate Informatique* n°28. Ce type d'appareil, que l'on peut trouver pour une quarantaine d'euros (**https://goo.gl/d6ysZ3**), constitue une solution bon marché pour profiter de toutes ces chaînes sur votre TV.

## 02 LES CHAÎNES

Téléchargez l'appli et après vous être façonné une liste de chaînes ou en avoir téléchargé une toute faite sur Internet (cherchez **IPTV m3u** ou **IPTV channels list** sur Google), transférez la sur votre appareil grâce à une clé USB, via le réseau ou le Bluetooth. Ouvrez l'appli IPTV, faites + Ajouter une sélection et trouvez votre fichier M3U ou XSPF dans l'arborescence. Toutes les chaînes vont alors s'afficher.


## 03 POPCORN !

Par défaut le lecteur vidéo est MX Player (vous pouvez changer cela dans les **Réglages** du menu avec les trois traits horizontaux). Si vous n'avez pas cette appli, on vous proposera le téléchargement. À vous de sélectionner la chaîne de votre choix. Si cela ne fonctionne pas, c'est que les flux sont périmés. C'est pour cette raison que la plupart des sites qui proposent des fichiers M3U gratuitement les mettent à jour quotidiennement. Mettez toutes les chances de votre côté en téléchargeant plusieurs listes à l'avance...




## ATTENTION AUX BOÎTES «MIRACLES» !

Sur Internet on trouve des boîtiers sous Android préconfigurés avec Kodi ou d'autres applications IPTV. Ils sont généralement bien plus chers que les boîtiers normaux, car ils proposent en plus une sorte d'abonnement d'un an à des centaines de chaînes. Attention à ne pas tomber dans le panneau, car non seulement vous ne savez pas ce qui se passera dans un an, mais vous n'avez aucune garantie que la liste des chaînes sera mise à jour. De même, on trouve pas mal de prestataires payants qui proposent des chaînes pour 5 ou 10 €/mois. C'est une solution comme une autre, mais à la rédaction nous n'aimons pas trop l'idée de payer ce qui devrait normalement être partagé. D'autant que ces box peuvent contenir des mouchards ou faire office de botnets. À vous de voir.

PAS À PAS

# VLC Media Player : pour le PC

CE QU'IL VOUS FAUT

**VLC MEDIA PLAYER**

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

DIFFICULTÉ :

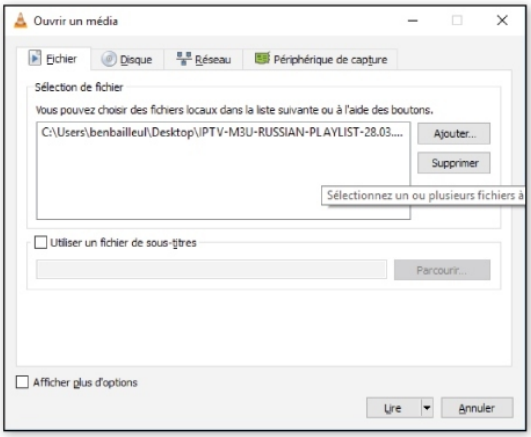
## 01 VOTRE LISTE

Cette solution est la meilleure si vous avez un PC (relié à la TV ou pas) ou si votre media center a une architecture PC puisque VLC Media Player est disponible sur Windows et Linux. Comme pour le précédent tuto, téléchargez le programme et après vous


être façonné une liste de chaînes ou en avoir téléchargé une toute faite sur Internet (cherchez **IPTV m3u** ou **IPTV channels list** sur Google), ouvrez VLC.

## 02 OUVREZ UNE CHAÎNE

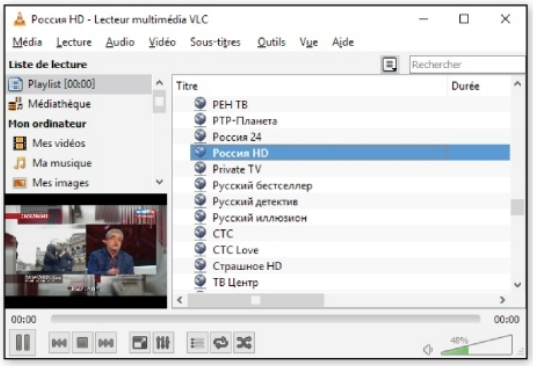
Allez dans **Media > Ouvrir un flux réseau** puis dans l'onglet **Fichier**, faites **Ajouter** et trouvez votre liste dans l'arborescence. Vous devriez voir la liste des chaînes, mais si ce n'est pas le cas, cliquez sur l'icône playlist en bas avec les trois




barres horizontales. Naturellement, VLC va tester les chaînes. Si vous voyez trop de messages d'avertissement, c'est que les flux sont périmés.

## 03 RESTEZ SUR LE MÊME FLUX

L'autre problème avec VLC c'est que dès qu'une chaîne va être un peu instable, le programme va changer sur la prochaine. Pour être bien sûr de rester sur la même chaîne, cliquez deux fois sur l'icône avec les deux flèches juste à côté de l'icône playlist (vous devriez voir un petit 1). Cela aura pour effet de rester sur le même flux quoiqu'il arrive. Attention, certaines listes de chaînes contiennent du porno. Faites le ménage si vous laissez les enfants choisir le programme.




# ÉCOUTER TOUTE LA MUSIQUE GRATUITEMENT AVEC NUCLEAR

**Au lieu d'investir une dizaine d'euros dans un service de streaming audio, pourquoi ne pas profiter d'un lecteur audio gratuit donnant accès gratuitement à quantité de titres ? C'est le service que rend Nuclear en proposant également les habituelles fonctionnalités de ces derniers. Le tout sans pub.**

Google Play Music, iTunes, Spotify… tous les services de streaming se valent. Ils proposent le même catalogue, pour un prix équivalent : 9,99 € par mois. En vous acquittant de cette somme, vous créez vos propres playlists, vous écoutez vos artistes en illimité…

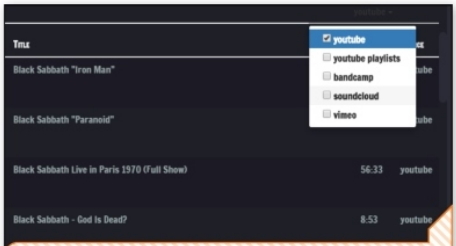
De nombreux services du même acabit, mais gratuits, se trouvent sur le Web. Une simple recherche sur votre moteur de recherche préféré avec les termes « streaming musique gratuit » vient le confirmer.

Nuclear s'ajoute ainsi à la liste de cette offre conséquente de service de streaming audio gratuit. Pas d'interface Web ici, il s'agit d'un bon vieux logiciel que vous installez sur votre PC. Depuis ce dernier, vous vous constituez votre bibliothèque musicale en piochant des chansons ou albums complets depuis différentes sources (Youtube, Bandcamp, Soundcloud ou encore Vimeo).

## COMPLET, MAIS PERFECTIBLE

Sur votre service de Cloud, vos fichiers apparaîtront cryptés et illisibles. Seul bémol : vous devrez impérativement installer Nuclear propose les fonctionnalités « classiques », celles que l'on trouve sur n'importe quel service de streaming audio. Recherche par chanson ou album, création de playlists à partir de ces derniers, découverte d'artistes similaires… l'utilisation du soft ne requiert aucune inscription. Notez que vous pouvez même télécharger, au format .mp3, les morceaux ou albums que vous recherchez.

Encore en version Alpha, le logiciel Nuclear n'échappe pas à quelques petits bugs de jeunesse (impossible de renommer ou de supprimer une playlist). Le développeur assure apporter des fonctionnalités supplémentaires à Nuclear au cours des semaines à venir… un logiciel à surveiller.




Lorsque vous recherchez un morceau, une playlist, un album via l'onglet **Search**, pensez à cocher, sur la droite, les services de streaming à sonder (YouTube, Bandcamp, SoundCloud…). En cochant YouTube playlists, vous dénicherez les playlists complètes de YouTube que vous ajoutez ensuite à votre propre liste de lecture dans Nuclear.

## LEXIQUE

**STREAMING :** Procédé de diffusion permettant la lecture en direct de flux audio ou vidéo. Cela s'oppose au principe de téléchargement qui présuppose la récupération préalable des données d'un morceau ou d'une vidéo pour en permettre la lecture.

PAS À PAS

# Organiser puis écouter sa musique

**CE QU'IL VOUS FAUT**

**NUCLEAR**

OÙ LE TROUVER ? : **https://goo.gl/qEqFNe**

DIFFICULTÉ :

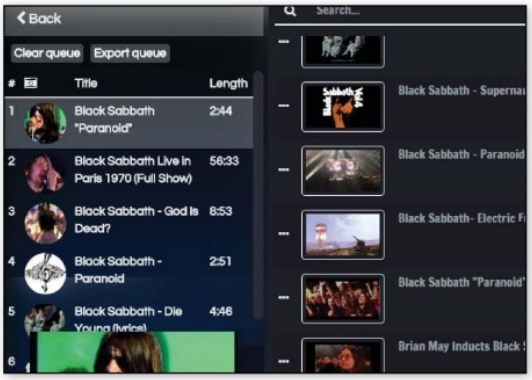
## 01 RECHERCHER

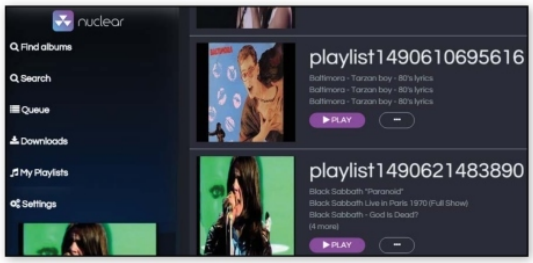
Ouvrez Nuclear puis cliquez sur **Find albums** puis recherchez à l'aide du nom de l'artiste ou de l'album désiré. Cliquez sur la pochette qui vous intéresse pour débuter la lecture. Les morceaux contenus dans l'album s'ajoutent dans la liste de


lecture (**Queue**). Avec **Search**, vous cherchez directement les morceaux que vous ajoutez à votre liste de lecture avec le **+** (en survolant la miniature).

## 02 CRÉER UNE PLAYLIST

Commencez par ajouter des morceaux à votre liste de lecture (**Queue**) en vous servant des outils de recherche présentés en étape 1. Allez ensuite dans l'onglet **Queue** pour choisir **Export queue**. Un message mentionne que votre playlist a été enregistrée. Faites **Clear queue** pour en démarrer une nouvelle




ou allez dans **My Playlists** puis choisissez **Play** en dessous de la playlist de votre choix pour en démarrer la lecture.

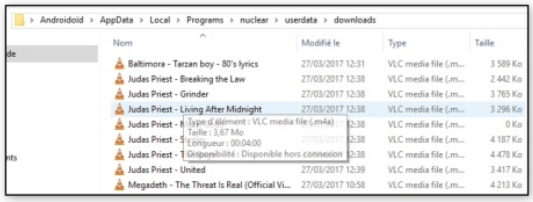
## 03 TÉLÉCHARGER

Depuis Nuclear, vous avez la possibilité de télécharger les morceaux de votre choix au format .mp3. Lancez votre recherche (de chanson ou d'album) via **Search** puis cliquez sur


les trois petits points avant de choisir **Download**. Allez ensuite dans l'onglet **Downloads** pour lancer l'opération avec **Start downloading**. Patientez quelques instants.

## 04 RETROUVER LES MORCEAUX

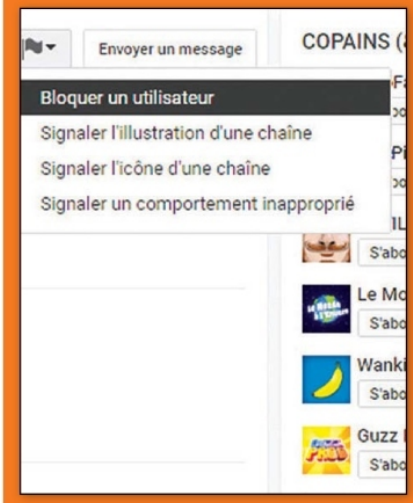
Partez à la pêche des morceaux que vous venez de télécharger. Pour ce faire, suivez le chemin **C:\Users\«votre nom d'utilisateur»\AppData\Local\Programs\nuclear\userdata**. Accédez aux morceaux que vous venez de télécharger en explorant le contenu du dossier **Downloads**. Faites un double clic sur le morceau de votre choix pour en débuter la lecture depuis votre lecteur multimédia de votre choix.



## #1 Bloquer les chaînes YouTube

AVEC YOUTUBE

Vous en avez plus que marre des vidéos de Squeezie, Cyprien, Amixem qui «pop» dans vos suggestions YouTube alors que vous ne les avez jamais regardées ? Rendez-vous sur la chaîne qui vous poursuit puis cliquez sur l'onglet **À propos**. Via le petit drapeau, sélectionnez **Bloquer un utilisateur** puis choisissez de **Valider**. Les suggestions de la chaîne visée disparaîtront.

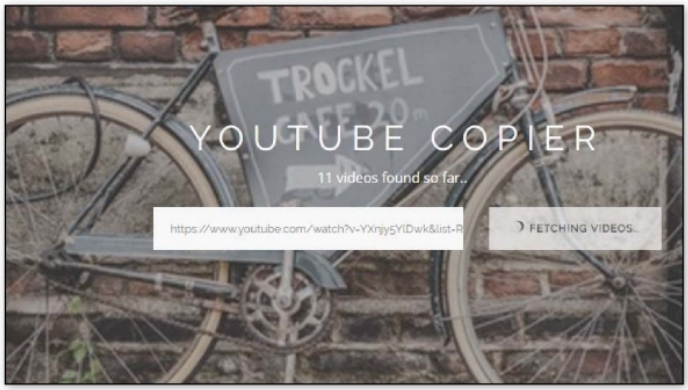



## #2 Copier une playlist YouTube

AVEC YOUTUBE COPIER

La playlist YouTube des plus grands tubes de Carlos, concoctée par Kévindu13leBG vous a tapé dans l'œil (comme on vous comprend !). Vous aimeriez avoir la même sur votre compte sans devoir la recréer vidéo par vidéo... Allez sur **YouTube Copier**, connectez-vous à votre compte Google, collez le lien de la playlist dans la boîte adéquate et validez avec **Fetch playlist**. À la fin, choisissez de la rendre publique (**Public copy**) ou privée (**Private copy**) sur votre compte.

Lien : **https://ctrlq.org/youtube/playlists**

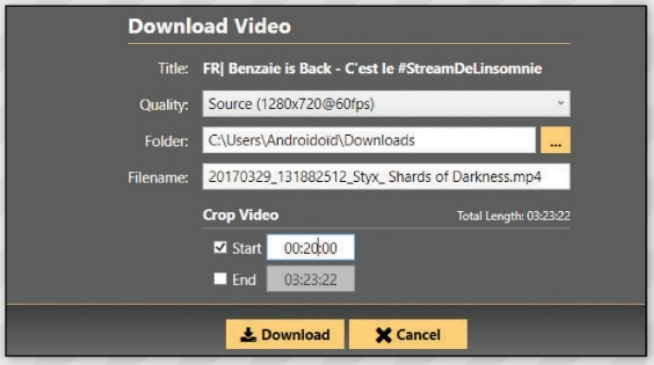



## #3 Télécharger les vidéos de Twitch

AVEC TWITCH LEECHER

Si vous êtes un gamer passionné de stream, voici un utilitaire permettant de télécharger les vidéos de la plate-forme Twitch. Sur Twitch Leecher, vous recherchez (**Search**) les chaînes que vous suivez habituellement. Notez que vous accédez directement au stream de votre choix en renseignant l'URL de ce dernier. Avec la petite icône représentant une flèche vous rapatriez directement au format .mp4 le stream sur votre bécane. Sachez que vous pouvez définir une plage d'enregistrement si seulement une partie du stream vous intéresse. Validez avec **Download**.

Lien : **https://goo.gl/7AmeGD**

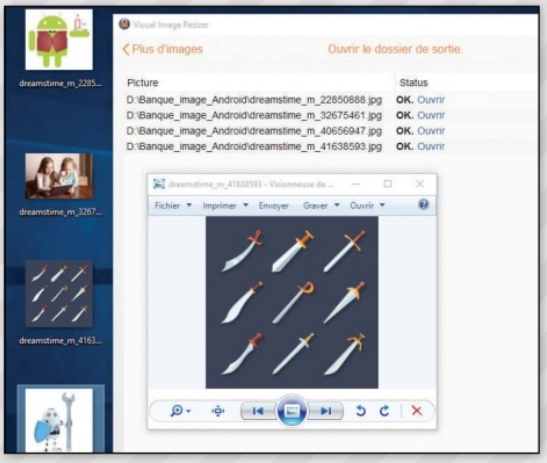


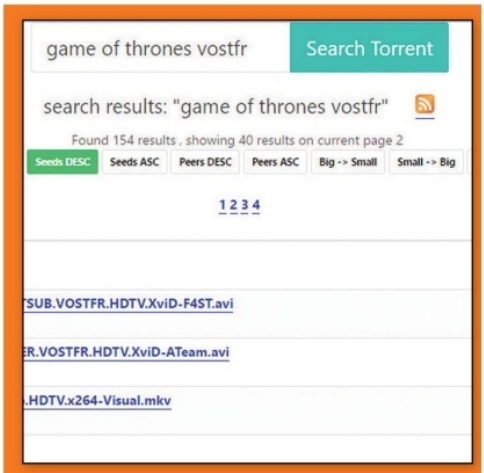
# #4 Redimensionner plusieurs images en même temps

**AVEC VISUAL IMAGE RESIZER**

Visual Image Resizer se charge de redimensionner plusieurs images simultanément, et ce qu'importe leur format. Le programme est capable de traiter près de 50 000 images en même temps... il y a de quoi faire. Sélectionnez les photos à modifier puis faites-les glisser dans le logiciel. Définissez le dossier de destination des photos corrigées (**Dossier de sortie**), le **Format** de sortie des images ainsi que la nature du redimensionnement. Vous pouvez choisir ici de renommer les images. Lancez l'opération avec **Redimensionner**.

Lien : **https://goo.gl/pdwhl1**




# #5 Chercher des torrents sans laisser de traces

**AVEC SKYTORRENTS**

Sans publicité, sans cookie, sans JavaScript, bref : sans aucune trace de votre passage en somme. Voilà ce que promet Skytorrents. Fort de plus de 12 millions de fichiers indexés , la recherche sur le moteur marche dans toutes les langues, et les résultats sont pertinents. L'interface est claire, sans fioriture, exactement comme on l'aime. Encore en bêta, voilà un site prometteur à surveiller de près.

Lien : **https://www.skytorrents.in**

# #6 De l'IPTV sur smartTV

**AVEC SIPTV.EU**

Vous avez aimé notre article sur l'IPTV à la page 43 mais vous n'avez qu'une smart TV à la maison ? Pas de problème, car si votre téléviseur connecté est compatible avec Smart IPTV (Samsung, LG, etc.), nous avons une solution ! Allez sur le store de votre TV, cherchez l'appli Smart IPTV et installez-là. A l'ouverture, l'appli vous donnera l'adresse MAC de votre appareil sur le réseau domestique. Ouvrez le site **Siptv.eu** et renseignez les champs avec votre adresse MAC, votre liste de chaînes M3U (voir notre article) ou un lien direct, cochez **Keep online** et cliquez sur **Upload** ou **Add Link** pour envoyer vos chaînes sur la télé ! Vous avez une solution plus pratique ou votre TV n'est pas compatible avec Smart IPTV ? Partagez vos astuces : benbailleul@idpresse.com...

Lien : **http://siptv.eu/mylist**


# X-MATÉRIELS

## > DataLocker Sentry FIP140-2

Les clés USB, ça se perd et ça se vole. C'est déjà assez embêtant de perdre des documents, mais si en plus ces derniers sont sensibles, ça peut virer au cauchemar: espionnage industriel, usurpation d'identité, chantage, etc. Pour éviter ce genre de désagréments, il existe des clés USB comportant un procédé de chiffrement matériel intégré. Vous pouvez certes créer un volume chiffré sur une clé USB «normale» avec VeraCrypt par exemple, mais les professionnels ou les plus réticents aux manipulations préfèreront opter pour une solution comme celle de DataLocker. Cette clé USB 3.0 baptisée Sentry propose un chiffrement natif AES 256 avec un mode XTS (qui utilise deux clés différentes pour le bloc et le vecteur d'initialisation). En gros, il s'agit d'une seconde couche de protection qui n'existait pas sur les modèles précédents. Comme ses grandes sœurs, cette Sentry nouvelle génération est certifiée par le National Institute of Standards and Technology et affiche la validation FIPS 140-2. Bizarrement le communiqué de presse parle d'une certification de niveau 3 alors que «Level 2» est affiché sur la boîte. Voyons comment cela fonctionne...


Prix : **de 100 € pour la version 4 Go à 300 € pour la version 32 Go (pas de prix pour la 64 Go)**

**https://datalocker.com**


## Zalman ZM-VE500,

### UN DISQUE DUR MULTI-BOOT

Ce périphérique USB3.0 se présente comme une simple coque pour disque dur 2,5 pouces (ceux des PC portables), mais il présente la particularité de proposer un écran LCD et un mini-pavé numérique. Ce dispositif sert en fait à booter son PC sur l'ISO de votre choix. Vous pouvez donc mettre plusieurs OS (distribution Linux, LiveCD, Windows) sur votre disque dur et choisir lequel lancer au moment opportun. Au niveau de l'alimentation, pas de problème puisque l'appareil est auto-alimenté. Vous n'aurez plus besoin de graver un DVD-R à chaque nouvelle version de Kali ou de MediCat. On peut aussi imaginer d'y placer ses ISO de jeux ou de DVD vidéo. Bien sûr vous pouvez faire la même chose avec le logiciel MultiBootUSB, mais il faut dire que ce boîtier a la classe et dispose en plus d'un chiffrement AES256bits intégré.

Prix : **75 €** **www.zalman.com**

## Auvisio Game Capture V3,

### SOURIEZ VOUS ÊTES CAPTURÉ !

Ce petit boîtier permet de capturer tous les signaux vidéo des appareils qui seront branchés dessus, qu'ils soient analogiques ou numériques. Vous pouvez vous en servir comme d'un magnétoscope numérique (comment ça, *c'est quoi un magnétoscope ?*) pour enregistrer la TNT ou le satellite, comme d'un appareil de capture pour vos parties de jeux vidéo ou de système pour sauvegarder vos anciens films de vacances d'analogique en numérique. Pour cela, il dispose d'une connectique très complète : RCA et HDMI (in et out), USB, MicroSD et Micro-USB 2.0 (pour brancher sur votre PC). L'appareil autorise des résolutions d'enregistrement HD (1080p ou 720p) et encapsule directement en MP4.

Prix : **130 €** **www.pearl.fr**

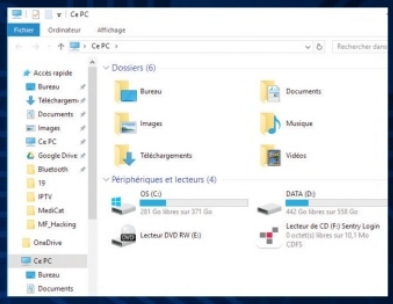
NOTRE TEST EXCLUSIF

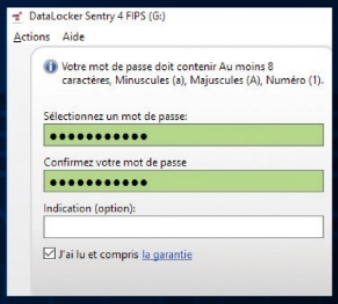
# DataLocker Sentry, la clé USB de James Bond


**Le packaging de la DataLocker Sentry est minimaliste : la clé et juste un cordon pour l'attacher autour du cou. La clé USB en elle-même est par contre robuste. Elle pèse son poids (10 g) et ne fait pas du tout «toc». Un bon point pour une clé censée renfermer des secrets. Déballage...**

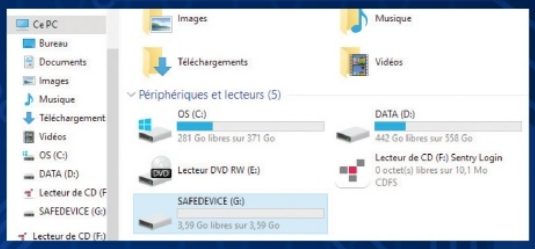
## #1 PREMIER BRANCHEMENT

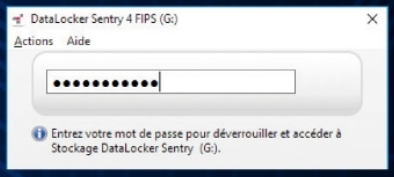
Branchez la clé USB sur votre PC et attendez quelques secondes le temps de voir la nouvelle lettre de lecteur s'afficher. Double-cliquez dessus et attendez que le programme intégré s'initialise. On vous demandera alors de choisir votre mot de passe et une indication en cas d'oubli. Attention si votre mot de passe est trop faible, ce type de clé ne sert à rien. D'un autre côté on imagine mal (même si rien n'est impossible) une attaque brute force ou par dictionnaire, sur un appareil comme celui-ci.




## #2 LE VOLUME CHIFFRÉ

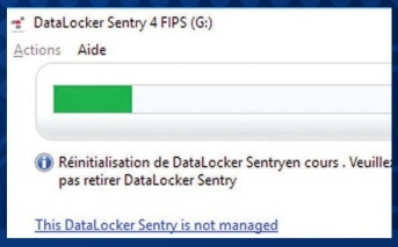


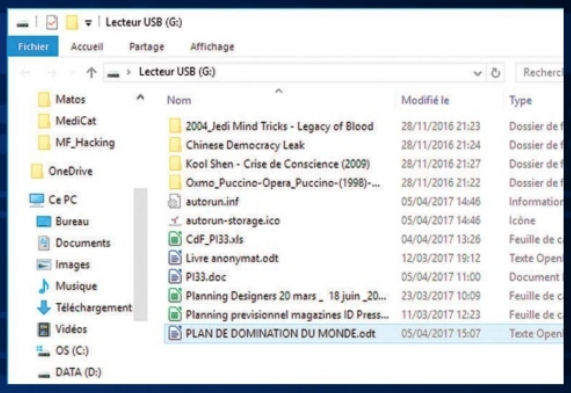




Attention à la question de sécurité, car on peut en savoir beaucoup sur vous avec les réseaux sociaux. Le nom de votre belle-mère ou la marque de votre première voiture ne sont pas des indications assez sécurisées. Cette option est d'ailleurs optionnelle et nous la déconseillons. Tapez sur **Entrée** puis votre nouveau mot de passe pour avoir accès au volume caché de 3,59 Go (pour la version 4 Gb). Votre antivirus va peut-être paniquer, car la clé contient naturellement un fichier autorun.inf.

## #3 VOS DOCUMENTS À L'ABRI !

Copiez-collez les documents que vous souhaitez dans ce volume et déconnectez la clé comme vous le feriez avec n'importe quelle autre. Si vous souhaitez protéger vos documents en laissant la clé branchée, il suffit de faire un clic droit dans la zone notification et faire **Blocage** pour rendre indisponible le volume chiffré. Lorsque vous voudrez retrouver vos fichiers, il faudra juste saisir à nouveau le mot de passe. Si vous avez perdu celui-ci, la clé sera toujours utilisable, mais vous perdrez vos documents. Depuis la fenêtre de saisie de mot de passe, faites **Action > Réinitialisation**.




IDPRESSE id presse
L 12730 - 33 - F: 4,90 € - RD

France METRO : 4,90 € - BEL/LUX : 6 € - DOM : 6,10 € - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – NCAL/A : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd