+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 26

PIRATE [INFORMATIQUE]

LE GUIDE DU PIRATE

60 HACKS & CRACKS

100% HACKING
AVEC CD GRATUIT
> PLUS DE 50 FICHES PRATIQUES

Mobile
eMails
Anti-NSA
Mots de passe
Films & Séries
Raspberry Pi
Géolocalisation
Détecteur d'espions

0% PUB
0 CENSURE

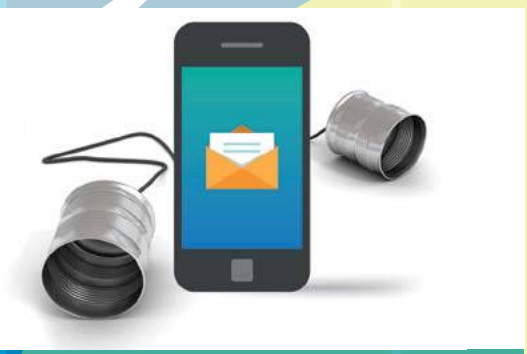
HACKING
CRACKER UN MOT DE PASSE WINDOWS

SÉCURITÉ
PROTÉGEZ-VOUS DES NOUVELLES MENACES

ANONYMAT
PEERIO MASQUE ET CHIFFRE TOUS VOS ÉCHANGES

SOMMAIRE

PROTECTION/ANONYMAT



HACKING

MULTIMÉDIA

+ NOTRE TEST

LES CAHIERS DU HACKER
PIRATE [INFORMATIQUE]

N°26– Août / Oct. 2015

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

Directeur de la publication :
David Côme
Tetsuo Shima : Benoît BAILLEUL
Masaru & Takashi :
Yann Peyrot & Jérémy Jager
Kei & Kaneda :
Stéphanie Compain & Sergueï Afanasiuk

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

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

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

ÉDITO

Depuis que nous avons pu vous demander votre avis sur *Pirate Informatique* (voir page 8) nous allons pouvoir vous proposer un magazine encore plus proche de vos attentes. Nous avons été notamment surpris par les très bonnes idées d'articles que vous nous avez suggérées. Lorsqu'une petite équipe comme la nôtre a la tête dans le guidon pour sortir le prochain numéro en temps et en heure, il est parfois un peu compliqué de relever la tête et trouver des sujets originaux. Grâce à vous, nous avons fait le plein ! Dans ce numéro vous trouverez donc des articles concernant le respect de la vie privée, mais aussi du chiffrement, du crack de mots de passe et l'interview exclusive de J-P Lesueur, le sympathique créateur de DarkComet RAT. Encore un magazine bien rempli !

Comme à chaque fois, vous retrouverez sur notre CD tous les logiciels dont nous parlons dans le magazine ainsi que certains anciens articles qui vous aideront à mieux comprendre nos démonstrations. Enfin, nous vous invitons à vous rendre à la page 22 pour vous abonner gratuitement à la mailing-list de magazine et être tenu au courant des parutions.

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

Bonne lecture !

Benoît BAILLEUL.

HACKTUALITÉS

ARNAQUES, BOÎTIERS ET CHAÎNES PIRATÉES

Voici une actualité qui nous rappelle les décodeurs Canal + pirates des années 80/90... La police anglaise a en effet fait une descente chez une revendeuse de boîtiers TV sous Android. La femme de 48 ans vendait ces box préconfigurées avec Popcorn Time, le media center Kodi et différents plugins permettant d'accéder à des programmes TV sans bourse délier : série TV, matchs de foot, films et chaîne à accès payant, etc.

Dommage collatéral de cette saisie de 1000 appareils, Amazon a banni le très légal Kodi de son App-Shop ! Notons tout de même que ces boîtiers, achetés pour une trentaine d'euros sur des sites chinois, étaient revendus 5 à 8 fois plus cher après l'installation de ces plugins IPTV pourtant gratuits. Pour comprendre comment cela fonctionne, rendez-vous à la page 46 !

Ce type d'appareil Android à brancher sur votre TV permet d'installer différentes applications pour accéder à du contenu et des chaînes piratés.

SANS CONTACT, MAIS AVEC DE GROS RISQUES

Nous vous avions déjà parlé des risques du paiement sans contact à partir de cartes bancaires avec puce NFC. Non seulement les clients ne sont pas forcement au courant qu'ils en possèdent (alors qu'ils sont plus de 30 millions en circulation), mais il faut parfois batailler avec son banquier pour désactiver cette fonction ou obtenir une carte bancaire sans cette fonctionnalité. L'année dernière des chercheurs britanniques avaient réussi à déjouer les limitations de ce type de paiement (20 € par transaction avec une limite de 100€/jour), mais c'est au tour du CNRS de tirer la sonnette d'alarme. Pour ces scientifiques, il s'agit même d'un retour en arrière puisque, comme à la belle époque du sabot, il est possible pour un commerçant de prélever plusieurs fois une somme. Il est aussi possible de voler votre argent en plaçant un lecteur à proximité et même de relayer les données bancaires à un complice qui fera ses achats avec vos deniers. Deux solutions s'offrent à vous pour éviter la fraude : fabriquer une cage de faraday dans votre portefeuille ou détruire physiquement la puce NFC avec une perceuse ! C'est ce que nous verrons dans le prochain numéro...

RETOUR DE BÂTON

Nous nous réjouissons rarement lorsqu'une société se fait pirater, mais il faut bien reconnaître que HackingTeam l'a bien cherché. Cette compagnie italienne, qui a reçu le prix d'*Ennemi d'Internet* par Reporters Sans Frontières, est connue pour fournir à plusieurs pays des solutions de surveillance. Parmi ses clients on compte des régimes très autoritaires comme ceux du Soudan, du Kazakhstan ou de la Malaisie. Outre une liste détaillée de contrats et de mots de passe, on en apprend un peu plus sur leur «produit phare», Da Vinci, un trojan permettant d'accéder à plusieurs moyens de communication (e-mails, conversation Skype) ainsi qu'à géolocaliser les citoyens qui aspirent à la liberté. SI vous voulez en savoir plus, les 400 Go de données volées sont disponibles un peu partout sur le Net. C'est beau la mondialisation.

HACKTUALITÉS

Avec l'aimable autorisation de notre ami Zach Weiner

Windows XP n'en finit plus de mourir

Alors que Microsoft a arrêté d'éditer des mises à jour pour son Windows XP depuis avril 2014, les utilisateurs de ce système d'exploitation représentent encore pas loin de 12 % de part de marché. La situation est préoccupante, car depuis le 14 juillet 2015, Microsoft ne met plus à jour la base virale de l'antivirus Security Essentials inclus dans XP. Utilisateurs de Windows XP, vous êtes maintenant complètement nus devant les attaques et les virus. Bien sûr vous pouvez installer un antivirus gratuit, mais si vous avez encore ce vieil OS datant de 2002, nous vous conseillons de mettre à jour vers une version plus récente (a moins de n'utiliser XP que pour du travail «hors ligne»). Si vous n'avez pas envie de débourser un centime, pourquoi ne *pas changer de crèmerie et opter pour la distribution Linux Mageia (voir Pirate Informatique* n°23) ?!

LE CHIFFRE 15,6 MILLIONS D'€

C'est l'amende colossale que doit payer Dimitri Mader avec un an de prison ferme en bonus ! Déjà condamné au civil, c'est la douche froide pour le webmaster de Wawa-Mania, le site de téléchargement direct crée en 2009. Alors certes, même si cette personne s'est clairement enrichie avec les revenus générés par la pub (nous ne croyons pas à la thèse des 42 000 € partis en frais de serveur), la condamnation est tellement disproportionnée qu'elle en devient ridicule. L'amende est un calcul d'apothicaire basé sur le nombre de téléchargements théoriques et le prix d'un DVD. Notons aussi que Wawa-Mania n'hébergeait aucun fichier, il s'agissait juste d'un forum où les intervenants s'échangeaient des liens. Bien sûr les émissions de télévision où il apparaissait à visage découvert, ses phrases-chocs («Hadopi ça sert à rien») et sa fuite aux Philippines n'ont pas plaidé en sa faveur... Parmi les sociétés qui doivent se partager ces (hypothétiques) millions, nous ne comptons que des PME au bord de la faillite : Disney, Paramount, Twentieth Century Fox, Universal, Warner Bros, Microsoft, etc.

RÉSULTAT DU SONDAGE *Pirate Informatique*

Merci aux 752 lecteurs qui ont répondu au sondage en ligne lancé dans notre précédent numéro ! Grâce à votre participation, nous avons pu vous connaître un peu mieux et cerner vos attentes. Des changements ont d'ores et déjà été apportés à la formule de Pirate Informatique que vous tenez dans les mains. Vous trouverez donc moins d'articles Multimédia puisque c'est la rubrique que vous aimez le moins. Les microfiches, le CD et les articles «Raspberry Pi» resteront en place puisqu'ils ont été plébiscités. Nous vous proposerons aussi des articles un peu plus techniques à l'avenir puisque même si 87 % des lecteurs trouvent les articles à leur goût, vous êtes 12 % a les trouver parfois trop «faciles».

Les questions qui fâchent

Dans la partie du sondage où nous vous demandions de suggérer des changements, nous avons souvent noté les mêmes questions. Vous êtes par exemple nombreux à nous demander plus de pages ou des parutions plus rapprochées. C'est à l'heure actuelle impossible à moins de baisser la qualité des articles : les bons journalistes spécialisés dans le hacking ne courent pas les rues ! Vous êtes aussi nombreux à nous demander des articles orientés Linux. Nous vous avons entendu et nous vous proposerons un article à chaque nouveau numéro, à commencer par celui-ci (voir page 39). Par contre nous ne désirons pas écrire sur les sujets Macintosh. Ce système n'est vraiment pas adapté au hacking et à moins d'une grosse actualité, nous n'en parlerons jamais. Concernant les articles sur les smartphones, vous êtes partagés. Certains en veulent plus et d'autres...moins. Pour les premiers, nous vous conseillons de courir chez votre marchand de journaux pour acquérir le numéro 4 des Dossiers du Pirate consacré exclusivement aux appareils mobiles sous Android et iOS. Enfin nous avons toujours une petite partie de jeunes chênes qui nous accusent de ne pas être de «vrais hackers» car pour eux, le hacking est synonyme de piratage de comptes Facebook, de vols de numéros de carte de crédit ou de création de virus. Si vous vous reconnaissez, vous êtes les bienvenus parmi nous, mais vous n'êtes peut-être pas au bon endroit...

RÉSULTAT DU CONCOURS

En participant au sondage, vous aviez une chance de gagner une clé USB contenant tous les numéros de Pirate Informatique au format PDF. Félicitation à Didier Filippetti (95) qui remporte la clé. Vous êtes jaloux et vous la vouliez pour vous cette clé ? Ce sera peut-être possible dans peu de temps (voir notre autre encadré)...

PRÉ-COMMANDE DES CLÉS USB PIRATE INFORMATIQUE

Dans notre sondage nous avons aussi noté beaucoup de lecteurs qui veulent acheter d'anciens numéros ou qui nous demandent des articles que nous avons déjà réalisés. Comme vous le savez, il n'est pas possible pour nous de fournir les numéros passés pour des questions pratiques et logistiques. Par contre nous désirons vendre des clés USB contenant tous les anciens numéros, comme celle qui a été gagnée par Didier ! Pour ne pas commander trop de clés auprès de notre fournisseur, il nous faudrait savoir combien de personnes sont intéressées. Si vous voulez acquérir une clé de ce type au tarif de 15 €, envoyez un e-mail à cette adresse : **usb@idpresse.com**. Cela ne vous engage à rien, mais ne le faites que si vous désirez vraiment cet objet. Merci !

BITMESSAGE:
UNE ALTERNATIVE À PGP

Nous vous avions déjà parlé de chiffrement d'e-mails avec des solutions plus ou moins complexe à mettre en place. La mode est au webmail (voir notre article sur Lavaboom à la page 26) mais Bitmessage s'adresse à ceux qui préfèrent écrire depuis un logiciel. Choisissez votre camp !

LEXIQUE

*** CHIFFREMENT ASYMÉTRIQUE :** Ce type de chiffrement repose sur l'utilisation d'une clé publique (qui est diffusée à ses correspondants) et d'une clé privée (gardée secrète dans votre PC). L'expéditeur d'un message peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder.

Inventé par Phil Zimmerman en 1991, PGP est un logiciel qui garantit la confidentialité des échanges par e-mail. Le problème, c'est que ce système de chiffrement asymétrique est assez lourd à mettre en pratique : il faut se créer une clé publique que l'on doit changer régulièrement et envoyer à tous ses correspondants par un moyen sûr tout en gardant les clés de vos amis. L'autre point noir concerne la centralisation de la technologie : tout passe par un serveur et il est très complexe de masquer son identité. Même si on ne peut pas savoir la teneur d'une conversation, on peut savoir qui parle à qui.

PLUS SIMPLE QUE PGP ET TOUT AUSSI PUISSANT

Bitmessage propose de chiffrer vos communications sans réglages complexes, échange de clés ou serveur central. Il s'agit en fait de mettre les intervenants en relation grâce au peer-to-peer. Vous disposez d'une adresse du type BM-2nTX1KchxgnmHvy9ntCN9r7sgK TraxczzyE qui correspond au hash de votre clé publique. Vous n'avez pas à vous inscrire à quoi que ce soit tout en créant autant d'adresses que vous le voulez. Sans avoir à gérer de certificat d'authentification, il sera impossible pour un tiers d'usurper une identité.

PAS À PAS

Création d'une adresse et premier message

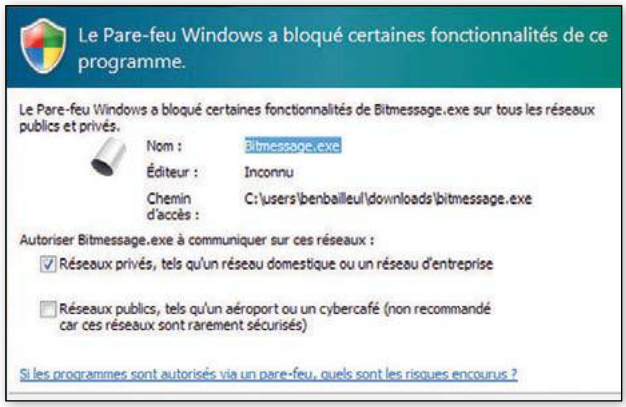
CE QU'IL VOUS FAUT

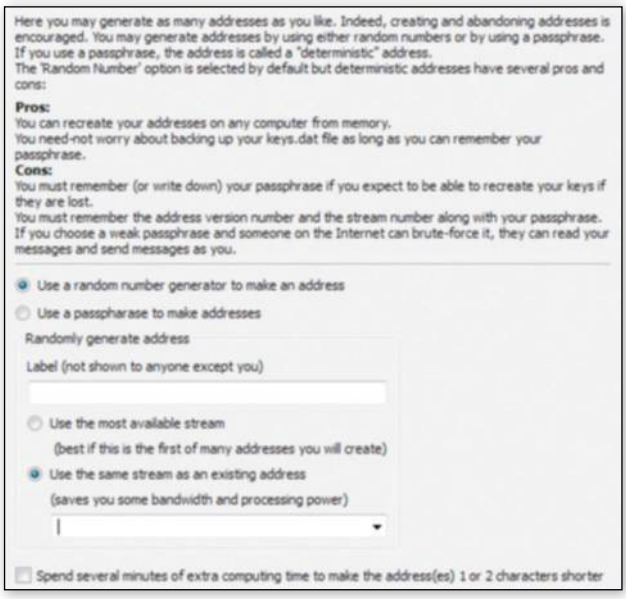
BITMESSAGE

OÙ LE TROUVER ? :
http://goo.gl/J86ic

DIFFICULTÉ :

01 CRÉATION DE VOTRE CLÉ

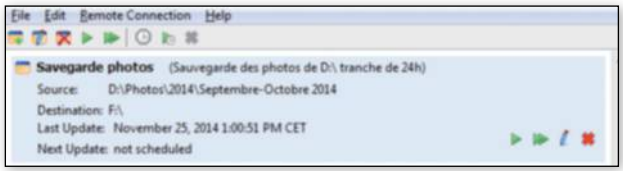


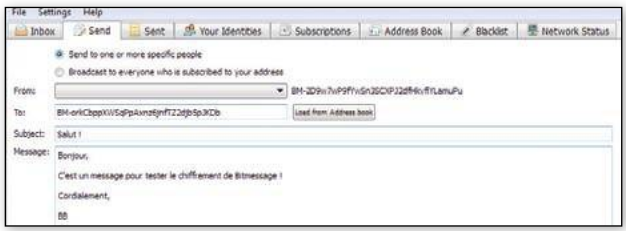


Bitmessage ne s'installe pas, il suffit de double-cliquer sur le fichier EXE pour le démarrer. Votre pare-feu devrait vous demander de créer une exception. Dans le cas contraire, libérez le port8444.
En premierlieu, allez dans l'onglet **Your Identities** et faites **New**. Il est possible de générer votre adresse en utilisant un nombre aléatoire ou un mot de passe (**passphrase**). Cette dernière solution est idéale pour retrouver ses adresses sur un autre PC ou en cas de perte du fichier **key.dat**. Par contre, utilisez un mot de passe long et complexe pour éviter qu'un pirate ne puisse le cracker et avoir accès à vos messages.

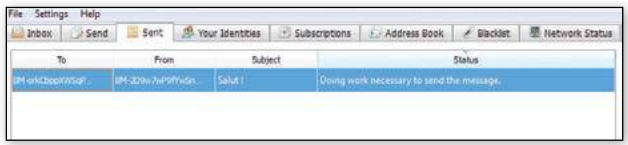
02 LA RÉDACTION ET L'ENVOI DU MESSAGE

En cochant la case tout en bas, vous pouvez réduire votre adresse de 1 ou 2caractères contre quelques minutes de calculs supplémentaires. Faites **OK** et attendez que le logiciel génère votre adresse. Une fois que c'est terminé, faites un clic droit dans cette suite alphanumérique pour voir les options. Il est possible de mettre l'adresse dans le presse-papier pour la coller dans un logiciel et la transmettre facilement. Pour votre premiermessage, allez dans l'onglet **Send** et mettez l'adresse d'un de vos amis dans le champ **To:.** Tapez votre message et faites **Send**. Une nouvelle fenêtre va alors s'ouvrir (l'onglet **Sent**) et vous pourrez voir la progression de l'envoi dans **Status** (Authentification, chiffrement, accusé de réception, etc.).





03 LES AUTRES OPTIONS



Cela peut prendre quelques minutes. Si vous essayez avec cette adresse (**BM-orkCbppXWSqPpAxnz6jnfTZ2djb5pJKDb**), vous pourrez tester le processus du début à la fin. Il s'agit d'une adresse «écho» qui vous répondra automatiquement. En ce qui concerne les autres fonctionnalités, sachez que l'onglet **Adress book** permet de garder les coordonnées de vos correspondants et **Blacklist** fait office de filtre. Sachez aussi que dans **Settings>User Interface**, vous pouvez cocher la case qui vous permettra de lancer l'application depuis une clé USB ().

NOS GUIDES WINDOWS 100% PRATIQUES

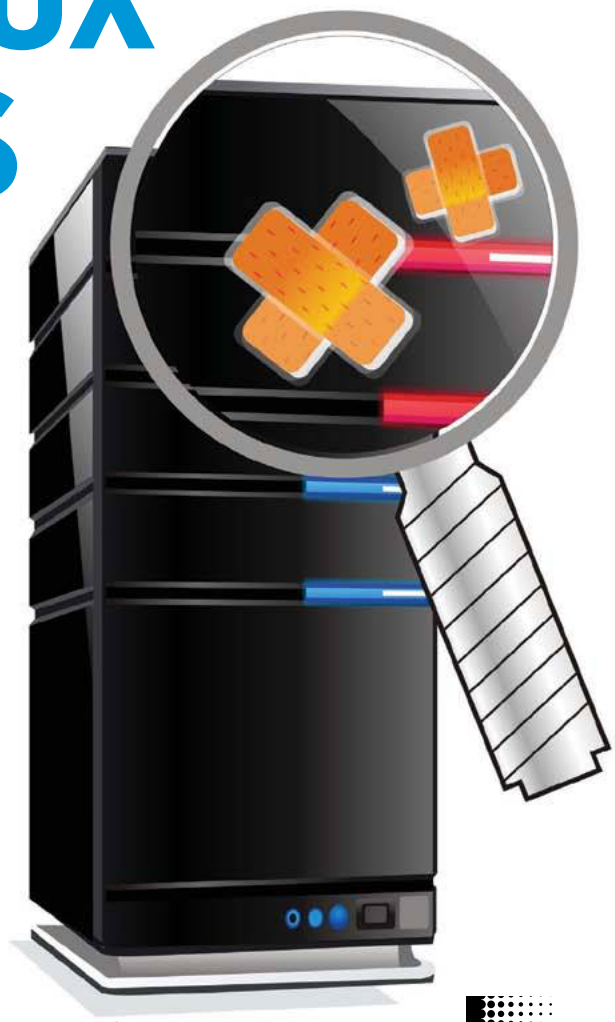
POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3€

Chez votre marchand de journaux

PROTÉGEZ-VOUS DES NOUVEAUX MALWARES

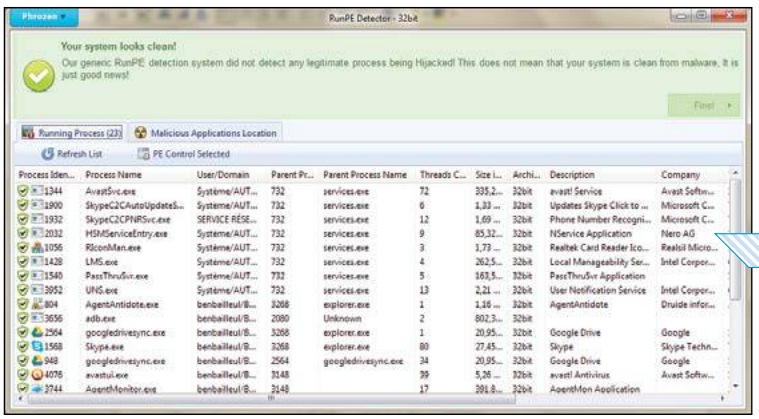


Phrozen Soft a dernièrement mis en ligne deux nouveaux logiciels de sécurité pour se prémunir de deux types d'attaques particulièrement sournoises. La première cible les volumes NTFS et la possibilité qu'ils ont à cacher des fichiers malveillants tandis que l'autre usurpe un processus légitime pour mieux attaquer...

Phrozen ADS Revealer et RunPE Detector sont l'œuvre de Jean-Pierre Lesueur (voir notre interview). Le premier détecte sur les volumes NTFS la présence de fichiers cachés pouvant être des malwares : les fichiers ADS. Ces derniers, bien qu'invisibles depuis l'explorateur de fichiers Windows, ont un contenu bien physique et peuvent pulluler sans éveiller les soupçons de l'utilisateur. Le développeur a même prouvé que malgré les restrictions de Microsoft, il est toujours possible d'exécuter du code directement à partir d'un emplacement ADS...

USURPER UN PROCESSUS, C'EST POSSIBLE ?

RunPE Detector s'occupe lui de repérer la présence de malwares de type RAT (contrôle à distance, comme DarkComet). Ce type de logiciel malveillant va démarrer un processus légitime (souvent Firefox ou explorer.exe) pour le remplacer juste avant sa mise en mémoire par l'image mémoire du malware. Ce dernier profite de ces droits pour passer à travers les mailles du pare-feu. RunPE Detector va comparer l'empreinte du processus en mémoire avec son image physique. Si les différences avérées, l'alerte est donnée.



Rien à signaler ici mais attention, Phrozen ADS Revealer et RunPE Detector sont à utiliser en plus de votre antivirus habituel !

LEXIQUE

***MALWARE :**
C'est le terme générique pour désigner les logiciels malveillants. Un malware peut être un virus, un vers, un trojan, un ransomware, etc.

***PROCESSUS :**
Windows est architecturé en services (processus) fonctionnant en arrière-plan. Il s'agit juste de programmes lancés par vous ou par le système et qui «tournent» en tâche de fond.

PAS À PAS

Les fichiers ADS à la loupe !

CE QU'IL VOUS FAUT

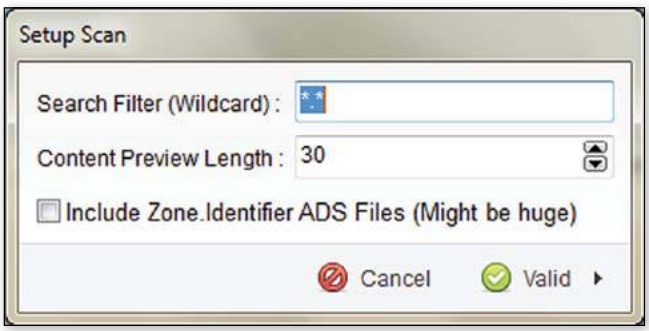
PHROZEN ADS REVEALER & RUNPE DETECTOR

OÙ LE TROUVER ? : **www.phrozensoft.com**

DIFFICULTÉ :

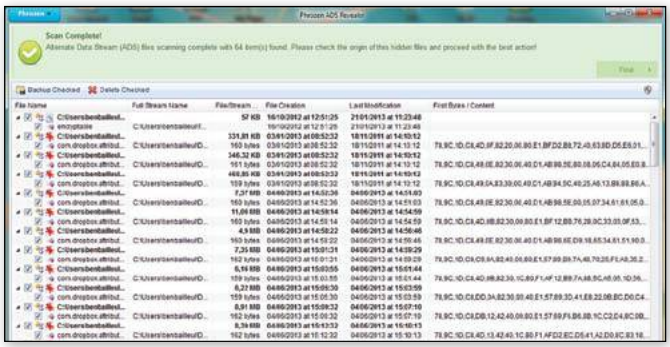
01 LES OPTIONS

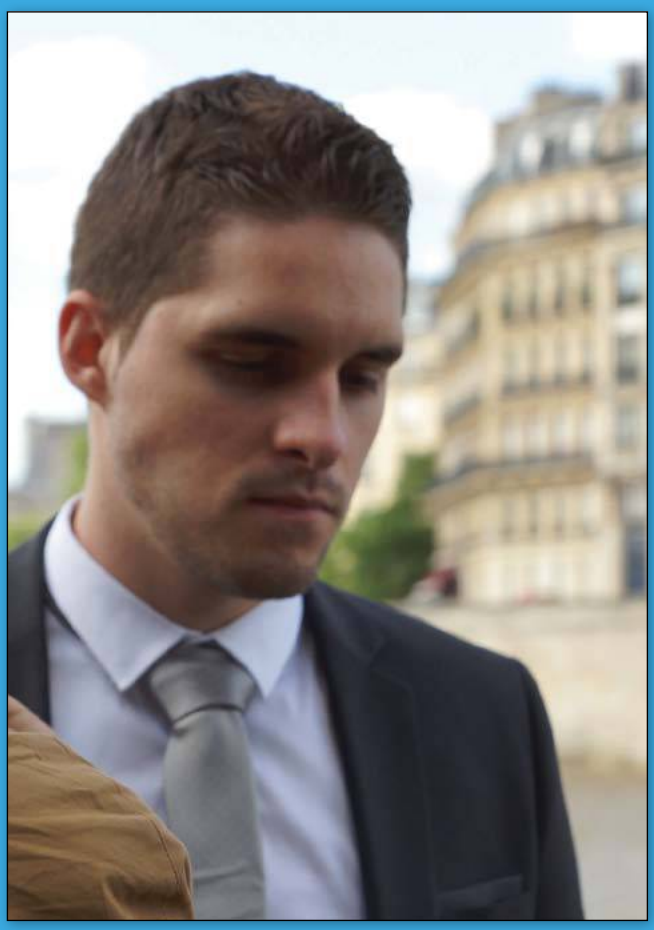
Le logiciel ne s'installe pas, il suffit de décompacter l'archive et de le lancer en tant qu'administrateur. Faites ensuite **Run Scan** puis choisissez la cible: tout le système (**Full System**), Tout le disque (**Target Drive**) ou un dossier particulier (**Target Folder**). Il est possible de filtrer la recherche (***.*** pour tous les fichiers, ***.exe** pour tous les fichiers EXE, etc.) La dernière case permet de scanner le fichier ADS **Zone.Identifier** utilisé par Microsoft. Ce scan est très lourd, mais si vous êtes sûr d'une infection...



02 LA MARCHE À SUIVRE

A la fin du scan, ADS Revealer va dresser une liste de fichiers. Dans notre exemple le logiciel n'a détecté que des miniatures de fichiers multimédias. Ne pensez pas pour autant qu'il s'agit de faux positif! Un ADS peut être tout aussi légitime qu'illégitime. Le but est ici de voir tous les fichiers ADS existants sur son disque et de choisir la meilleure action: garder le fichier s'il parait normal ou le supprimer s'il est louche. Les colonnes **File Creation** et **Last Modification** devraient vous être utile pour faire le tri...





Interview de Jean-Pierre Lesueur, créateur de DarkComet RAT et fondateur de la société Phrozen SASU

POUVEZ-VOUS VOUS PRÉSENTER EN QUELQUE LIGNE, VOTRE PARCOURS ET CE QUE VOUS FAITES ACTUELLEMENT ?

J'ai bientôt 25 ans et je suis un passionné d'informatique depuis mes 15 ans, particulièrement de la sécurité informatique appliquée en programmation. J'ai eu un parcours assez banal : Bac STI puis BTS d'informatique et gestion. Le but était d'obtenir un minimum de diplômes pour commencer à bosser dans le domaine qui me plaisait. J'ai travaillé pendant 6 ans dans une société d'informatique en tant qu'analyste-programmeur et en parallèle de mes études/travail je développais déjà mes propres solutions.

PAS À PAS

Stop à l'usurpation de processus !

CE QU'IL VOUS FAUT

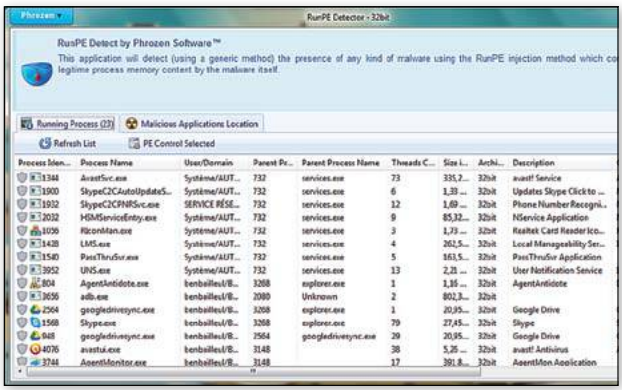
PHROZEN ADS REVEALER & RUNPE DETECTOR

OÙ LE TROUVER ? : **www.phrozensoft.com**

DIFFICULTÉ :

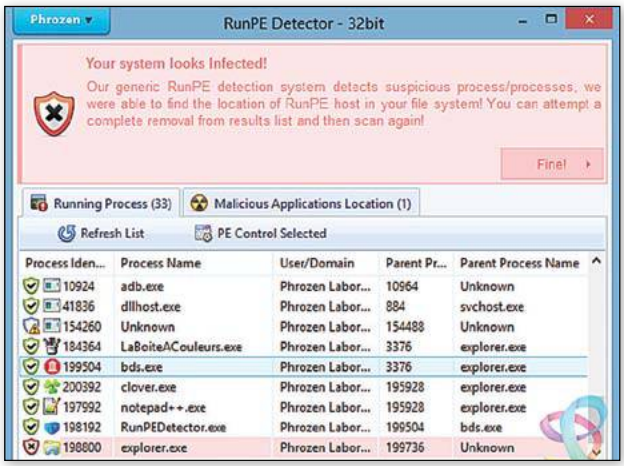
01 LA LISTE DES PROCESSUS

Comme ADS Revealer, il faudra décompacter l'archive et le lancer en tant qu'administrateur. Vous verrez alors l'intégralité des processus qui tournent en tâche de fond sur votre machine. Faites alors **Run Scan**. Le logiciel va alors comparer les empreintes de ces processus avec des empreintes «connues».



02 USURPATION DÉTECTÉE !

Dans notre exemple, le processus n°198800 est suspect. Il se nomme **explorer.exe**, mais n'a pas l'empreinte attendue. Il s'agit en fait de DarkComet qui a usurpé l'identité de l'explorateur Windows ! En cliquant sur **Fine** ! Vous pourrez le supprimer...



VOUS ÊTES LE CONCEPTEUR DE DARKCOMET RAT ET DE PHROZEN KEYLOGGER (PRÉSENTÉS DANS NOTRE PRÉCÉDENT NUMÉRO, NDLR). CES DEUX LOGICIELS NE SONT PLUS DISPONIBLES SUR VOTRE SITE, POURRIEZ-VOUS NOUS EXPLIQUER POURQUOI ?

Je suis en effet le concepteur du logiciel espion DarkComet RAT. Cependant le développement et sa mise à disposition ont été stoppés en Juin 2012 suite à une forte pression médiatique et à la possible utilisation de DarkComet RAT par les services secrets Syrien afin de traquer les opposants du régime. Ceci n'est que la partie immergée de l'iceberg, car d'autres faits sordides se sont enchaînés à la suite : utilisation de DarkComet par des pirates Somaliens pour attaquer des bases de l'armée américaine, tentative d'attaque chez Areva, affaire d'infections informatique surfant sur l'affaire Charlie Hebdo, etc. N'aillant jamais cru que le logiciel puisse être à ce point détourné de son utilisation primaire, j'ai décidé d'y mettre un terme. En ce qui concerne Phrozen Keylogger, il devrait être mis à disposition rapidement. Pour ce dernier je voulais ajouter des améliorations et appliquer la nouvelle charte graphique à l'interface. Vous retrouverez d'ailleurs bientôt Phrozen VirusTotal Uploader, Phrozen Safe USB, Windows File Monitor et bien d'autres...

CETTE HISTOIRE AVEC L'UTILISATION DE DARKCOMET PAR LES PRO-EL ASSAD EN SYRIE VOUS A-T-ELLE FAIT DU TORT ? AVEZ-VOUS ÉTÉ CONTACTÉ PAR DES SERVICES SECRETS OU INQUIÉTÉ DE QUELQUE MANIÈRE QUE CE SOIT ?

Moralement cette histoire a été difficile, mais je n'ai jamais été inquiété par la justice, j'ai su réagir comme il le fallait et à temps : j'ai retiré le logiciel du site et développé un «antidote» pour aider les personnes infectées à s'en débarrasser. Concernant d'éventuels contacts avec les services secrets, je ne pourrais malheureusement rien dire à ce sujet.

ADS REVEALER ET RUNPE DETECTOR SONT DEUX LOGICIELS PERMETTANT DE DÉTECTER DES MALWARES PARTICULIÈREMENT BIEN «CACHÉS». À VOTRE CONNAISSANCE, LES ANTIVIRUS CONNUS SUR LE MARCHÉ UTILISENT-ILS CES MÉTHODES DE DÉTECTION ?

Cela dépend de l'antivirus. Mon désir n'est pas de remplacer les antivirus, mais simplement d'ajouter un contrôle supplémentaire avec des techniques qui ne sont pas forcément pensées par les concepteurs en sécurité. Certaines personnes, dont je fais partie, n'utilisons pas d'antivirus par souci de confidentialité (beaucoup d'antivirus scannent sur le cloud sans nous avertir). Ce genre de petits outils est donc parfait pour scanner de manière ciblée le comportement de certains types de malware, mais en aucun cas ne remplace un bon antivirus.

PEERIO : Un nouvel outil de COMMUNICATION CHIFFRÉE

La nouvelle loi sur le renseignement place l'enjeu la confidentialité et de la protection de ses données au devant de la scène. Découvrez ainsi Peerio, un outil qui vous permettra de tchater et d'envoyer des fichiers chiffrés.

Si vous êtes un lecteur assidu de notre magazine, vous vous souvenez probablement de Minilock et Cryptocat. Minilock est une extension Chrome qui permet d'encrypter des fichiers très facilement avant de les partager. Cryptocat, de son côté, est une application qui propose un tchat sécurisé dans lequel toutes vos communications sont chiffrées. Le rapport entre ces deux applis ? Outre le fait qu'elles soient très accessibles, gratuites et simples d'utilisation, elle ont surtout été créées par la même personne, Nadim Kobeissi.
Pourquoi vous parler de tout ça ? Tout simplement car Kobeissi a lancé un nouveau projet bien plus ambitieux actuellement en bêta : Peerio.
Pour faire simple, Peerio est un service gratuit de messagerie et de partage de fichiers sécurisés en bout-à-bout fonctionnant via leur cloud. En somme, l'enfant tant attendu de maman Minilock et papa Cryptocat. Ce logiciel est disponible sur Windows, Mac et en extension Chrome. De plus, à l'heure où nous écrivons ces lignes, Peerio est en phase de test alpha sur mobile.
Peerio cherche à se positionner sur un marché professionnel en axant son activité sur les travaux en équipe via un partage fonctionnant en cloud. Il est donc très facile d'ajouter des fichiers sur le cloud Peerio et les partager à tous ses contacts. Il n'y a cependant aucun moyen de limiter ce que les destinataires en feront : ils peuvent ainsi télécharger le fichier et le partager à leurs contacts librement.
Peerio propose néanmoins la fonction "détruire" qui efface entièrement votre fichier du cloud, il disparaîtra donc du compte de toutes les personnes à qui il a été envoyé. Gardez une chose en tête par contre : nous ne sommes pas dans Mission Impossible, le fichier sera uniquement supprimé du cloud et non pas de l'ordinateur de ceux l'ayant téléchargé. Avant que vous ne demandiez : non, il n'y a pas non plus de décompte vocal et de fumée blanche une fois la destruction effective.

COMMENT ÇA MARCHE ?

Parmi toutes les choses que Peerio fait bien, il y a une chose à retenir au niveau de la protection de vos informations : Peerio n'a aucunement accès au contenu chiffré que vous envoyez. En effet, le cryptage et décryptage sont effectués côté client, les clés sont donc entre vos mains et celles de vos contacts tout au long de la procédure et il n'est aucunement possible pour un employé malveillant de s'emparer de vos données. C'est une différence majeure qui distingue Peerio d'autres services.
Peerio fonctionne de manière simple et requiert aucun réglage de la part de l'utilisateur. L'interface est également intuitive et épurée, ainsi même votre grand-mère technophobe n'aurait pas de mal à le prendre en main. Cela peut cependant être un problème pour les utilisateurs avancés qui aiment paramétrer les choses à leur façon : il est par exemple impossible d'utiliser un autre cloud que celui de Peerio.
Nul besoin non plus de mémoriser ou de noter une clé de chiffrage étant donné qu'une nouvelle est générée à chacune de vos connexions. Sur des systèmes concurrents comme PGP, une clé privée compromise signifie que tous vos fichiers le sont aussi. Avec Peerio, ce n'est pas le cas. Cependant, la sécurité du compte dépend ainsi entièrement de votre phrase-de-passe, ou passphrase pour faire plus classe. N'ayez pas peur, avec sa longueur de 30 caractères, il faudrait plusieurs milliers de siècles avec les technologies courantes actuelles pour la cracker. . Mais si vous êtes légèrement paranoïaque, vous pouvez tout simplement modifier cette phrase régulièrement.

PAS À PAS

Comment l'utiliser de Peerio

CE QU'IL VOUS FAUT

PEERIO

OÙ LE TROUVER ? :
https://peerio.com

DIFFICULTÉ :

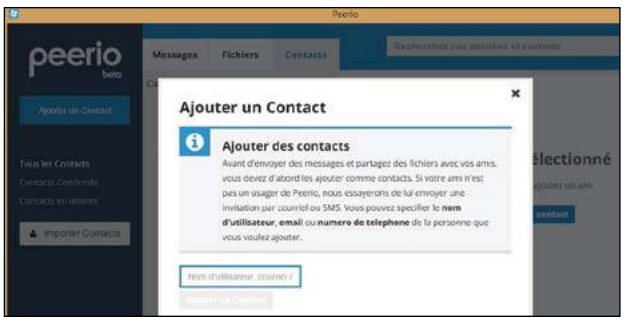
01 CRÉATION DE VOTRE COMPTE PEERIO

Téléchargez l'application et procédez à l'installation. Si vous avez choisi la langue de Maïté, ne prenez pas peur en voyant le

bouton **Abonnement**, le terme résulte probablement d'une simple traduction hasardeuse. Choisissez un nom d'utilisateur, enregistrez votre prénom, nom et e-mail et faites "continuer". Pour valider votre compte, il faudra entrer un code que vous allez recevoir par e-mail instantanément. Vous serez ensuite invité à choisir une phrase de passe.

02 AJOUTER DES CONTACTS

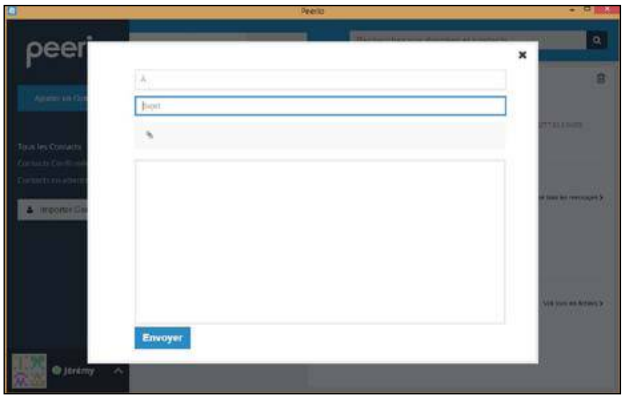
Maintenant que vous avez créé votre compte, il ne vous manque plus que les contacts. Cliquez sur **Contact** dans le menu supérieur puis **Ajouter un nouveau contact** sur la droite. Si vous connaissez des gens qui utilisent Peerio, vous pouvez entrer leur



nom d'utilisateur ou leur e-mail ou même numéro de téléphone. S'ils n'utilisent pas Peerio, ils recevront une invitation de votre part et un lien pour télécharger l'application. Vous pouvez également ajouter vos contacts Gmail en cliquant sur le bouton **Importer contacts** dans le menu de gauche.

03 ENVOYER DES MESSAGES ET DES FICHIERS

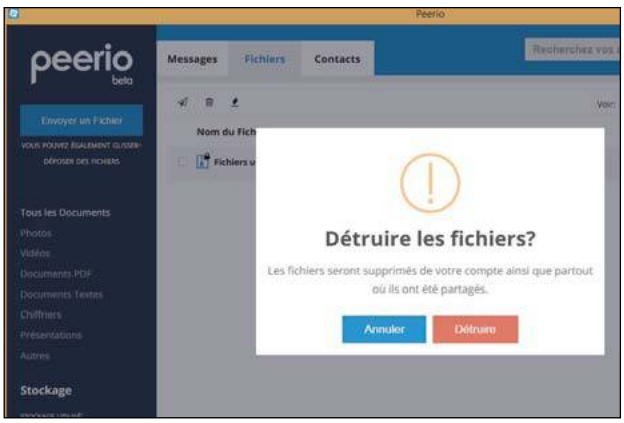
Rien de plus simple, il suffit de choisir un contact et de cliquer sur **Envoyer un message**. Cela se présente comme un e-mail avec un



sujet, un corps de texte et la possibilité d'ajouter des pièces jointes. Quand vous ajoutez un fichier, vous pouvez soit en choisir un que vous avez déjà uploadé ou en ajouter un nouveau.

04 SUPPRIMER OU DÉTRUIRE SES FICHIERS

En allant dans le menu **Fichier** en haut, vous avez accès à tout ce que vous avez ajouté et reçu sur le cloud. Vous pouvez supprimer ce que vous désirez et, si vous en êtes le propriétaire, vous pouvez détruire un fichier. Cela supprimera le fichier de votre compte mais également de celui de vos contacts et les leurs.



QUELLE ÉVOLUTION PAR RAPPORT À CRYPTOCAT ?

Cryptocat est avant tout un moyen simple de tchater en toute sécurité. Il n'y a cependant aucun gestion des contacts et il faut donc se mettre au point avec son interlocuteur par un moyen tiers avant de lancer la discussion chiffrée. Peerio est plus ambitieux, il intègre un véritable système de messagerie et d'envoi de fichiers ainsi qu'une liste de contacts.
On peut voit Cryptocat comme une tentative réussie qui a permis d'amener Peerio sur le marché du partage chiffré.

DASHLANE : LE GESTIONNAIRE DE MOTS DE PASSE PAR EXCELLENCE

Sécurisez vos sésames avec Dashlane, un gestionnaire de mots de passe qui rend la vie plus facile et votre vie numérique plus sécurisée. Plus besoin de retenir des dizaines de mots de passe, désormais un seul suffit !

S'il y a bien une chose que nous ne prenons pas à la légère chez *Pirate Informatique*, c'est la sécurité. Ainsi, si vous utilisez toujours le gestionnaire de mots de passe incorporé à votre navigateur, nous nous sentons investis d'une mission de la plus grande importance : vous faire perdre cette vilaine habitude. En effet, le gestionnaire de votre navigateur n'a absolument rien de sécurisé. Il suffit d'accéder à votre ordinateur ou même à votre compte, aller dans les options et afficher les mots de passe. Rien de plus facile pour quelqu'un de mal intentionné qui ne se générera pas pour vous remercier de lui avoir mâché le travail. Dashlane est un gestionnaire de mots de passe et un portefeuille numérique qui adopte une méthode de chiffrement en AES-256. Sachez également que Dashlane n'a aucunement accès à vos informations. Toutes vos données, même si vous décidez de les stocker sur le cloud, sont chiffrées localement et nécessitent votre mot de passe maître, sésame que vous seul possédez.

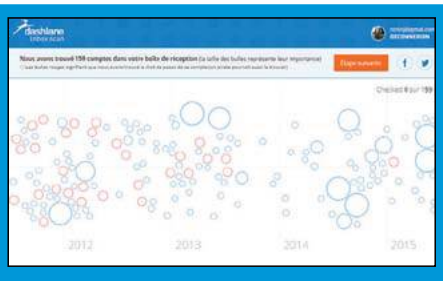
SIMPLICITÉ D'UTILISATION POUR UNE SÉCURITÉ PERFORMANTE

Dashlane s'impose comme un compagnon de choix pour sécuriser vos mots de passe et surtout, s'assurer d'en utiliser des différents et efficaces sur chacun de vos comptes sur la toile. Par ailleurs, le logiciel permet également de stocker vos informations personnelles pour remplir les formulaires et de gérer vos moyens de payement pour effectuer vos commandes en quelques clics. Vous pouvez même synchroniser différents appareils pour y avoir accès sur chacun d'entre eux, mais cela nécessite l'achat d'un abonnement Premium. Un mois vous est cependant offert lors de votre inscription.

VOS E-MAILS, LE TALON D'ACHILLE DE LA SÉCURITÉ

Il n'est pas rare que de nombreux services vous envoient vos identifiants après votre inscription sur leur site. Le problème c'est que n'importe quel petit fripon ayant accès à vos e-mails aura également accès à tous vos autres comptes. Pour répondre à cette problématique, Dashlane propose Dashlane Inbox Scan, une application qui accède à votre boîte mail pour détecter et analyser les vulnérabilités. Une fois l'analyse effectuée, vous obtenez un rapport confidentiel renseignant votre niveau de sécurité. Restez donc bien accroché à votre siège, ça risque de secouer...

Lien : **www.dashlane.com/scan/11**



Optimisez Dashlane avec ces fonctionnalités

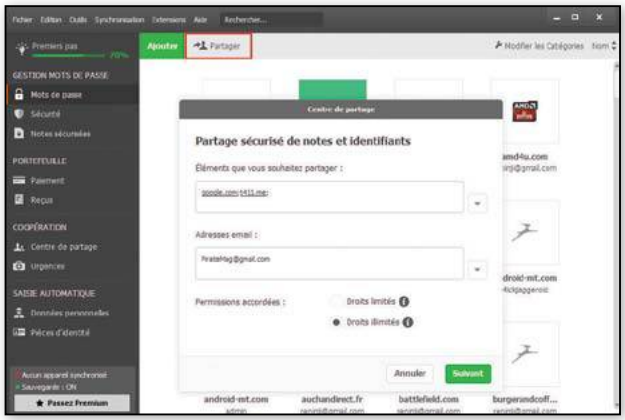
CE QU'IL VOUS FAUT

DASHLANE

OÙ LE TROUVER ? :
www.dashlane.com

DIFFICULTÉ :

01 PARTAGER DES MOTS DE PASSE



Dashlane vous permet de partager des identifiants avec vos contacts. Pour cela, cliquez sur le bouton **Partager** du logiciel, sélectionnez l'élément souhaité dans le premier champ puis l'adresse e-mail de votre contact dans le second. Définissez les droits et cliquez sur suivant. Laissez un gentil message puis cliquez sur **Envoyer**. Sachez que votre contact doit lui aussi utiliser Dashlane.

02 CONFIGURER LA SAISIE AUTOMATIQUE

Sur Dashlane, rendez-vous dans **Données personnelles** sous **Saisie Automatique**. Vous pouvez ici renseigner vos informations personnelles comme votre nom, votre e-mail, ou encore votre adresse. Quand un site vous demande vos informations, cliquer sur un champ ouvre un pop-up Dashlane. Choisissez l'information adéquate et, si indisponible, entrez-la pour la stocker sur Dashlane.

03 SYNCHRONISATION SUR PLUSIEURS APPAREILS

La synchronisation se fait automatiquement toutes les 5 minutes. Pour cela, il suffit d'avoir un compte Premium actif et de s'être connecté avec le même compte Dashlane sur les différents appareils. Pour accéder aux préférences, allez dans le menu **Synchronisation**. Vous pouvez ici faire une synchronisation manuelle ou, si vous le souhaitez, la désactiver.

04 OPTIMISER LA SÉCURITÉ DE SES COMPTES

Dans le menu **Sécurité**, vous pouvez voir le niveau de sécurité de vos différents comptes. Dashlane met en avant les plus fragiles et vous redirige vers les sites en question pour les changer. Dans **Outils > Préférences > Sécurité**, vous pouvez modifier la sécurité de votre compte et ajouter notamment une déconnexion automatique après inactivité ou la double identification.

QUELLE DIFFÉRENCE ENTRE LA VERSION GRATUITE ET PREMIUM ?

Dashlane Premium propose des fonctionnalités supplémentaires pour 39,99€ par mois. Parmi celles-ci nous notons principalement la synchronisation sur plusieurs appareils, le partage illimité d'identifiants, la sauvegarde du compte sur le cloud et la consultation des identifiants directement depuis le site (très pratique si vous n'avez aucun de vos appareils sous la main!). Des fonctionnalités très utiles, mais pas non plus obligatoires pour tirer parti de Dashlane.

TRUPAX : LE CHIFFREMENT SUR MESURE

Dans le précédent numéro, nous vous avions parlé de VeraCrypt, une sorte de successeur de TrueCrypt à la française. TruPax fonctionne différemment : au lieu de créer un espace défini où vous mettriez vos fichiers sensibles, TruPax ajuste la taille du conteneur au fichier que vous voulez chiffrer. La sécurité sans prise de tête !

LEXIQUE

***VOLUME :**
Il s'agit d'une partition ou d'une partie de partition. Un espace de stockage défini qui peut être chiffré. TruPax permet de créer des fichiers chiffrés sans auparavant créer de volume dédié. Le fichier devient instantanément un volume chiffré.

Les dernières versions de TrueCrypt n'étant pas sûr (n'utilisez pas TC après la 7.1a) et VeraCrypt ne permettant pas de faire des conteneurs sur mesure, nous vous présentons ce mois-ci TruPax (TP). Contrairement à ce que l'on pourrait penser, ce logiciel n'est pas basé sur le code de TC mais ils sont compatibles. À condition d'être formaté en FAT32, un conteneur TC pourra être monté dans TP. Dans l'autre sens, il n'y a pas de restrictions.

UN CONTENEUR CHIFFRÉ À LA DEMANDE

Alors pourquoi utiliser TP ? Avec TC, l'espace chiffré que vous avez créé est fixe. S'il devient trop réduit, il faudra tout refaire. Pas très pratique pour envoyer des fichiers chiffrés sur le cloud ou à un ami. TP propose de chiffrer un fichier ou un dossier à la demande. Chaque élément sera considéré comme un conteneur à part entière. Plus besoin de créer des volumes chiffrés trop grands de peur de manquer de place un jour. Pas de problème d'interopérabilité puisque les conteneurs sont formatés en UDF, un système de fichier qui peut être exporté sur plusieurs OS. Bien sûr, les sources sont disponibles et il est possible d'utiliser TP dans vos propres applications.

Chiffrez vos données facilement

CE QU'IL VOUS FAUT

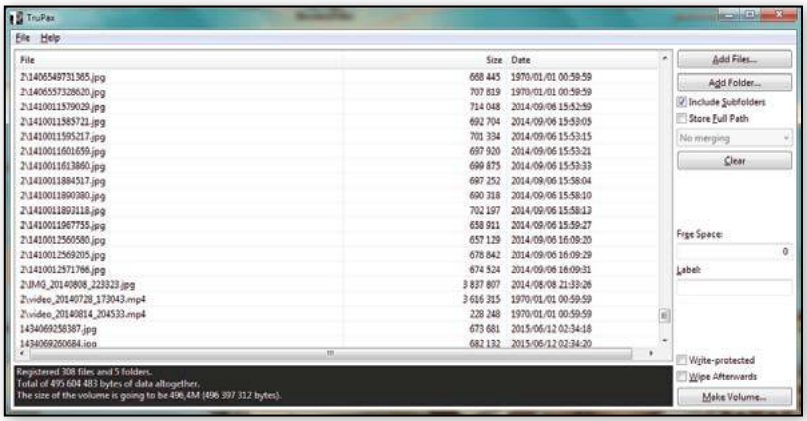
TRUPAX

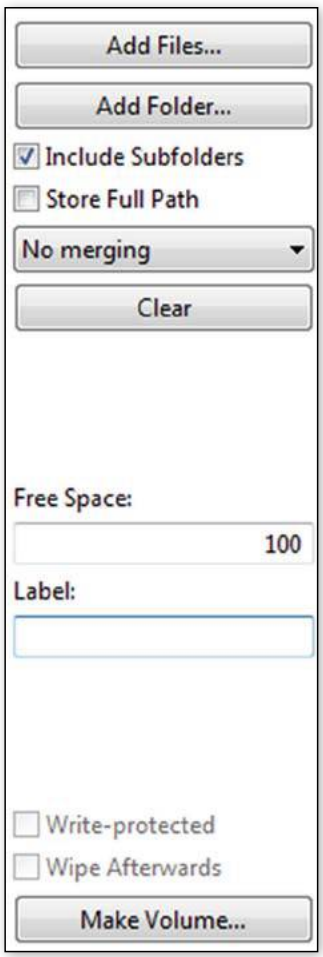
OÙ LE TROUVER ? :
www.coderslagoon.com

DIFFICULTÉ :

01 L'INTERFACE

Téléchargez la version adéquate pour votre ordinateur Windows (celle sur le CD correspondant à la version 64 bits) et dézippez l'archive. Pour afficher l'interface graphique, lancez trupaxgui.exe et choisissez la langue anglaise. Notons que TruPax ne nécessite pas d'installation, il est donc possible de placer le programme sur une clé USB. Pour commencer, il suffit de faire un glisser-déposer des éléments à chiffrer dans la fenêtre principale ou de cliquer sur **Add Files...** ou **Add Folder...** Si vous voulez intégrer les sous-répertoires, il faudra laisser la case **Include Subfolders** cochée.



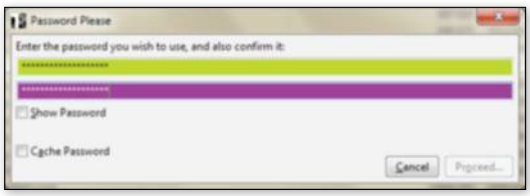


02 LES OPTIONS...

Dans le menu déroulant, **No Merging** signifie que les éléments ne seront pas combinés lors du chiffrement (dans le cas où les noms des dossiers seraient les mêmes par exemple) et **Free space** permet de garder un peu de place pour ajouter des fichiers ou pour des mises à jour. En bas, vous aurez un résumé des opérations futures: taille totale des fichiers avant et après le chiffrement. Notez qu'en bas à droite, vous pourrez cocher **Wipe Afterwards** pour effacer les éléments qui auront été chiffrés dans leur répertoire d'origine.

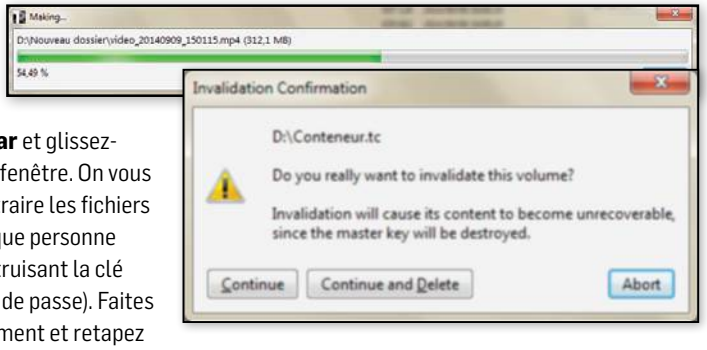
03 LA CRÉATION DU VOLUME

Lorsque tout est près, faites **Make Volume...** Choisissez un nom à votre conteneur et spécifiez un mot de passe. Il est possible de mettre le mot de passe en cache pour ne pas avoir à le retaper sur votre machine (attention, il faut être sûr que personne d'autre n'a accès à votre PC) et surtout garder le mot de passe en cas de panne. Votre conteneur TrueCrypt au format **.tc** ajusté pile-poil à la taille de vos fichiers est prêt à l'endroit spécifié. L'opération est très rapide: 16 secondes pour près de 500 Mo de données.



04 LE DÉCHIFFREMENT

Vous pouvez alors l'envoyer à un ami ou le stocker où vous le désirez. Pour pouvoir avoir à nouveau accès aux fichiers, faites **Clear** et glissez-déposez le fichier **.tc** dans la fenêtre. On vous demandera si vous voulez extraire les fichiers ou invalider le volume (pour que personne ne puisse y avoir accès en détruisant la clé dans le cas d'un oubli de mot de passe). Faites **Extract**, spécifiez l'emplacement et retapez votre mot de passe. Faites ensuite **Proceed** pour décrypter vos fichiers. Dans TC ou VeraCrypt il faudra «monter» le volume pour le déchiffrer.



LES RANSOMWARES :

QUAND VOS DONNÉES SONT PRISES EN OTAGE

C'est le nouvel Eldorado des petits malins qui veulent se faire de l'argent facilement. Les ransomwares (ou «rançongiciels» dans la langue de Lorie) prennent en otage vos données en les bloquant ou en les chiffrant. Pour récupérer vos précieux fichiers, il faudra payer les méchants. Faisons le point sur cette menace pas si récente..

On en entend parler depuis l'année dernière, mais le concept de ransomware n'est pas nouveau. Le premier du genre date en effet de 1989, mais il faudra attendre 1996 pour voir arriver le premier ransomware «moderne» avec une paire de clés asymétriques. Tout commence par un malware de type «ver» qui va charger un programme malicieux. Ce dernier 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 (RSA 2048 bits). Au bout de quelques minutes, vos fichiers les plus sensibles 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. Bien sûr le moyen de paiement est discret : Paypal, Bitcoin, uKash, etc. N'espérez pas envoyer un chèque. 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.

LES DIFFÉRENTES APPROCHES

Il existe en effet plusieurs approches intéressantes. Certains ransomwares vont saturer votre écran d'images pornos pour vous faire payer. Les utilisateurs passent alors à la caisse pour éviter d'être pris pour des pervers. D'autres vont interdire l'accès à Windows (il faudra alors appeler un numéro surtaxé pour obtenir un protocole de désinfection), vous faire peur ou culpabiliser pour vous faire passer à la caisse. Les ransomwares n'hésitent pas à se faire passer pour la police ou pour une organisation gouvernementale ! Sur la fenêtre d'avertissement, vous pourrez voir le logo de la police de votre pays et un message qui vous expliquera qu'un pirate a utilisé votre PC pour télécharger des images pédopornographiques ou vous avertir que vous avez téléchargé des films illégalement et qu'il faut payer une amende. La plupart du temps, les gens payent de peur de finir devant les tribunaux.

Voilà ce que vous ne voulez pas voir sur votre écran: «*Vos documents ont été chiffrés avec une clé publique RSA 2048 bits. Vous avez 72 heures pour nous payer 300 € ou nous effacerons la clé privée.*»

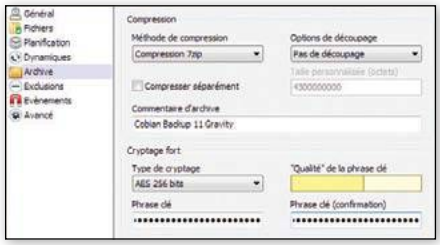
LEXIQUE

*** ANALYSE HEURISTIQUE :** À l'inverse de l'analyse par signature qui va détecter si un fichier malicieux est déjà connu par comparaison, l'analyse heuristique va étudier le comportement d'un fichier. De nos jours les antivirus disposent des deux types de protection.

PAS À PAS

Évitez les problèmes liés à un ransomware

01 FAITES DES SAUVEGARDES RÉGULIÈRES



Nous avons vu que les ransomwares ciblent les fichiers qui vous sont chers (photos, document texte, PDF ou fichiers de jeux). Le plus simple est donc de faire des sauvegardes régulières sur un disque dur externe déconnecté du PC en temps normal. Les logiciels gratuits Cobian Backup (*Pirate Informatique* n°18) ou EaseUS Todo Backup (n°13) s'acquitteront très bien de cette tâche... Pour plus de confort, et à moins d'avoir un disque dur suffisamment gros, on peut aussi faire un clone de son système avec XXClone (n°23).

02 UN ANTIVIRUS MIS À JOUR

Pas besoin de passer à la caisse pour disposer d'une protection antivirus résidente. Les ransomwares attaquent souvent avec un simple fichier EXE contenu dans un ZIP. Des antivirus gratuits comme Avast, Avira Free ou AVG mettront le fichier en quarantaine dès qu'il bougera une oreille. Il faudra tout de même être sûr de renouveler votre licence et de mettre à jour la base de données virale. Et même si vous n'avez pas de chance et que le ransomware n'est pas connu de la base de données au moment de l'infection, la protection heuristique n'en fera qu'une bouchée.

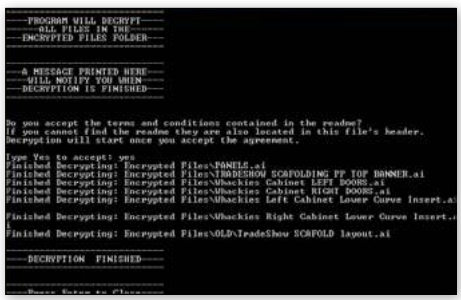
03 PRÉVENIR ET GUÉRIR

Avant toute infection vous pouvez «vacciner» votre PC avec CryptoPrevent (**https://goo.gl/NhPRaS**), mais s'il est déjà trop tard, déconnectez votre machine d'Internet, quitte à débrancher la box. Vous pouvez tenter une désinfection avec votre antivirus ou MalwareBytes (aussi très bon contre les roguewares). Pour connaître l'étendue des dégâts, vous pouvez utiliser CryptoLocker Scan Tool (**http://goo.gl/dwylum**) qui vous dira quels fichiers ont été chiffrés (attention, il ne fonctionne pas pour toutes les variantes).

04 NE PAS PAYER !

Si vous êtes infecté, que vous n'avez pas de sauvegarde et que tout espoir semble perdu, ne payez pas les ravisseurs ! Des victimes ont rapporté que, même après un paiement dans le temps imparti, la clé de déchiffrement envoyée par les pirates n'a pas fonctionné ! Faites une recherche sur Internet car avec un peu de chance votre ransomware n'est pas très sophistiqué : certains fonctionnent en fait avec la même clé de chiffrement pour toutes les victimes. Vous pourriez donc récupérer vos données avec la clé d'une victime qui a déjà payé ! Le site Ransomware Decryptor (**https://noransom.kaspersky.com**) contient des clés privées saisies lors de descentes de police chez les méchants... Pourquoi ne pas essayer?

05 UN DERNIER ESPOIR



Si vous êtes infecté, que vous n'avez pas de sauvegarde et que Si vous pensez que tout est perdu, il reste encore quelques pistes pour garder l'espoir.

Le site Malware Tips dispose d'une section entière sur les ransomwares et propose des protocoles de désinfections: **http://goo.gl/2Ui34z**. Si, une fois désinfecté, vous n'avez pas eu d'autre choix que de payer la rançon, il arrive que certains fichiers ne soient pas correctement déchiffrés (clé de registre obsolète, etc.) La solution consiste alors à les déchiffrer «à la main» avec Crypto-un-Locker (**https://goo.gl/Cmr8Ju**), un script Python qui détectera et déchiffrera les fichiers récalcitrants.

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.

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

Actuellement #Guide pratique

100% HACKING & SMARTPHONES

QWANT, UNE ALTERNATIVE À GOOGLE

Il ne se passe pas une semaine sans qu'une start-up ne se lance dans un combat perdu d'avance contre des géants du Web. Le français Qwant ne cherche pas à contrer Google, mais à proposer une alternative au moteur de recherche numéro 1. Pour cela, il mise sur une interface innovante et met l'accent sur le respect de la vie privée...

LEXIQUE

***TRACKING :**
Ensemble de procédés permettant à un logiciel ou un site de cerner un profil type de consommateur en fonction des sites visités ou des informations saisies dans des formulaires (centres d'intérêt) à partir duquel des sociétés vont pouvoir cibler de la pub personnalisée.

***API :**
Application Program Interface ou Interface de programmation désigne un logiciel ou un service utilisé par d'autres logiciels ou services. Par exemple l'API Google Maps est utilisé par beaucoup d'autres sites pour proposer des cartes sans avoir à développer de solution interne.

Nous vous avions déjà parlé de DuckDuckGo (*Pirate Informatique* n°16 et *Dossier du Pirate* n°3), ce moteur de recherche, qui fait la guerre au tracking propose des résultats de recherche en respectant votre vie privée. Mais il utilise malheureusement les API de Google : vos recherches et données personnelles sont à l'abri, mais les résultats sont les mêmes que si vous utilisiez Google avec les « mises en avant maison » que l'on connaît. Vous vous retrouvez donc avec des liens triés par Mountain View. Dans notre précédent numéro, nous avons vu comment limiter les intrusions de Google dans votre vie privée, mais pourquoi ne pas carrément s'en passer ?

QWANT, LE PLAN B

Qwant ne se place pas comme un concurrent de Google, mais plutôt comme une alternative. Les incursions du moteur dans votre ordinateur se limitent à un cookie de session permettant de retrouver vos préférences de navigation lors de la prochaine connexion. Qwant ne mémorise pas vos recherches, ne fouille pas votre historique et ne vous propose pas des liens sponsorisés ou des liens commerciaux à chaque recherche. Le moteur vit grâce aux produits que vous achetez par son biais, mais il ne vous bombardera pas de liens pourris à chaque utilisation. Ce qui peut choquer les utilisateurs habitués à l'interface épurée de Google c'est la quantité d'éléments qui apparaît à l'écran lors d'une recherche. Il est certes possible de faire le ménage (votre plus loin), mais lors de votre première recherche, vous aurez des images et des vidéos en haut, des liens sur la gauche, des actus et Wikipédia au milieu, des résultats issus de réseaux sociaux sur la droite et le tout sur une seule page. Contrairement à Google, si Qwant pense que les résultats sont peu pertinents, il ne les affichera pas. Vous mettez souvent le nez dans la page n°2 de Google vous ? Nous non plus... Les « carnets » permettent de personnaliser votre interface et d'ajouter des éléments par thème. Pratique pour classer les résultats sur un sujet particulier et reprendre une recherche passée.
En ce qui concerne la qualité des résultats, nous avons été surpris. Qu'il s'agisse de requêtes simples (*PSG*), maladroites (« *Comment ouvrir un script sous Linux* ») ou avec des inclusions/exclusions (*+foire +Rouen -vin*), le moteur répond sans problème et pendant notre phase de test nous n'avons jamais été tentés de revenir vers Google... à part pour les cartes. Mission accomplie ?

PAS À PAS

Comment fonctionne Qwant ?

CE QU'IL VOUS FAUT

QWANT

OÙ LE TROUVER ? :
www.qwant.com

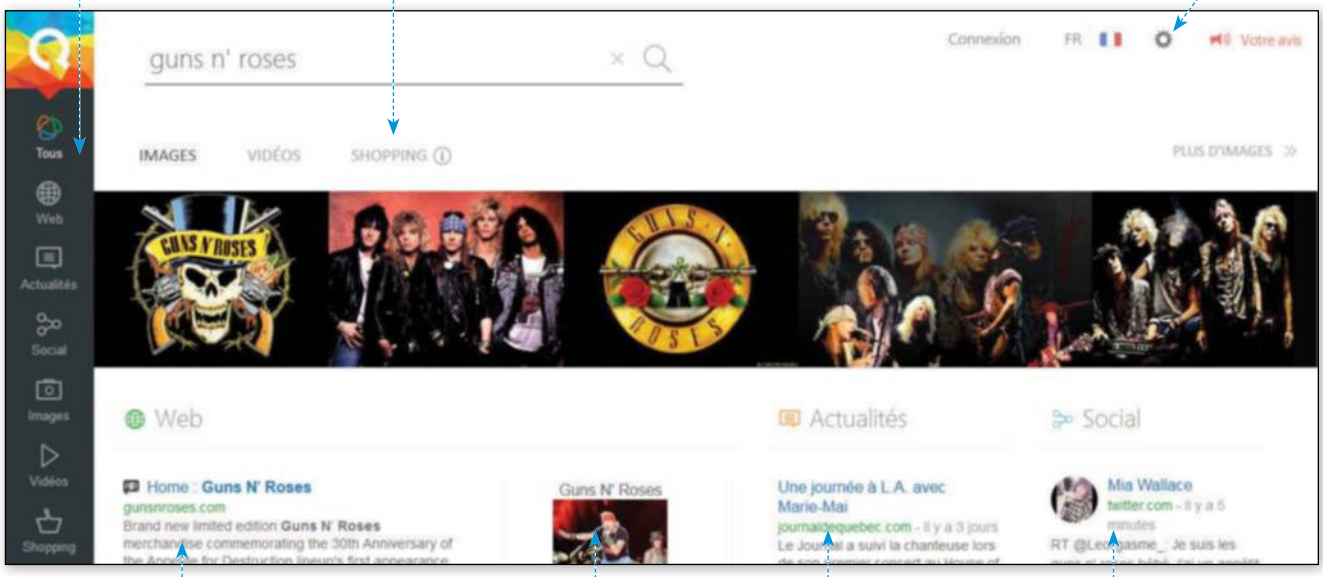
DIFFICULTÉ :

01 L'INTERFACE

Cliquez sur l'engrenage pour avoir accès aux Réglages : filtre contenu adulte, tendances du jour, suggestion de recherche, etc.

Onglets de recherches spécifiques

Bandeau multimédia. Notez que la recherche **Shopping** n'est pas particulièrement mise en avant



Résultats Web

Wikipédia

Actualités

Réseaux sociaux

02 QWANT À TOUS LES ÉTAGES !

Vous voulez passer à Qwant sur tus vos appareils, mais vous ne savez pas comment paramétrer le moteur de recherche par défaut? Pas de problème, il suffit de suivre ce lien : **https://goo.gl/eEOkXK**. Vous aurez toutes les marches à suivre que vous soyez sur Firefox, IE, Chrome, Safari ou Opera.

TRAQUE SUR INTERNET

Google vous connaît bien et vous connaît mieux à chaque recherche : les mots que vous saisissez sur son moteur de recherche, votre adresse IP, l'endroit où vous vivez, les liens sur lesquels vous cliquez, etc. Pour Google, qui tire la majeure partie de ses revenus grâce aux pubs qu'elle vend via son système AdWords, les recherches sur son moteur valent de l'or. Ne vous étonnez pas de voir des publicités pour des jouets Star Wars sur une page quelconque si vous venez de passer l'après-midi à chercher le nom de famille de la princesse Leia ou la planète d'origine de Chewbacca. En effaçant tous vos cookies et en passant à Qwant vous n'aurez plus jamais l'impression d'être fliqué !

E-MAILS SÉCURISÉS: PENSEZ À LAVABOOM

Chez *Pirate Informatique*, nous n'avons pas attendu les révélations d'Edward Snowden pour vous conseiller d'être prudent. Car il n'y a pas que les services secrets qui vous espionnent : Gmail et Yahoo balayent votre courrier pour vous inonder de publicités ciblées. Pensez à Lavaboom !

Les gouvernements brandissent sans hésiter le spectre du terrorisme ou de la pédophilie lorsqu'il s'agit de s'attaquer à la vie privée. C'est ainsi que des projets de webmails chiffrés comme Lavabit (voir encadré) sont morts avant d'avoir eu le temps de se faire un nom. Heureusement, après Tutanota (voir *Pirate Informatique n°* 23) voici qu'arrive Lavaboom.

CHIFFREMENT LOCAL ET ASYMÉTRIQUE

Ce service basé en Allemagne propose gratuitement 1 Go de stockage avec une authentification en 2 étapes, mais surtout un chiffrement de bout-à-bout. Lors de la création de votre compte, un duo clé publique/clé privée sera généré. Si vous voulez utiliser une autre machine ou un autre navigateur, il faudra importer ce trousseau de clés. Ce dernier est un simple fichier au format .json qui contient en fait deux clés PGP lorsqu'on l'ouvre avec un éditeur de texte. Lavaboom ne stocke pas de mots de passe : impossible de réinitialiser un compte, mais aussi impossible pour les employés d'ouvrir votre correspondance, même sous la torture ! Le seul moyen pour un pirate d'accéder à votre compte sera de vous voler ce fichier .json avec un malware ou en ayant accès à votre machine. Pour les accros du smartphone, Lavaboom prépare des applis, mais il est tout à fait possible de se connecter au service en utilisant son navigateur. Notons aussi que Lavaboom peut fonctionner de concert avec la Yubikey, une clé USB permettant d'authentifier des sessions que nous testerons dans le prochain numéro.

LEXIQUE

*** CHIFFREMENT DE BOUT-À-BOUT :** Les messages que vous envoyez sont chiffrés sur votre PC avant même d'être envoyés sur Internet. Le site ne fait rien d'autre que relayer le message chiffré et c'est le destinataire qui le déchiffre. Une interception du message par un tiers ne permet donc pas de corrompre la correspondance.

LES WEBMAILS CHIFFRÉS SONT DANS L'ŒIL DU CYCLONE

Lancé en 2004, Lavabit a fermé ses portes en 2013 dans des conditions dramatiques. En fait, le directeur Ladar Levison n'a jamais pu expliquer pourquoi il avait la boutique, mais le message qu'il a laissé sur son site laisse à penser qu'il a du choisir entre saborder son projet ou trahir la confiance de ses utilisateurs. Car aux États-Unis, lorsque la NSA vous demande des renseignements, vous n'avez pas le droit de dire non et surtout vous n'avez pas le droit d'en parler ! Si l'on considère que Edward Snowden utilisait son compte Lavabit au moment où il était coincé à l'aéroport de Moscou en juillet 2013 et que Levinson a fermé en août, il n'y a pas besoin de s'appeler Colombo pour comprendre ce qui s'est passé... Hasard du calendrier (ou pas), Silent Circle le webmail créé par Philip Zimmermann (l'inventeur de PGP) a fermé au même moment.

Introduction à Lavaboom

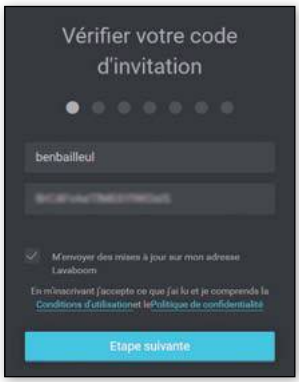
CE QU'IL VOUS FAUT

LAVABOOM

OÙ LE TROUVER ? :
https://lavaboom.com

DIFFICULTÉ :

01 DEVENEZ BÊTA TESTEUR !



Sur le site il faudra cliquer dans **Reserve username** et choisir son nom d'utilisateur. Lavaboom vous recontactera sur votre e-mail habituel pour vous inviter avec un code d'authentification unique pour éviter que quelqu'un n'usurpe votre identité. Renseignez les champs concernant votre nom. Cette étape est obligatoire même si le service met l'accent sur le côté légal de la chose.

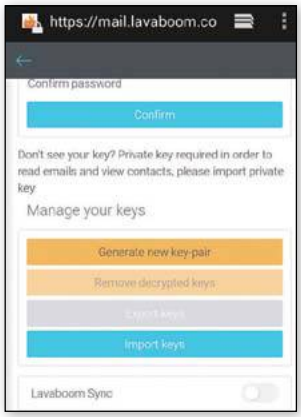
02 PREMIÈRE AUTHENTIFICATION

Personne ne vérifiera ces données et elles ne seront pas intégrées à vos e-mails. Le choix du mot de passe est primordial. Comme d'habitude, alternez les types de caractères alphanumériques. En cas de perte de ce sésame, vous perdrez tout ! Vous pouvez laisser votre navigateur se souvenir de ce mot de passe puisqu'il existe une deuxième authentification.

03 DEUXIÈME AUTHENTIFICATION

Cliquez ensuite sur **Générer mes clés**. La clé privée ne doit jamais être donnée, car c'est celle qui servira à chiffrer les messages envoyés à une personne dont vous possédez la clé publique. Votre clé publique, elle, servira à d'autres pour vous envoyer des messages chiffrés. Rassurez-vous, pour les utilisateurs de Lavaboom, ces étapes sont complètement transparentes. Sur l'écran suivant, faites **Sauvegarder ma clé** et mettez là en lieu sûr. Cette étape n'est pas nécessaire si vous utilisez uniquement l'ordinateur sur lequel vous avez créé le compte.

04 VOTRE TROUSSEAU DE CLÉS



Dans le cas contraire, sauvez ce fichier .json dans un conteneur chiffré ou une clé USB bien cachée car si vous voulez vous connecter depuis un autre PC ou un smartphone vous en aurez besoin. Dans **Paramètres>Sécurité**, faites **Importer des clés**. Car sans ces clés vous ne pourrez pas accéder à vos e-mails, même avec votre mot de passe de compétition !

05 ATTENTION !

Ensuite, vous pourrez constater que l'interface de Lavaboom n'a rien de complexe : boîte de réception, indésirables, corbeille, etc. Attention si vous envoyez un e-mail à quelqu'un qui n'a pas de solution chiffrée (PGP, GnuPG, Tutanota, gAES, etc.) ce que vous direz peut être visible: adresse, nom, etc. Par contre un pirate/espion ne pourra pas lire vos autres e-mails depuis votre compte Lavaboom. Vous saurez si la conversation est complètement sûre en regardant le petit cadenas en dessous de l'heure d'envoi du mail.

LA VERSION PAYANTE ?

La version pour les bêta-testeurs est limitée à 1 Go de stockage (qui descendra à 500 Mo plus tard donc dépêchez-vous!), mais ceux qui ne peuvent pas se contenter de cela pourront aussi passer à la caisse. La version Premium proposera 15 Go avec une authentification en 3 étapes et la personnalisation du nom de domaine. Rien n'a encore filtré sur le prix du service, on sait juste que l'on pourra payer par Bitcoin pour brouiller encore plus les pistes.

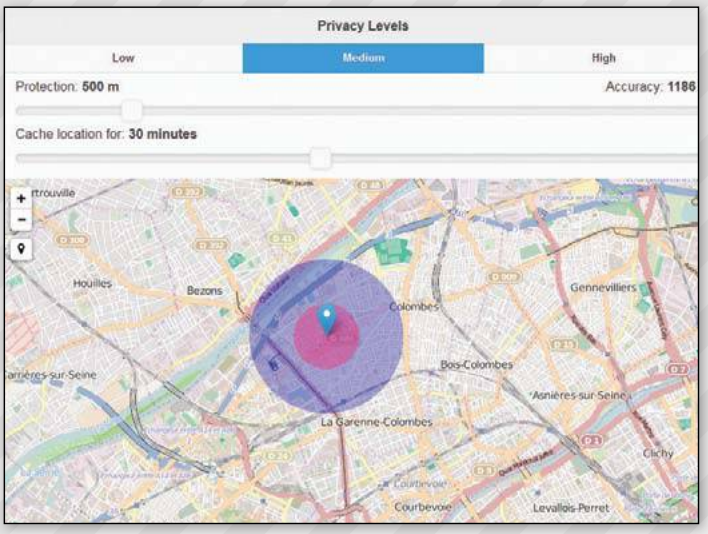
#1 Gardez secret l'endroit d'où vous vous connectez

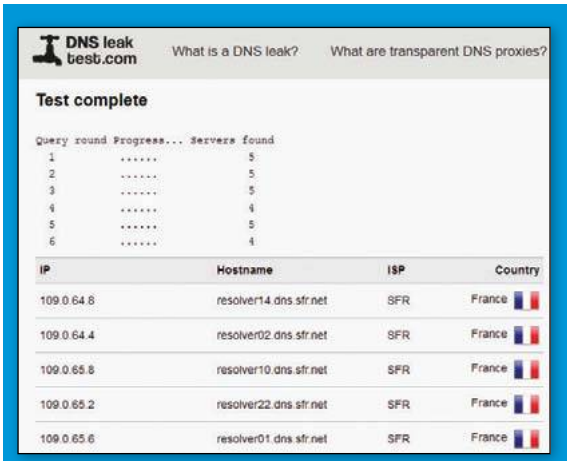
AVEC LOCATION GUARD

Même si vous n'utilisez pas de VPN ou de solution d'anonymat, vous n'avez pas forcément envie que les sites sur lesquels vous vous connectez sachent où vous vous trouvez. En effet certains sites vous demandent souvent de partager votre location. Par exemple le site 20minutes.fr utilise cette fonction pour vous afficher en priorité des infos sur Lyon si vous êtes lyonnais, etc. L'extension Location Guard vous permet d'éviter d'avoir à refuser cette collecte d'informations en paramétrant pour chaque site un refus total de partager votre localisation, une localisation fantaisiste ou aléatoire.

Lien: **https://goo.gl/PHSVLf** (Firefox)

Lien : **https://goo.gl/TvGwdU** (Chrome)





#2 Un VPN bien étanche

AVEC DNS LEAK TEST

Il n'y a pas que le protocole WebRTC qui peut éventuellement poser des problèmes à votre VPN. Avez-vous déjà entendu parler des fuites de DNS ? Il s'agit en fait de l'envoi accidentel de paquet d'information utilisant le DNS de votre FAI au lieu de celui que vous utilisez normalement avec votre service de VPN. En clair, il est parfois possible, même avec un VPN, de ne pas être à 100% protégé. Lancez un test sur le site DNS Leak et si les serveurs qui s'afficheront ne sont pas ceux de votre VPN (comme sur notre capture), alors vous êtes potentiellement vulnérable ! Nous verrons comment le régler dans le prochain numéro si vous êtes suffisamment nombreux à nous le demander...

Lien : **www.dnsleaktest.com**

#3 Contourner les géolocalisations

AVEC ZAPYO

Zapyo est une extension pour Firefox, Chrome et Opera permettant de contourner les géolocalisations des sites. Il vous autorise par exemple à accéder à des Web TV, site de stream ou webradios qui ne sont pas disponibles en France pour des histoires de propriété intellectuelle. À l'inverse, des expatriés Français peuvent accéder de l'étranger à des sites «bien de chez nous»: 6play, Pluzz, etc. Attention, il n'est pas question d'anonymat, mais juste de vous localiser quelque temps dans un pays donné. Sur le site, faites **Get Zapyo Now** et acceptez l'installation sur votre navigateur et inscrivez-vous. Le site vous montrera des services populaires et vous pourrez filtrer par pays

Lien: **https://zapyo.com**

#4 Un (autre) webmail chiffré

AVEC PROTONMAIL

À la page 26 nous avons réalisé un article sur Lavaboom, un webmail chiffré très convivial. Nous aurions aussi pu faire un article complet sur son concurrent Protonmail, mais l'invitation est arrivée quelques jours après celle de Lavaboom... Au niveau technique c'est presque un copier-coller: chiffrement bout-à-bout, double vérification (mot de passe + paire de clés), etc. Comme pour son concurrent, il faudra attendre pour les versions mobiles, mais il est possible de s'y connecter depuis son navigateur. Faites votre demande d'invitation sur le site (**Request an invite**).

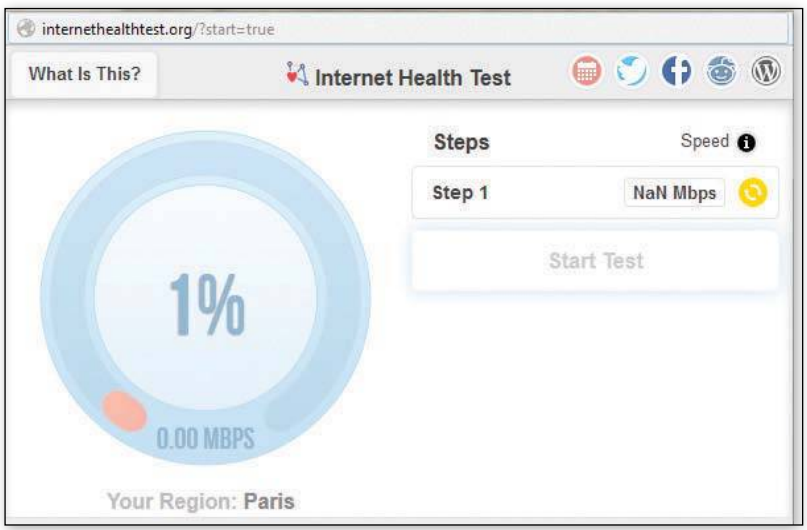
Lien : **https://protonmail.ch/login**

#5 Vérifiez votre connexion

AVEC THE INTERNET HEALTH TEST

Vous avez des doutes concernant votre connexion ? Des disparités entre votre débit théorique et la vitesse réelle de votre connexion ? Vous êtes à l'étranger et vous avez peur d'être une victime de «l'Internet à deux vitesses» ? Sans nécessiter d'installation, Internet Health Test va lancer un diagnostic sur votre PC pour déterminer si votre connexion est bridée. Le service réalise des tests de vitesse sur plusieurs serveurs et les compare aux internautes de votre région géographique.

Lien : **www.battleforthenet.com/internethealthtest**



#6 Évitez les e-mails «trackés»

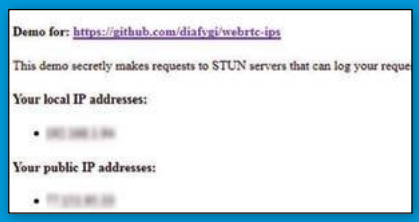
AVEC AVEC UGLYMAIL

Disponible pour Chrome et bientôt pour Firefox, Uglymail permet de savoir avant l'ouverture d'un e-mail si ce dernier sera utilisé pour vous tracker. En effet certaines compagnies et certains réseaux sociaux intègrent des moyens de surveillance à leurs e-mails : heure d'ouverture, navigateur utilisé, nombre de clics dans le corps du message, etc. Par exemple, si vous êtes abonnés à la mailing-list de Pirate Informatique, sachez que la société qui gère ce service utilisera un tracker pour savoir si vous avez bien ouvert l'e-mail (cela nous permet de savoir si ces derniers ne tombent pas trop souvent dans la boîte de spam). Rien de bien méchant ici, mais si cette collecte de données vous gêne, Uglymail vous permettra de passer entre les gouttes. N'ouvrez pas les e-mails où s'affiche un petit oeil noir dans votre boîte de réception...

Lien : **http://goo.gl/A78FE8**

#7 Vérifiez votre anonymat

AVEC WEBRTC-IPS



Même bien caché derrière Tor, Freenet, un proxy anonyme ou un VPN, il n'existe pas d'anonymat 100% sûr. Dernièrement une faille a été découverte dans le protocole WebRTC utilisé pour la communication en temps réel. Grâce à cette faille, un pirate, un gouvernement ou un site peut retrouver votre véritable IP. Faites le test ! Allez sur le site ci-dessous alors que vous utilisez votre solution d'anonymat. Si votre véritable IP apparaît, c'est que vous êtes vulnérable ! La parade consiste à désactiver le WebRTC de vos navigateurs en utilisant l'extension Disable WebRTC sur Firefox ou ScriptSafe sur Chrome.

Lien : **https://diafygi.github.io/webrtc-ips**

Merci à Korben.info !

DÉBLOQUEZ N'IMPORTE QUEL PDF

-PARTIE 2-

Dans le précédent numéro de *Pirate Informatique* nous avons vu les différentes protections d'un fichier PDF : mot de passe d'autorisation et mot de passe d'ouverture. Le premier pose rarement problème alors que le second est beaucoup plus difficile à cracker. Nous avons néanmoins quelques solutions...

LEXIQUE

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

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

Le mot de passe d'ouverture (user password) d'un fichier PDF va, comme son nom l'indique, interdire l'ouverture d'un document, mais l'opération va en plus chiffrer le fichier avec l'algorithme RC4 128 bits. Pas de contournement possible ici, il faudra traiter ce mot de passe avec un des deux techniques que nous avons abordé dans nos articles sur John The Ripper : l'attaque par dictionnaire. Il s'agit en fait d'essayer le plus de mots possible afin de trouver le bon. Pour cela il faut un logiciel et une liste de mots dans lequel il ira piocher. Il est possible de trouver ce type de liste sur Internet dans plusieurs langues et avec plusieurs types de caractère.

ATTAQUE PAR DICTIONNAIRE

PDFCrack est un logiciel destiné à fonctionner sur système Linux, mais il existe une version pour Windows. Il permet de tirer profit des processeurs multicœurs et de la puissance de plusieurs ordinateurs (cluster). La progression est automatiquement sauvegardée pour reprendre un projet en cours. Sur notre PC de test, PDFCrack a été capable de passer en revue 37 500 mots de passe à la seconde. Pour tester la liste complète de notre dictionnaire de 10 millions de sésames, il ne lui faudrait que 5 minutes.

PAS À PAS

Utilisation de PDFCrack

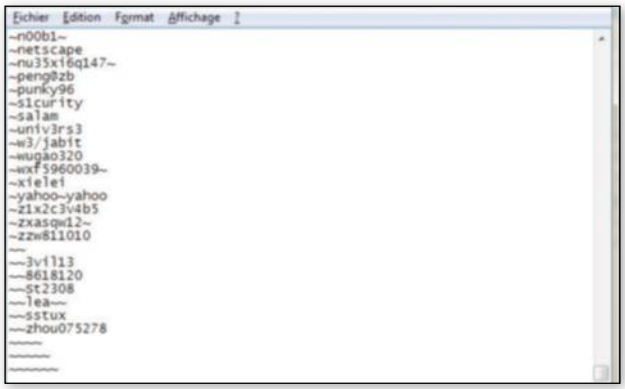
CE QU'IL VOUS FAUT

PDFCRACK

OÙ LE TROUVER ? :
http://andi.flowrider.ch/research/pdfcrack.html

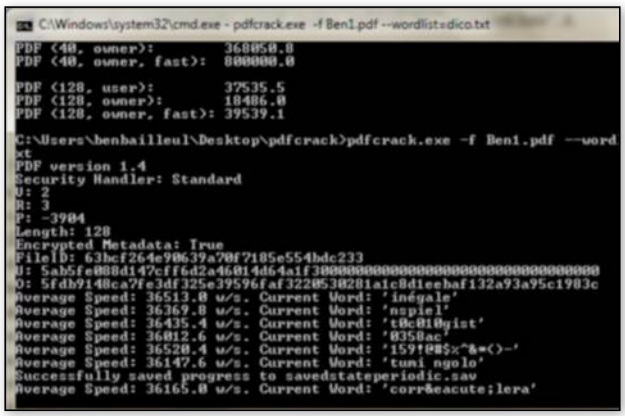
DIFFICULTÉ : ☠☠☠

01 NOTRE DICTIONNAIRE



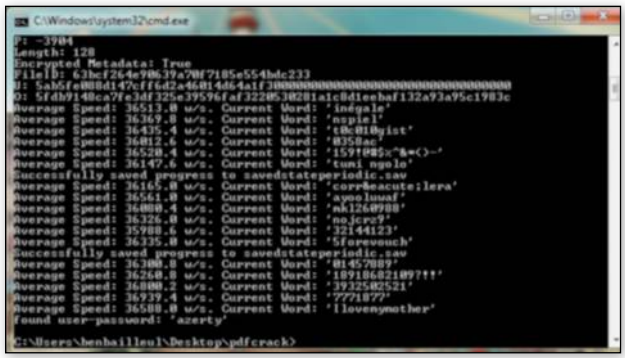
Téléchargez et décompactez les fichiers dans un dossier où vous placerez aussi le fichier PDF à cracker et votre fichier dictionnaire au format TXT ou LST. Pour trouver ce type de fichier, il faudra fureter sur Google ou se rendre ici : www.openwall.com/passwords/wordlists. Vous devriez pouvoir en trouver sans payer. Le mieux est de récupérer plusieurs listes puis de les mettre dans un seul fichier. Après quelques minutes nous avons pu nous «fabriquer» un fichier de 48 Mo contenant près de 10 millions de mots.

02 LES COMMANDES



Précisons avant de commencer que dans notre exemple, le fichier PDF à cracker s'appelle **Ben1** et que notre dictionnaire a pour nom dico. Maintenez la pression sur la touche **Maj** du clavier et faites un clic droit dans le dossier contenant vos fichiers et sélectionnez **Ouvrir une fenêtre de commandes ici**. Tapez ensuite **pdfcrack.exe -f Ben1.pdf –wordlist=dico.txt**. Notez qu'il est possible d'ajouter d'autres commandes pour affiner la recherche (voir encadré).

03 ET «CRACK» LE MOT DE PASSE



Pendant la recherche, le logiciel vous dira où il en est dans la liste des mots de passe et sauvegardera la progression automatiquement. Pour reprendre depuis ce point de sauvegarde on écrira: **pdfcrack.exe -f Ben1.pdf –wordlist=dico.txt –loadState=savedstateperiodic.sav**. Dans nos exemples, les mots de passe azerty et secret ont été trouvés en moins d'une minute. Par contre pour **Mx3^Zi_kL28**, le problème est tout autre puisqu'il y a peu de chance de trouver ce mot de passe dans un dictionnaire. Il faudra utiliser la méthode «brute force». C'est ce que nous verrons dans le prochain numéro
À suivre...

QUELQUES OPTIONS SUPPLÉMENTAIRES

Ces commandes sont à taper après avoir écrit le nom du fichier PDF. Il est possible d'en mettre plusieurs à la suite.

--permutate : permet d'ajoutera une majuscule à un mot de passe pour le premier caractère si ce dernier est en minuscule.

--bench : permet de savoir combien de mots de passe seront essayés à la seconde. Regardez la ligne PDF (128, user).

--minpw=3 : ne pas tenter les mots de passe plus courts que 3 caractères

--maxpw=15: arrêter lorsque le logiciel atteindra la liste des mots de passe de 15 caractères

--owner: commande permettant de s'attaquer au mot de passe d'autorisation (le mot de passe d'ouverture est attaqué par défaut)

CRACKER

LE MOT DE PASSE DE WINDOWS

Que vous ayez oublié votre mot de passe Windows ou que vous ne le connaissiez pas (achat d'occasion, dépannage chez un ami, etc.), il existe une solution pour réinitialiser ce dernier et en définir un autre… Ce n'est pas vraiment un «crack» mais l'effet est le même.

Windows stocke les informations concernant l'utilisateur dans le fichier **SAM** du répertoire C:Windows\system32\config. Ce fichier contient les mots de passe cryptés et plusieurs autres choses sensibles. Malheureusement, il n'est pas possible de changer le mot de passe si vous ne pouvez pas ouvrir une session avec les droits pour le faire. Si vous ne vous souvenez pas du mot de passe et que vous n'avez pas créé de clé USB permettant d'ouvrir votre session (voir encadré), vous êtes bloqué avec un PC qui ne se lancera pas. La seule solution consiste alors à formater.

UN NOM À RALLONGE POUR UN LOGICIEL TRÈS EFFICACE

Heureusement, il y a Offline NT Password & Registry Editor. Il s'agit d'un logiciel permettant de réinitialiser le mot de passe des comptes utilisateurs de tous les Windows de NT jusqu'à 8.1 en passant par XP. Nul besoin de connaître l'ancien mot de passe pour en définir un nouveau. Il suffit de graver l'image sur un disque (ou de le placer sur une clé USB) puis de «booter» dessus pour afficher l'interface. Que votre disque dur soit formaté en FAT 32 ou en NTFS, le logiciel détectera les comptes utilisateur locaux et les déverrouillera. Il est même possible de les désactiver ou d'ajouter un utilisateur pour devenir administrateur.

LEXIQUE

***SAM :**
Accronyme de Security Account Manager. Le fichier SAM est stocké dans C:Windows\system32\config. C'est un fichier «ruche», il fait donc partie de la base de registre. La fonction de hachage utilisée pour les mots de passe est le MD5 (voir *Pirate Informatique* n°24)

PAS À PAS

Préparation du CD ou de la clé USB de boot

CE QU'IL VOUS FAUT

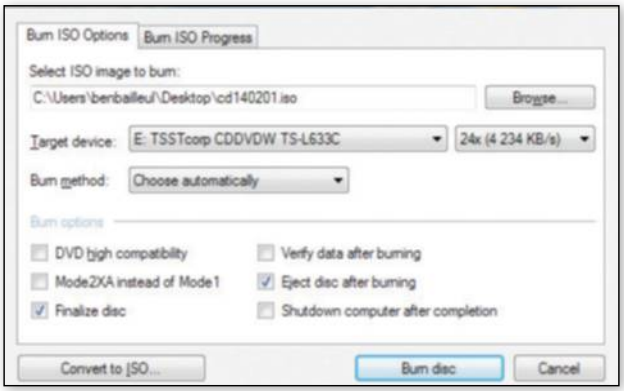
OFFLINE NT PASSWORD & REGISTRY EDITOR

OÙ LE TROUVER ? :
http://pogostick.net/~pnh/ntpasswd

DIFFICULTÉ : ☠☠☠

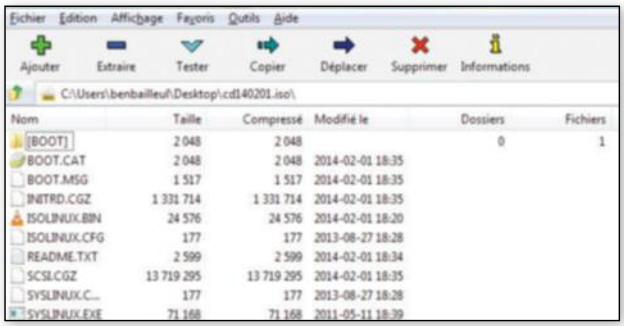
01 LE CD DE BOOT

Dézippez le fichier ZIP pour extraire le fichier ISO. Il s'agit d'une image de CD que vous pouvez graver avec n'importe quel logiciel de gravure comme CDBurnerXP (option **Burn ISO Image** au démarrage). Au final, vous devriez avoir 10 fichiers et un dossier sur votre CD.



02 LA CLÉ USB DE BOOT

Si vous préférez utiliser une clé USB, il suffit de décompresser le fichier ZIP et de décompresser encore une fois le fichier ISO (avec 7-Zip, par exemple) pour mettre la totalité des fichiers sur la clé. Depuis une invite de commande (tapez **cmd** dans le champ **Rechercher** du menu **Démarrer**), tapez depuis l'unité de votre clé USB la commande **j:\syslinux.exe -ma j:** (si J est la lettre correspondante à la clé). Votre clé USB est prête...

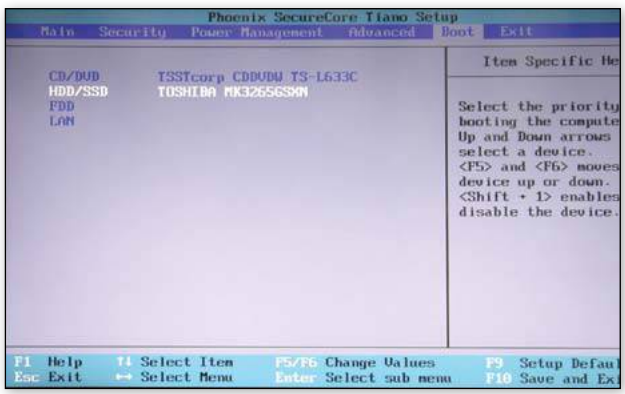


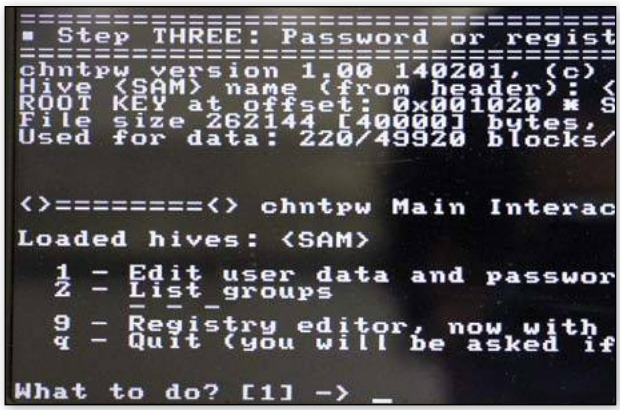
PAS À PAS

Réinitialiser le mot de passe Windows

01 BOOT SUR LE CD OU LA CLÉ USB

Si le programme ne se lance pas au démarrage du PC, c'est que l'ordre du boot n'est pas le bon. Faites **Suppr** ou **F1** (en fonction de votre carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** et modifiez l'ordre en mettant en premier votre lecteur de CD/DVD ou la clé USB. Parfois, l'option de boot est à l'extérieur du BIOS, regardez bien ce que s'affiche au démarrage pour entrer dans ce menu.





02 LE DÉMARRAGE

Lors du démarrage du logiciel, validez en tapant sur **Entrée**. Sélectionnez la version de boot. Dans la plupart des cas, laissez le choix **1** pour sélectionner la partition détectée. Validez avec la touche **Entrée** du clavier. Laissez le choix du chemin du dossier de registre de Windows et validez. Laissez le choix 1 pour changer le mot de passe et laissez encore le choix 1 pour éditer le compte. Validez à chaque étape en tapant sur **Entrée**.

03 FAITES VOS COMPTES...

Laissez le compte Administrateur par défaut et validez encore. Il est bien sûr possible de sélectionner d'autres comptes. Certains comptes peuvent être désactivés (**Dis**) ou verrouillés (**Lock**). Vous pourrez les réactiver ou les déverrouiller depuis cette interface.

04 RÉINITIALISATION OU CHANGEMENT

Tapez **1** (clavier numérique) pour réinitialiser le mot de passe et validez encore une fois. Vous pouvez aussi ajouter un nouveau mot de passe avec l'option **2** (attention au type de clavier), faire en sorte de mettre un compte en administrateur (option **3**) ou activer un compte verrouillé (option **4**).

QUEL OS ?

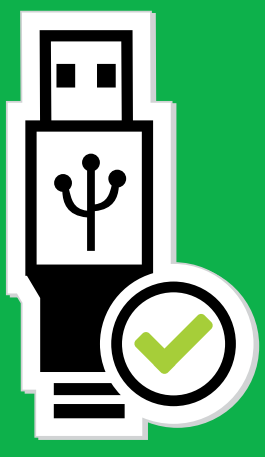
Le programme fonctionne pour Windows NT3.51, NT4 (toutes les versions), Windows2000, Windows Millenium, WindowsXP (SP1, 2 et 3), Windows Server (2003, 2008 et 2012), Windows Vista, Windows 7 et Windows 8. Bien sûr les versions 32 et 64 bits sont toutes concernées.

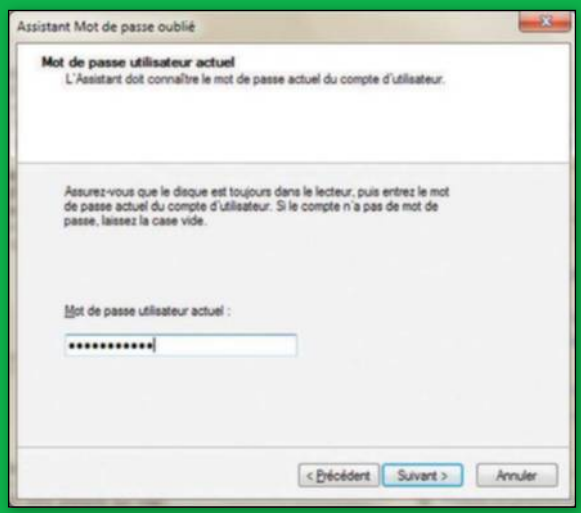
05 RETOUR À WINDOWS !

Tapez **!** pour quitter (sur un clavier AZERTY, faites **Maj** + **&**) et validez. Tapez **Q** pour quitter (**A** sur un clavier AZERTY) et **Y** pour valider les changements. Lorsque l'on vous demande **New run?**, faites **N** et redémarrez la machine en faisant **Ctrl** + **Alt** + **Suppr** (sans oublier de retirer le CD ou la clé). Vous pouvez maintenant entrer dans Windows en laissant le mot de passe en blanc ou en entrant le nouveau !

LA CLÉ USB «PENSE-BÊTE»

Si vous n'avez pas envie de retenir votre mot de passe, il est possible de créer une clé USB qui fera office de «pense-bête» si vous oubliez votre mot de passe Windows. Dans le champ **Rechercher** de votre Windows, tapez **mot de passe** et sélectionnez **Modifier votre mot de passe Windows**. Sur la nouvelle fenêtre, cliquez à gauche dans **Créer un disque de réinitialisation de mot de passe** en ayant pris soin de placer une clé USB. Faites deux fois **Suivant**, tapez votre mot de passe et laissez Windows opérer. Un fichier PSW sera présent sur votre support amovible. Mettez cette clé en lieu sûr...





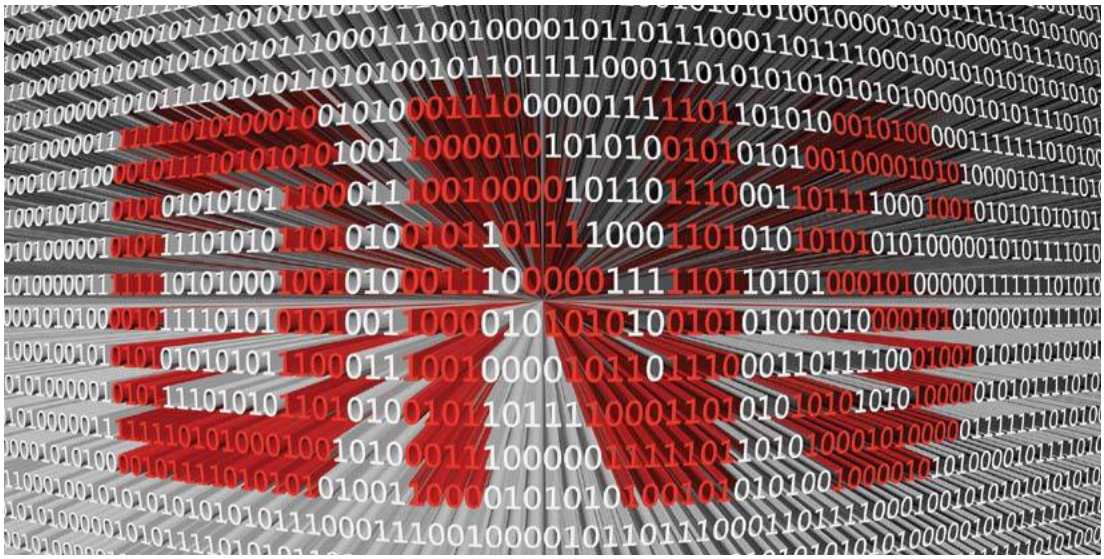
TÉLÉCHARGER // STREAMING

MAGAZINE INTERDIT

CHEZ VOTRE MARCHAND DE JOURNAUX !

VOTRE SERVEUR DNS À LA MAISON

Les DNS font le lien entre vous et les sites que vous voulez consulter. Le problème c'est que les serveurs DNS de vos FAI sont à la botte des censeurs et que les autres (Google, Verizon, etc.) sont à l'étranger et mangent dans la main de la NSA. La solution ? Tout héberger à la maison !



Un serveur DNS est le premier chaînon entre votre ordinateur et Internet lorsque vous voulez consulter un site. Le travail de ce type de serveurs est de mettre une adresse IP sur le nom que vous aurez tapé dans la barre de recherche ou sur le lien sur lequel vous cliquez. En effet, chaque site a une adresse unique du type 154.18.05.42 et pourtant vous ne tapez jamais une IP pour aller sur tel ou tel site.

CONTOURNER LA CENSURE, MAIS PAS À N'IMPORTE QUEL PRIX !

La plupart du temps vous utilisez sans le savoir le DNS de votre FAI. Ce dernier sait alors sur quels sites vous vous rendez et quelles sont vos habitudes de surf. Ce n'est pas vraiment un problème car la société ne peut vous «trahir» que sur décision d'un juge. Les problèmes commencent lorsqu'il s'agit de faire disparaître purement et simplement un site de la surface du Web français comme avec The Pirate Bay ou dernièrement avec t411. Ces sites ont en effet disparu temporairement (t411 a dû changer son nom de domaine pour contourner la décision) puisque les FAI français ont été sommés de les retirer de la liste des sites accessibles.

ON N'EST JAMAIS MIEUX SERVI QUE PAR SOI-MÊME

De nombreux sites ont alors conseillé les DNS de Google pour contourner la censure. En effet le géant du Web possède des serveurs DNS que tout le monde peut emprunter. Cerise sur le gâteau, Google propose même un pre-fetching : il charge les sites les plus populaires pour afficher plus rapidement les pages que vous voulez consulter. C'est formidable sauf qu'une fois encore il s'agit d'un stratagème de Google pour mettre en avant ses propres services (*«Ouah, ça charge bien plus vite YouTube depuis que j'ai changé pour les DNS Google !»*) mais aussi pour savoir exactement ce que vous faites sur Internet. Attention, car Google n'est pas votre FAI, il fait ce qu'il veut de ces informations. Et si Google sait ce que vous faites alors la NSA le sait aussi ! Longtemps la solution de repli a été OpenDNS mais ce dernier a été racheté par Cisco, une grosse compagnie américaine qui collabore sans honte avec les services secrets. On peut aussi envisager de changer pour les DNS du FAI associatif FDN (80.67.169.12 et 80.67.169.40) mais la solution la plus sûre est encore d'héberger vous-même en local votre propre serveur DNS...

LEXIQUE

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

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

Installation de Unbound en local

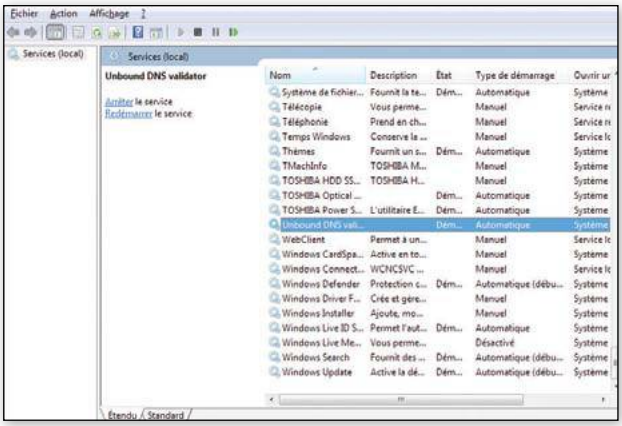
CE QU'IL VOUS FAUT

UNBOUND

OÙ LE TROUVER ? :
https://unbound.net

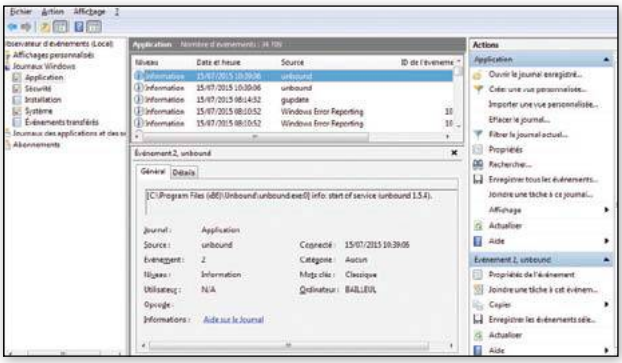
DIFFICULTÉ :

01 INSTALLATION



Unbound est un simple logiciel Windows à installer sur votre PC. Une fois l'installation terminée, vérifiez sa présence dans les services de Windows en tapant **services.msc** dans le champ de recherche. Vérifiez aussi que le lancement du service se fera automatiquement en faisant un clic droit dans **Unbound** puis **Propriétés**. Le Type de démarrage devrait être sur **Automatique**.

02 VÉRIFICATION



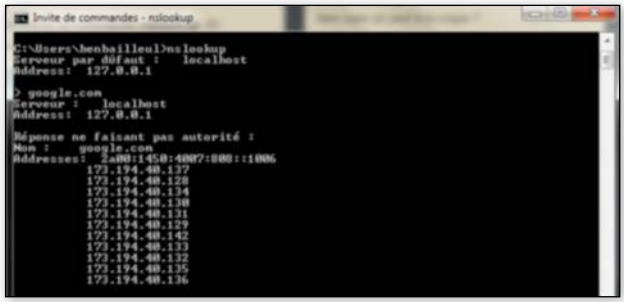
Vérifiez ensuite que tout se passe bien au niveau de l'implémentation depuis l'**Observateur d'événements**. Tapez **observateur** dans le champ de recherche puis sur la gauche Journaux **Windows>Application**. Si vous ne voyez pas de point d'exclamation, c'est que tout va bien !

03 ADRESSE DNS

Allez ensuite dans le **Panneau de configuration** puis, dans la zone de recherche en haut à droite tapez **carte réseau**. Dans **Centre Réseau et partage**, cliquez sur **Afficher les connexions réseau**. Faites un autre clic droit dans votre

connexion puis cliquez sur **Propriétés**. Sélectionnez **Protocole Internet version 4 (TCP/IPv4)** et faites **Propriétés**. Dans la deuxième partie de cette fenêtre choisissez **Utiliser l'adresse de serveur DNS suivante**, tapez **127.0.0.1** sur la première ligne et validez.

04 VOTRE SERVEUR EST EN PLACE !



Pour être sûr que votre serveur DNS est bien en place, il est possible de lancer une **Invite de commandes** (**cmd** dans le champ de recherche), de taper **ipconfig /all** et de chercher la ligne concernant les DNS. On peut aussi faire **nslookup** et chercher un site pour résoudre certains domaines (tapez **google.com** par exemple). Si le temps de réaction de votre connexion vous semble un peu long, c'est normal. Tout rentrera dans l'ordre lorsque le système sera rodé.

CHEZ VOTRE MARCHAND DE JOURNAUX

MINI PRIX
2,90 €
Seulement

LE 1ER MAGAZINE
100% ANDROID ET 100% PRATIQUE

KALI LINUX S'INVITE SUR RASPBERRY PI 2 !

Chez *Pirate Informatique* on aime le Raspberry Pi et Kali Linux. Il est donc tout naturel de les réunir dans un article, car non seulement une version de Kali est disponible pour les machines à base d'ARM, mais qu'en plus, un nouveau Raspberry vient de sortir dans une version quatre fois plus musclée !

SUR NOTRE CD

Si vous avez raté les derniers numéros de *Pirate Informatique*, retrouvez tous les précédents articles concernant le Raspberry Pi sur notre CD : la présentation de l'appareil, la conception d'un Media Center, d'un système de vidéosurveillance, d'une borne d'arcade, d'un récepteur Webradio, d'une radio FM amateur et d'un cloud personnel.

Le Raspberry Pi 2 vient de sortir et le moins qu'on puisse dire c'est qu'il écrase complètement l'ancienne version en terme de puissance (voir encadré). Comme nous avons eu la chance d'en voir un malgré les fréquentes ruptures de stock, nous voulions réaliser un projet permettant de profiter de cette puissance de calcul. Inutile de dire que ce nouveau Raspberry est encore plus à l'aise lorsqu'il s'agit de faire office de NAS ou de Media Center, mais comme nous l'avons déjà fait (voir notre CD avec les anciens PDF), nous avons décidé de faire tourner «la bête» avec Kali Linux. Pour tester les réseaux sans fil, il faudra néanmoins acheter un module WiFi pour une quinzaine d'euros. Notez aussi qu'une version spéciale de ce Kali pour Raspberry propose aussi la prise en charge d'un écran TFT (que vous pourrez trouver pour une trentaine d'euros sur Internet).

LES DIFFÉRENCES ENTRE LES RASPBERRY PI

Si les différences entre les versions A et B+ du premier Raspberry ne concernaient que l'ajout de RAM (de 256 à 512 Mo), cette nouvelle mouture Pi 2 voit gonfler toutes ses caractéristiques pour le même prix (environ 40 €). Notez que le Pi 2 est compatible avec tous les anciens modules (caméra, dongle WiFi, etc.) Pas la peine de racheter quoi que ce soit... Si vous voulez connaître les différences de puissance «sur le terrain» suivez ce lien : **http://goo.gl/UYHs0m.**

	Raspberry Pi B+	Raspberry Pi 2
Date de sortie	Février 2012	Février 2015
Chipset	ARMv6 (1 cœur)	ARMv7 (4 cœurs)
Horloge	700 MHz	900 MHz
RAM	512 Mo	1 Go
Type de mémoire	SDRAM 400 MHz	DDR2 450 MHz
Stockage	Carte SD	Carte MicroSD
Ports USB	2	4

Ce tableau ne rend compte que des différences entre les deux machines, le reste des spécifications restant identiques (port RJ45, connectiques HDMI, RCA, GPIO, jack 3.5mm, etc.)

À gauche notre bon vieux Raspberry B+ utilisé depuis 2 ans par la rédaction pour nos différents projets. À droite la nouvelle version 2 très prometteuse...

LEXIQUE

***RASPBERRY PI :**
Le Raspberry Pi est un nano-ordinateur créé dans le but d'encourager l'apprentissage de l'informatique aux personnes avec peu de moyens ou dans les pays en voie de développement. Tous les composants sont réunis sur une seule carte et le tout est livré sans moniteur, clavier, souris, système d'exploitation, disque dur ou alimentation pour privilégier la récupération et les licences libres.

***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.

PAS À PAS

Kali sur Raspberry !

CE QU'IL VOUS FAUT

KALI LINUX CUSTOM ARM IMAGE
OÙ LE TROUVER ? : **https://goo.gl/HDf3Zo**

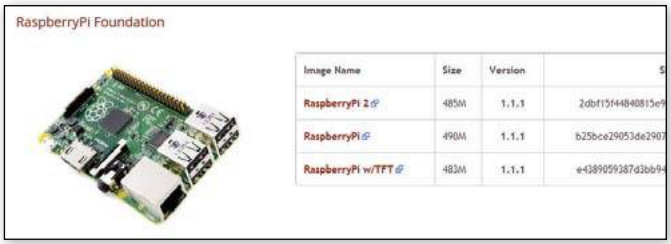
WIN32 DISK IMAGER
OÙ LE TROUVER ? : **http://sourceforge.net/projects/win32diskimager**

DIFFICULTÉ : ☠☠☠

Un Raspberry Pi 2 (ou une ancienne version) ; Un câble micro-USB (pour l'alimentation) ; Une carte SD d'au moins 8 Go (classe 10) ; Une TV ou un écran de récupération ainsi qu'un clavier et une souris

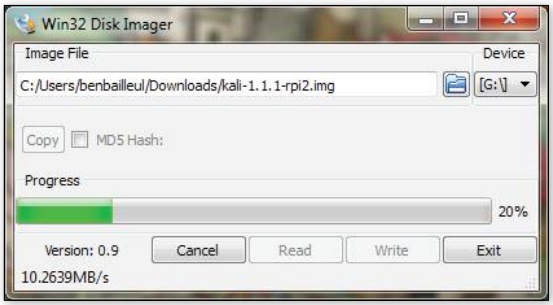
01 TÉLÉCHARGEMENT DE L'IMAGE «CUSTOM»

Commençons par placer l'image de Kali spécialement conçue pour les appareils à base de processeur ARM. Suivez notre lien et allez dans la section **Raspberry Pi Foundation**. Vous trouverez ici les images pour les premières versions (avec ou sans écran TFT) et pour la version 2. Le format XZ se décompacte sans problème avec le logiciel 7zip. Vous devriez avoir au final un fichier **kali-1.1.1-rpi2.img**. Pour mettre le contenu de ce dernier dans la carte, il faudra utiliser le logiciel Win32 Disk Imager.



02 INSTALLATION DES FICHIERS

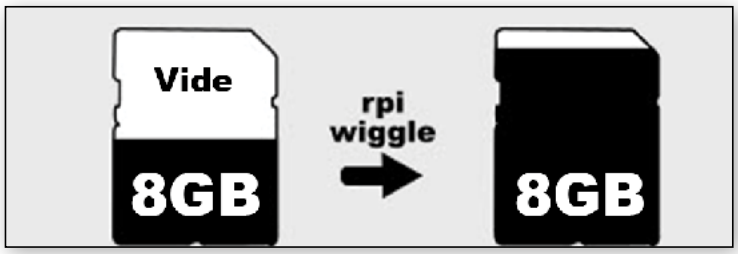
Téléchargez le logiciel et munissez-vous d'une carte SD d'au moins 8Go. Lancez Win32 Disk Imager, sélectionner **kali-1.1.1-rpi2.img** avec l'icône en forme de dossier puis spécifiez l'emplacement de la carte SD dans la colonne **Device**. Ne vous trompez pas sous peine d'effacer le contenu d'un de vos disques durs! Faites **Write** et attendez la fin du processus. Notez que pour revenir en arrière et récupérer une carte en FAT32, il faudra passer par le logiciel gratuit MiniTool Partition Wizard.



03 BRANCHEMENT ET LANCEMENT

Il est temps de brancher le Raspberry Pi sur l'écran via les ports HDMI ou RCA. Pour profiter des mises à jour du système et d'Internet, il faudra connecter une prise RJ45 si vous n'avez pas de module WiFi. Une fois que l'alimentation est branchée, Kali va démarrer. Le login est **root** et le mot de passe est **toor**. Lorsque vous aurez le prompt **root@kali :~#** il faudra taper **startx** pour lancer l'interface graphique (tapez sur **q** pour faire le **a**). Dans **Applications Menu**>**Settings**>**Keyboard**, vous pourrez configurer le clavier à la française

04 OPTIMISATION DE LA CARTE SD



Optimisons maintenant la place disponible sur la carte SD pour mettre à jour Kali et charger la version complète avec tous les logiciels. Pour cela il va falloir télécharger le script rpi-wiggle. Ouvrez le **Terminal Emulator** (dans **Applications Menu**) et faites:

apt-get install sudo puis **apt-get install parted** et enfin

wget http://raw.github.com/dweeber/rpiwiggle/master/rpi-wiggle

Le script devrait être dans **Home** (sinon trouver le répertoire de destination avec la commande **cd**).
Tapez alors

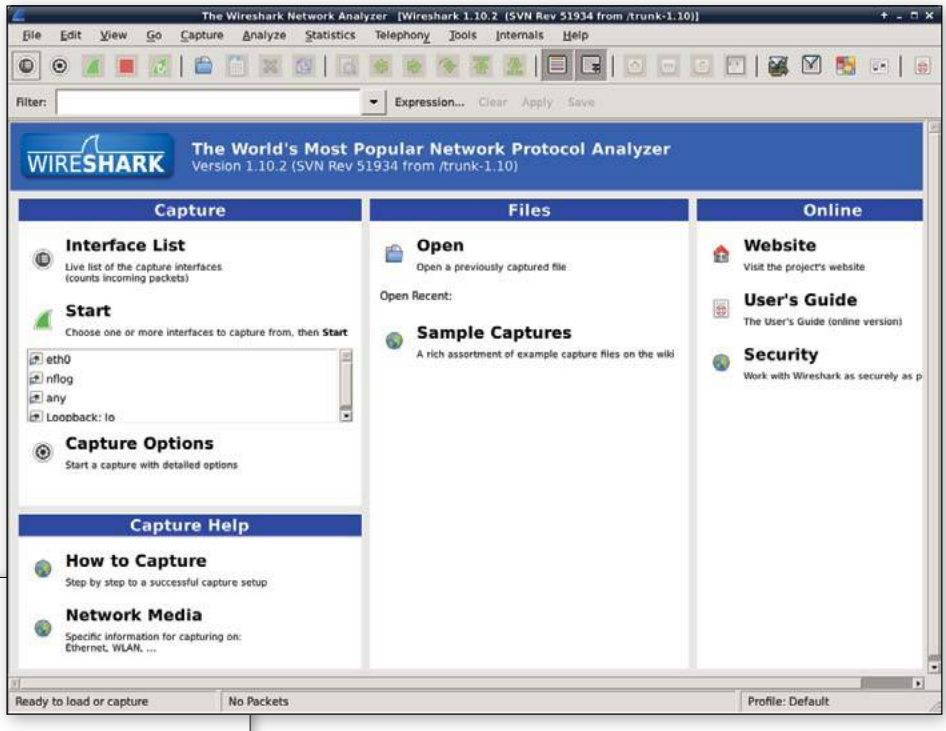
chmod +x ./rpi-wiggle pour autoriser l'exécution du script

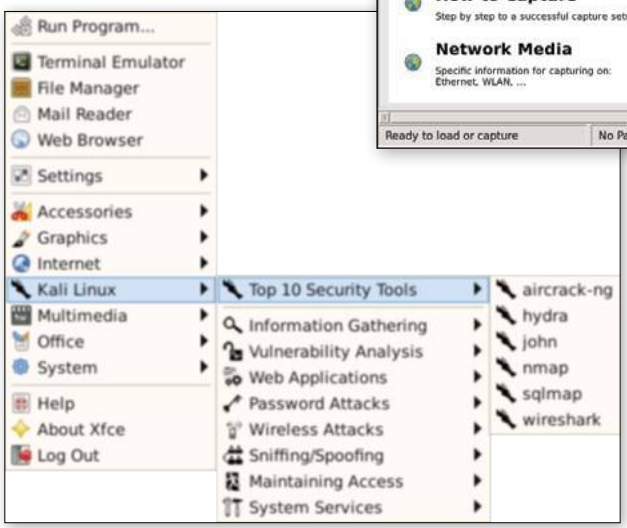
puis

./rpi-wiggle

05 KALI LINUX FULL !

Le script va alors afficher différentes informations sur votre volume et sur les modifications à venir. Redémarrez en tapant **Entrée** lorsqu'on vous le demandera. Vous pourrez enfin faire **apt-get update** puis **apt-get install kali-linux-full** pour télécharger le build complet de Kali Linux. Devrait ensuite s'ensuivre une longue session de téléchargement et d'installation, mais à la fin vous retrouverez WireShark, John The Ripper et tous les autres logiciels de cette distribution!





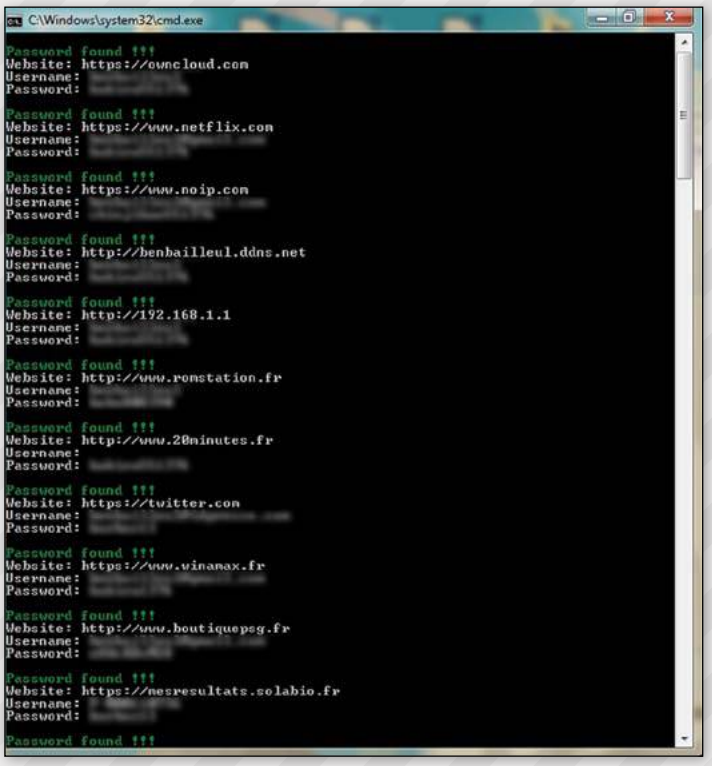
DANS NOTRE PROCHAIN NUMÉRO, NOUS FERONS UN SUJET SPÉCIAL SUR KALI LINUX AVEC LA PRÉSENTATION DES OUTILS ET DES FONCTIONNALITÉS SYMPAS ! BIEN SÛR VOUS POURREZ EN PROFITER MÊME SI VOUS N'AVEZ PAS DE RASPBERRY PI...

#1 Récupérez des mots de passe

avec LaZagne

Après FilePizza pour transférer vos fichiers, voici Lazagne pour récupérer des mots de passe! Dans le même genre que RecALL (voir Pirate Informatique n°23), ce programme en ligne de commande va pomper les sésames contenus dans vos navigateurs et plusieurs autres logiciels. Il est légèrement moins complet que RecALL, mais est beaucoup plus discret et rapide. Décompactez le fichier ZIP et rendez-vous dans le dossier **LaZagne-master\Windows**. Maintenez la touche **Maj** du clavier, faites un clic droit dans **Standalone** puis cliquez sur **Ouvrir une fenêtre de commande ici**. Tapez ensuite **lazagne.exe all**. Magique!

Lien: **https://github.com/AlessandroZ/LaZagne**



#2 Surfez sans connexion

avec Offline sur Android

Ce type de programme, très populaire sur PC dans les années 90 (quand on devait se connecter depuis un modem à chaque fois que l'on désirait un accès à Internet) revient naturellement sur nos mobiles. Offline Browser permet en fait de charger le contenu d'un site en mémoire pour pouvoir naviguer ultérieurement sans connexion. Pas de réseau? Voyage en train, en avion? Perdu dans la pampa? Avec Offline vous réglez la quantité de données à mettre en mémoire avant de partir et vous pourrez lire tutos, news, etc.

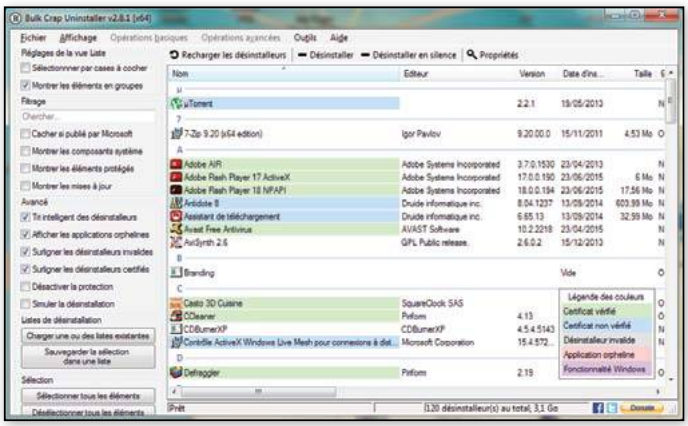
Lien: **https://goo.gl/wH4zZS**

#3 Désinstallez par lot!

avec BCUninstaller

Si vous avez l'habitude d'installer et de désinstaller des logiciels pour les tester, Windows n'autorise pas la désinstallation par lots : il faut attendre qu'un programme soit parti pour se débarrasser du suivant. BCUninstaller va s'occuper de cette tâche ingrate à votre place. Il suffit de cocher les cases et de laisser faire le programme. Pratique si vous avez récupéré un PC d'occasion ou si vous devez faire le ménage sur l'ordi de mamy. Pour chaque logiciel une couleur sera associée pour éviter de désinstaller des éléments importants. Cerise sur le gâteau, le mode silencieux est géré : pas besoin de rester collé à la souris pour faire avancer le processus...

Lien: **http://klocmansoftware.weebly.com**

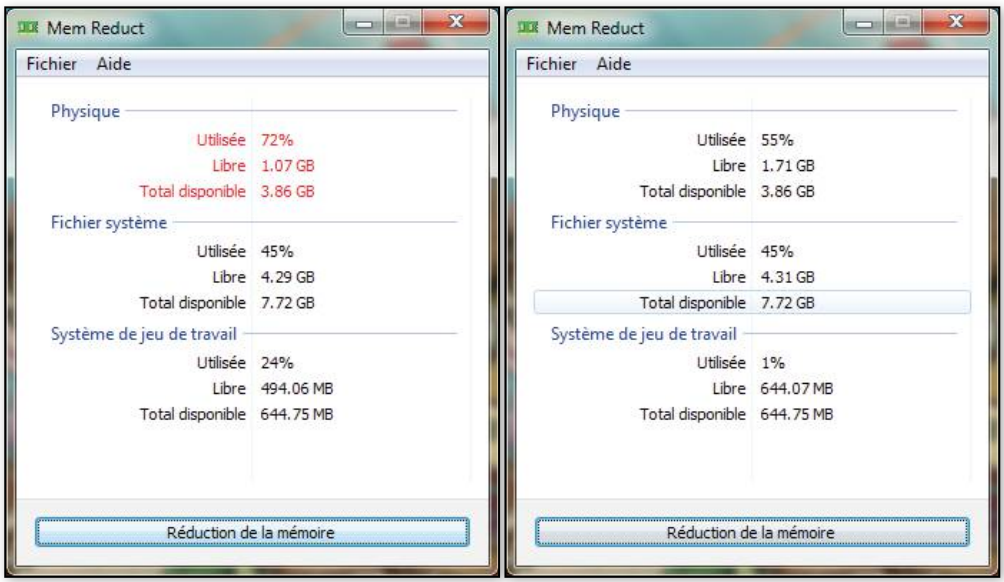


#4 Économisez de la mémoire

avec Mem Reduct

Voici un petit programme très simple permettant de déplacer sur le disque dur les données contenues dans la mémoire cache. Il s'agit en fait de récupérer artificiellement de la mémoire vive lorsqu'on en a le plus besoin. Certes Windows gère lui-même la RAM (avec plus ou moins de succès), mais cet outil peut s'avérer utile si vous devez lancer un programme gourmant en mémoire sans avoir à redémarrer l'ordinateur ou à faire le ménage dans vos processus.

Lien: **www.henrypp.org/product/memreduct**

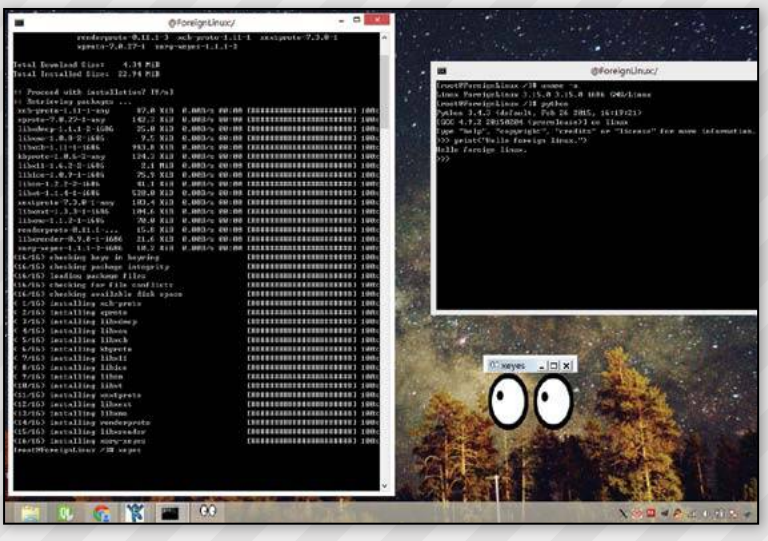


#5 Linux sur Windows

avec Foreign Linux

Pour disposer de Linux sur son PC on peut l'installer sur une partition dédiée ou utiliser un Live CD. Mais si vous n'avez pas votre matériel sous la main et que vous voulez tester une application, il reste encore la solution de l'émulateur. Bien sûr il existe WINE, mais ce dernier émule tout le système Linux (ce qui est lourd) tandis que Foreign Linux va simplement traduire les requêtes du système Linux vers leur équivalent Windows. Le but est de faire fonctionner des programmes Linux simples sous un environnement 100% Windows. Bien sûr tout ceci est expérimental. Si Linux vous intéresse, mais que vous ne voulez pas mettre les mains dans le cambouis, lisez notre article sur la distribution Mageia (dans le dossier *Un PC à 0€* que nous avons réalisé dans *Pirate Informatique* n°23)

Lien**: https://github.com/wishstudio/flinux**



#6 Envoyez ce fichier sans tarder

avec FilePizza

Vous avez besoin d'envoyer ce gros fichier sans tarder à un correspondant qui l'attend de pied ferme devant son PC ? Pas besoin de l'uploader avec FilePizza ! Ce service vous demande simplement l'emplacement de votre fichier pour générer un lien. En

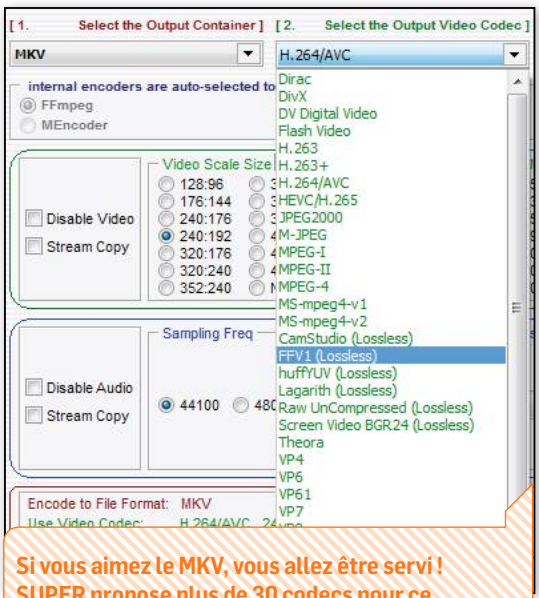
cliquant sur ce dernier, votre correspondant téléchargera le fichier directement chez vous sans passer par un serveur. Seul inconvénient, le lien ne sera plus valable dès que vous aurez fermé la page ou l'onglet FilePizza.

Lien: **http://file.pizza**

UN ENCODAGE SUPER© !

Il n'y a pas que m4ng dans la vie ! Et même si vous avez un autre logiciel préféré pour encoder vos musiques ou vos vidéos, SUPER risque bien de vous faire changer de crèmerie. Doté d'une interface simple ce programme très puissant permet les réglages les plus pointus...

Dans *Pirate Informatique*, nous vous parlons souvent de m4ng, Media Coder ou de Format Factory, mais de nombreux lecteurs nous ont écrit pour nous conseiller de tester SUPER (pour Simplified Universal Player Encoder & Renderer). Malgré son interface un peu rude, ce dernier propose d'encoder et de convertir tous les fichiers multimédias que vous voulez. Comme m4ng, SUPER apporte une interface graphique unifiée à divers programmes et librairies d'encodage (x264, FFmpeg, Mplayer, etc.) dans le but de proposer un outil ultime. Il suffit de prendre un ou plusieurs fichiers et de choisir le conteneur et les codecs de votre choix pour lancer la machine. Les plus exigeants pourront bien sûr choisir le birate, la résolution, le ratio de l'image, etc. Les débutants, eux, auront à dispositions des préréglages pour différents appareils : PlayStation 3, produits Apple, Android, etc. À essayer d'urgence d'autant qu'aucun codec additionnel n'est à installer.



Si vous aimez le MKV, vous allez être servi ! SUPER propose plus de 30 codecs pour ce conteneur, y compris le très récent VP9...

POURQUOI CHOISIR SUPER ?

Nous avons découvert SUPER grâce à un lecteur qui nous a demandé comment mettre une vidéo sur la tablette Vtech Storio 3S de sa fille. Comme Vtech vend des dessins animés en ligne, la marque n'a pas forcément envie que l'on puisse mettre des fichiers multimédias sans passer par la caisse. C'est bien légitime, mais dans notre cas, il s'agissait de vidéos de vacances ! Nous nous sommes donc penchés sur le problème. Plutôt que de mettre une protection DRM coûteuse sur leurs appareils, la marque a décidé de faire autrement : rendre uniquement compatible des fichiers encodés d'une manière très alambiquée : AVI H264/AVC (Profile Baseline levels 3.1) avec un Bitrate de 624Kbps à 15 fps, etc. Le but ? Décourager les utilisateurs de mettre leur propre vidéo sur la tablette. SUPER nous a permis de gérer ces petits détails... avec succès !

LEXIQUE

***ENCODAGE :**
L'encodage consiste à modifier les données d'un fichier multimédia pour le compresser ou pour le faire fonctionner sur un appareil ne permettant pas l'installation de codec. Avec SUPER il est par exemple possible de changer un film lu sur PC (codec DivX, conteneur AVI) pour le lire sur une PlayStation 3 (codec H264, conteneur MP4). Cela fonctionne aussi pour le son alors que pour la photo on parlera plutôt de conversion.

***CODEC :**
Mot-valise pour «codeur-décodeur». Il s'agit d'un programme capable de compresser et/ou de décompresser un signal numérique : audio ou vidéo. Par exemple, il vous faudra le codec Xvid installé sur votre PC pour lire un fichier AVI encodé en Xvid.

PAS À PAS

L'interface de SUPER

CE QU'IL VOUS FAUT

SUPER

OÙ LE TROUVER ? : **www.erightsoft.com**

DIFFICULTÉ :

01 LE SITE

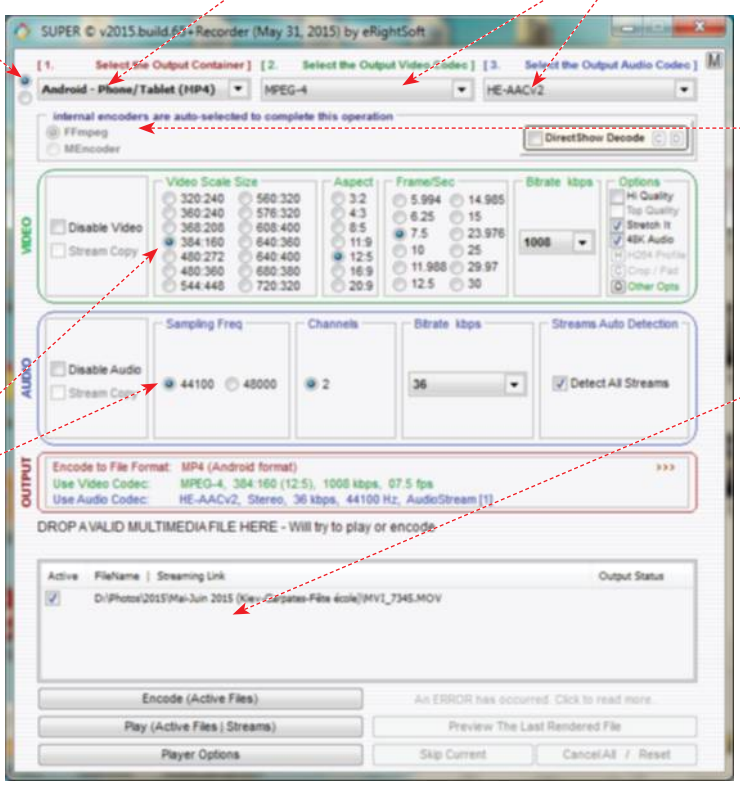
Sur le site allez tout en bas et cliquez sur **Start Downloading SUPER** puis encore tout en bas, allez sur **Donwload SUPER Setup file**. Vous pouvez aussi récupérer le logiciel sur notre CD. Attention car sur certaines versions SUPER, le programme d'installation vous proposera des logiciels additionnels. À vous de décocher les cases si c'est le cas... En cas d'erreur, utilisez AdwCleaner pour faire le ménage.

02 LES DIFFÉRENTES ÉTAPES

Menu d'outils secondaires : assembler et compartimenter des fichiers, retirer la bande son, etc.

> ÉTAPE 2
Sélection du conteneur (AVI, MP4, etc.), de l'appareil (PSP, Xbox, etc.) ou de la structure (DVD par exemple).

> ÉTAPE 3
Sélection des codecs vidéo et audio. Certains codecs ne seront pas disponible en fonction de ce que vous aurez choisi à l'étape 2.



En fonction de vos réglages, SUPER choisira l'encodeur adéquat mais parfois vous aurez le choix.

Les réglages liés à la vidéo et au son : résolution, bitrate, fps, ratio de l'image, échantillonnage, etc. Laissez les valeurs par défauts si vous encodez un fichier pour un appareil précis. Rien ne vous empêche cependant de faire différents essais...

> ÉTAPE 1
Glissez-déposez un ou plusieurs fichiers ici. Le logiciel l'analysera automatiquement et vous affichera un descriptif complet avec les codecs utilisés, le format, le poids, etc.

03 VOTRE FICHIER DE SORTIE

Lorsque vous aurez terminé les réglages, il suffira de faire **Encode (Active Files)** et de laisser le logiciel travailler pour vous. Le fichier de sortie devrait être dans le même répertoire que le fichier d'origine. Si cela ne vous convient pas, il faudra faire un clic droit dans l'interface, aller dans **Output File Saving Manager,** décocher la deuxième case et faire **Browse Folder**.

DES CHAÎNES DE TÉLÉ À LA DEMANDE

LEXIQUE

***MEDIA CENTER :**
Media Center peut désigner un disque dur multimédia relié à une TV ou un Home Cinema mais nous ne parlerons ici que de la partie logicielle. Kodi est un programme qui peut se greffer sur presque n'importe quel système pour en faire une interface de lecture conviviale. Il permet de regrouper vos vidéos, musiques et photos pour en profiter sur votre téléviseur.

***PLUGIN :**
Il s'agit d'un programme qui vient se greffer sur un autre pour ajouter des fonctionnalités. On peut aussi parler d'extension ou d'add-on.

Dans *Pirate Informatique* n°24 nous avions fait un article complet sur Kodi (ex-XBMC), un Media Center multi plates-formes disposant d'un nombre très important de plugins. Faisons le point sur un de ces derniers : PVR IPTV Simple Client.

Téléchargement, sous-titres, bases de données multimédia, tchat, cloud, Facebook : Kodi est doté de centaines de plugins très intéressants. En un clic (ou une pression de télécommande) il st possible d'ajouter diverses fonctionnalités à ce merveilleux Media Center. Récemment nous avons fait la découverte de PVR IPTV Simple Client. Sur les dernières versions de Kodi (14,15 et XBMC 13), ce dernier permet de profiter de chaînes de télévision françaises ou étrangères. Il suffit d'ajouter le plugin, de trouver ou de se confectionner une liste de chaînes au format «playlist» M3U et de faire son choix. On pourra aussi ajouter des logos pour les chaînes et un affichage de programmation en temps réel (*tiens, le sumo commence à 10*h).

UNE DIFFUSION ALTRUISTE

Ce type de diffusion est possible grâce à certains utilisateurs qui proposent de partager leurs flux personnels avec les internautes, comme pour Sopcast ou Veetle. C'est une solution très sympa pour les étrangers, les polyglottes, les expatriés ou les personnes en vacances. D'autant que pour les chaînes françaises, il ne s'agit pas de piratage si vous payez la redevance ! Bien sûr on trouve des chaînes de sports et là, il faudra jouer le jeu. Regarder la L1 ou la Champion's League sans payer ce n'est pas bien, mais en ce qui concerne les disciplines qui ne sont pas diffusées en France, il n'y a pas mort d'homme. À vous le lacrosse, le curling, les fléchettes ou le cricket !

PAS À PAS

Comment utiliser Kodi PVR IPTV?

CE QU'IL VOUS FAUT

KODI

OÙ LE TROUVER ? : **hhttp://kodi.tv**

DIFFICULTÉ :

Commencez par télécharger la dernière version de Kodi 15 pour votre appareil. Notez que le plugin est disponible pour les versions Windows, Linux, Android et iOS (seulement pour XBMC 13). Si vous avez déjà une version 13 ou 14, pas de problème. En suivant notre lien, trouvez ensuite le plugin adéquat au format ZIP. Choisissez la version 2 du plugin et placez-le localement: sur votre disque si vous utilisez la version Windows ou sur la mémoire de votre Media Center (clé USB, carte SD, mémoire flash interne, etc.)

02 INSTALLATION

Sur Kodi allez dans **System>Settings>Add-ons** et **Install from ZIP file**. Trouvez le chemin vers le fichier contenant le plugin. Il est également possible d'utiliser votre réseau local pour y accéder. Une fois installé, retournez au menu **Add-ons**, ouvrez la liste **Disabled Add-ons** et sélectionnez **PVR Client**. Dans **PVR IPTV Simple Client2**, faites **Enable** et allez dans **Configure**.

Ici, deux solutions s'offrent à vous. Vous pouvez soit trouver un lien **http://** dirigeant vers une liste de chaîne (**Remote Path**) ou alors télécharger votre propre liste pour l'héberger en local (**Local Path**). Dans le premier cas, vous aurez peut-être la chance de trouver un utilisateur qui mettra à jour les chaînes que vous désirez tandis qu'en choisissant la deuxième solution vous pourrez vous faire votre propre liste de chaînes (voir encadré). Dans les deux cas, il faudra utiliser Google pour trouver des liens ou des fichiers M3U.

04 SHOW TIME !

Il faudra ensuite valider et redémarrer Kodi pour que la liste des chaînes se charge en mémoire. Un nouveau menu TV fera son apparition sur l'interface principale du Media Center. D'ici vous aurez accès aux chaînes avec la possibilité de les enregistrer (à condition d'avoir une unité de stockage). Le menu **EPG** permettra d'avoir un affichage de la programmation pour ne rien rater. Il faudra néanmoins installer cette fonctionnalité depuis l'onglet **EPG** de **Configure**.

STRUCTURE D'UN FICHIER .M3U

Pour avoir des chaînes, il faudra télécharger ou se «fabriquer» une liste au format M3U. C'est le format de vos chères playlists musicales. Il est possible d'ouvrir ce type de fichier avec le bloc-note de Windows 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 allez dans n'importe quelle fenêtre de l'explorateur Windows, faites **Organiser>Options des dossiers>Affichage** et décochez **Masquer les extensions des fichiers dont le type est connu**.

#1 Récupérer le son d'un film

avec VLC Media Player

Vous craquez pour la bande-son d'un film enregistré sur votre PC ? Vous désirez récupérer l'audio d'un spectacle comique ? Depuis VLC, déroulez le menu **Média** et choisissez **Convertir/Enregistrer**. Cliquez sur **Ajouter** et sélectionnez le fichier du film, puis faites **Convertir/Enregistrer**. Dans la liste **Profil**, optez pour **Audio (MP3, FLAC...)**. Avant de **Démarrer l'extraction**, veillez à définir un dossier de destination avec **Parcourir**.

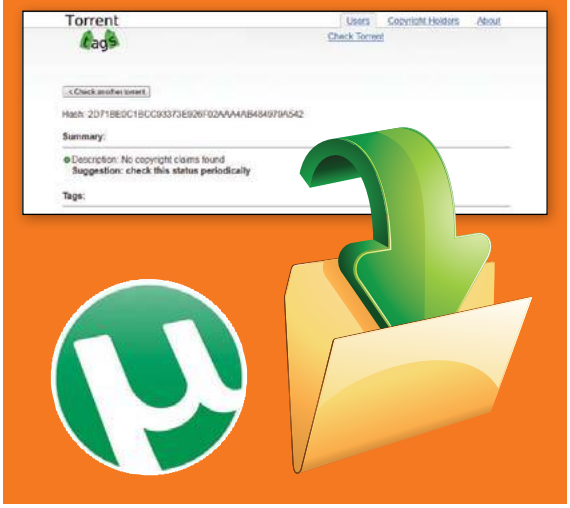
Lien : **www.videolan.org**

#2 Ne piratez plus

avec Torrent Tags

Entre les films indépendants, certains documentaires ou les logiciels libres, il n'est pas tout le temps facile de savoir si tel ou tel fichier .torrent est légal ou pas. Bien sûr lorsqu'il s'agit d'un blockbuster choppé sur Cpasbien.pw ou t411.me, le doute n'est pas permis, mais si vous vous demandez par exemple si vous pouvez télécharger sereinement Steal this Film (un docu sur la propriété intellectuelle), rendez-vous sur TorrentTags.com ! Placez le fichier .torrent ou collez le hash d'identification et faites **Submit**. Si vous voyez une petite pastille verte, c'est que le téléchargement est légal !

Lien : **https://torrenttags.com**

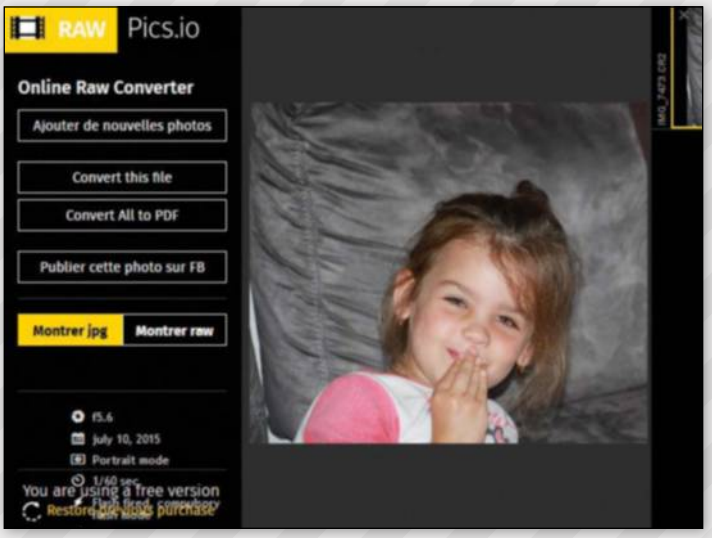


#3 Convertir les fichiers RAW en ligne

avec Rawpics

Le format RAW est un format de photo spécial (même si dans la réalité il existe un type de format par marque : CR2, DNG, etc.) Cette spécification produit des images non compressées, contenant toutes les informations capturées par l'objectif. Pratique pour les modifications, le RAW nécessite un logiciel spécifique aux constructeurs (Canon, Nikon, etc.) pour être lu. Rawpics est un outil de conversion en ligne très simple. Déposez la photo dans la fenêtre prévue à cet effet et récupérez un fichier JPEG.

Lien : **http://raw.pics.io**

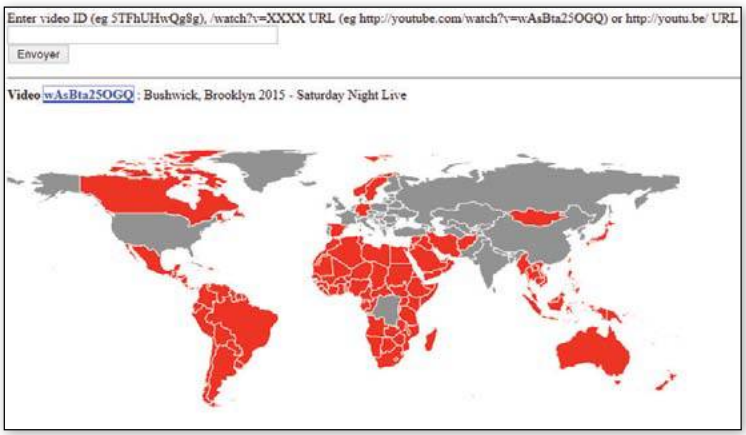


#4 Identifier dans quels pays une vidéo est interdite

avec YouTube Region Restriction Checker

Si vous postez des vidéos sur YouTube, sachez qu'elles ne sont peut-être pas visibles par tous. En collant l'URL d'une vidéo dans la barre de recherche du site YouTube Region Restruction Checker, vous identifiez les pays où elle est autorisée (en gris) et interdite (en rouge). Pratique avant d'utiliser un proxy pour mieux choisir le pays adéquat.

Lien : **http://polsy.org.uk/stuff/ytrestrict.cgi**



#5 Faire pivoter une vidéo

avec Freemake Video Converter

Rien de plus simple que de pivoter une photo de 90 ou 180°, mais lorsqu'il s'agit d'une vidéo la tâche est plus ardue. Il arrive en effet de se tromper de sens lorsque vous capturez une vidéo avec un téléphone. Une fois sur votre TV, PC ou tablette la vidéo est «penchée» et rares sont les lecteurs à proposer une option pour remettre le tout à l'endroit. Pour régler le problème, il faut réencoder la vidéo. Avec le logiciel Freemake Video Converter, allez dans **Video** puis **Edit** (l'icône «ciseaux»). Dans la fenêtre de lecture vous trouverez une icône en forme de flèche vous invitant à pivoter votre vidéo de 90° vers la gauche ou vers la droite. Faite **OK**, choisissez le format de sortie et cliquez sur **Convert**.

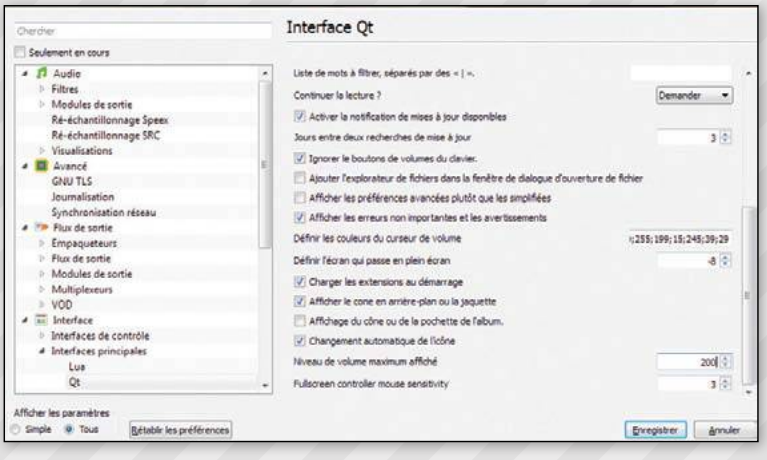
Lien : **http://www.freemake.com/fr**

#6 Pousser le volume à 200%

avec VLC Media Player

Les dernières versions de VLC bloquent le volume maximal d'une vidéo à 125%, au lieu de 200% auparavant. Allez dans **Outils > Préférences**. Tout en bas à gauche, sous **Paramètres**, cochez **Tous**. Cliquez ensuite sur **Interface > Interfaces principales > Qt**. À droite de Niveau de volume maximum affiché, écrivez **200** et validez avec **Enregistrer**.

Lien : **www.videolan.org**

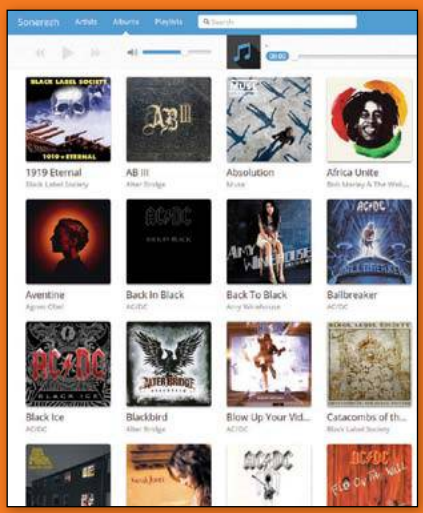


#7 Un cloud musical «maison»

avec Sonorezh

Vous souhaitez héberger vous-même vos fichiers musicaux? Vous disposez d'un serveur et de quelques notions de PHP? Sonorezh propose un service basé sur l'HTML5 et doté d'une interface graphique très jolie et réactive. Le déploiement est assez simple et vous pourrez partager de la musique avec vos proches. Il n'existe pas encore de fonctionnalité mobile ou hors-ligne, mais cela est en cours de développement. Si vous avez besoin d'un coup de main pour l'installation : http://goo.gl/HRdTqX.

Lien : **www.sonerezh.bzh**



X-MATÉRIELS

> Origin Storage DataLocker DL3

Le DataLocker DL3, disponible en version 500 Go, 1To, 1.5To et 2To est un disque dur amovible autoalimenté sur port USB 3.0. Vous l'aurez remarqué, son originalité vient de son écran tactile intégré qui permet de saisir un mot de passe lors d'une connexion pour autoriser l'accès à son contenu. En effet l'appareil propose une double couche de chiffrement AES 256 (modes XTS et CBC). Aucun logiciel particulier n'est à installer pour profiter de cette fonction, toute la partie «cryptage» étant contenue dans le cœur même du disque dur. Certains modèles proposent aussi une double autorisation, par puce RFID puis par mot de passe (d'une longueur de 6 à 32 caractères). Si une personne non autorisée essaye de saisir le mot de passe et qu'il échoue 10 fois, les données seront écrasées. Il est possible de régler le nombre de PC auquel le DataLocker pourra être connecté et de paramétrer un mot de passe utilisateur pour un individu qui n'aura alors qu'un accès limité aux fichiers (lecture seule). Il est aussi possible d'activer une fonction CD virtuel pour monter un ISO depuis le disque dur. Il s'agit bien sûr d'un appareil destiné aux professionnels ou aux utilisateurs qui souhaitent une protection drastique contre le vol de données.

Prix : de **320** à **440 €** (700 € pour le SSD 256 Go) **http://goo.gl/ajzVUO**

Odroid-C1, UN NANO-ORDINATEUR DE PLUS ?

L'Odroid-C1 est un nouveau clone du Raspberry Pi (Model B+) proposé à peu près au même prix, mais contenant des composants beaucoup plus récents. Le processeur est un Amlogic S805 quatre cœurs cadencés à 1,5 GHz et le circuit graphique Mali-450 permet d'afficher de la HD sans problème. Il s'agit donc plus d'un concurrent au Rapsberry Pi 2 (même connectique HDMI, USB et RJ45 10/100/1000) sauf que le système est ici basé, au choix, sur un Android 4.4 ou un Ubuntu 14. Il existe de plus en plus d'appareils de ce type sur le marché, mais si vous êtes à la recherche d'un Media Center très abordable ce Odroid est très intéressant. Notez aussi qu'il peut très bien faire office d'ordinateur d'appoint puisqu'il est possible d'ajouter une horloge RTC et que la connectique permet une utilisation tout terrain...

Prix : **35 €** **www.hardkernel.com**

Diamond 36000N, UNE PORTÉE DE 3 KM !

Vous avez une grande maison ou un large terrain ? Au lieu de prendre deux abonnements à Internet ou d'utiliser des répéteurs WiFi, vous aimeriez peut-être opter pour l'antenne longue portée. Il s'agit d'un adaptateur WiFi sur USB comme on voit partout sauf qu'ici il est couplé avec une petite parabole de 8 cm de diamètre et 2 antennes. Compatible avec la plupart des protocoles (WEP, WPA-TKIP et AES) ce dispositif de 36dBi (les antennes standards sont au alentour de 2 dBi) permet de recevoir un signal à 5 km en terrain dégagé et à 3 km lorsqu'il y a des habitations. L'appareil ne date pas de la dernière pluie, mais il est toujours considéré comme un «must».

Prix : **40 €** **http://goo.gl/50D9Jw**

Wireless Bug Detection, LES MURS ONT DES OREILLES ?

Voici un petit gadget «à la James Bond» comme nous aimons en présenter de temps en temps. Il s'agit d'un détecteur de dispositif d'enregistrement vidéo ou sonore. L'appareil va en fait scanner les ondes de 1 à 8000 MHz et afficher un signal lumineux sur les 10 LED qu'il comporte en façade. Plus de lumières sont allumées et plus vous êtes proche de la source. Il s'agit bien sûr pour des professionnels de lutter contre l'espionnage (industriels, avocats, etc.) et permettre aux particuliers de dormir sur leurs deux oreilles. Attention, si le dispositif d'enregistrement ne fonctionne pas en communicant par les ondes (caméra ou micro avec espace de stockage intégré et placés dans le but d'être récupéré plus tard), l'appareil ne pourra rein détecter du tout.

Prix : **75 €**

www.chinavasion.com/rj4n

NOTRE TEST EXCLUSIF

DataLocker DL3, simple et puissant

Avec sa coque antichocs, ce DataLocker DL3 en impose ! Armée de son authentification à deux niveaux, le modèle que nous avons eu l'opportunité de tester s'est révélé être une très bonne surprise. Non seulement les paramètres de sécurité sont ajustables, mais tout se passe depuis le menu de l'écran tactile : pas de logiciel à installer ou de volume chiffré à monter/démonter. Présentation...

#1 PREMIER CONTACT

Dès que vous aurez branché le disque dur sur un port USB, l'écran tactile s'illuminera et vous proposera de déverrouiller l'accès aux données avec une authentification RFID. Dans notre version de test, l'appareil est en effet fourni avec deux petits porte-clés contenant une puce chacun. Nous vous invitons d'ailleurs à activer les deux puces dans les options et à noter la clé hexadécimale quelque part en cas de perte de ces deux pupuces.

NB : Dans le feu de l'action notre brillant journaliste n'a pas remarqué qu'il était possible de régler la langue sur Français.

#2 LES OPTIONS

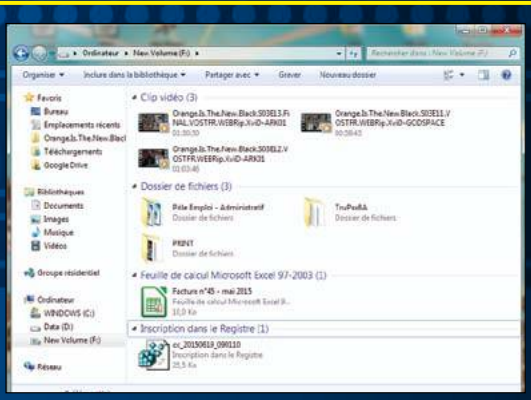
Après l'authentification RFID, le DataLocker vous demandera le mot de passe. D'origine il s'agit de **000000**. Il faudra bien sûr le changer dès la première utilisation. Avant d'autoriser l'accès à votre PC (**Connect**), faites **Setup** pour accéder aux menus et changer le mot de passe. Dans **Strong Password** il est possible de changer la longueur maximum du mot de passe et dans **Virtual CD** vous pouvez activer le mode permettant de configurer le disque dur comme un lecteur virtuel.

#3 LES LIMITATIONS

Toujours dans le **Setup** vous trouverez aussi une option limitant le nombre de PC qui peuvent accéder aux données (**DataLocker Link**). S'il est réglé sur 1, même un utilisateur ayant les codes et la puce ne pourront accéder aux données s'il ne s'agit pas de votre machine. **Zeroize Drive** permet quant à lui d'effacer les données, et de remettre les options d'authentification à 0: mot de passe usine et remise à zéro de la mémoire RFID.

#4 AVEC WINDOWS

Lorsque vous ferez enfin **Connect**, Windows vous préviendra qu'un nouveau volume est disponible. Ce dernier se comportera comme un disque dur externe (sauf en mode **Virtual CD**) et vous pourrez y transférer des fichiers sans avoir à monter un volume chiffré comme c'est le cas avec des solutions logicielles comme VeraCrypt (voir notre précédent numéro)



CD OFFERT

LE PACKAGE DU PIRATE

Tous les logiciels INDISPENSABLES

100% GRATUIT

LE GUIDE PRATIQUE

100% MICRO-FICHES, TRUCS & ASTUCES

SMARTPHONE

Qwant

DNS

PDF protégé ?

RANSOMWARE

KAI LINUX

Télécharger

DÉBRIDEUR

SURVEILLANCE

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

L 12730 - 26 - F: 4,90 € - RD