+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 31

PIRATE [INFORMATIQUE]

100 % PIRATAGE avec CD GRATUIT » BEST-OF LOGICIELS

Le GUIDE du HACKER

[100% TUTOS & ASTUCES]

Windows 10
Kali Linux
Tor
WireShark
Prise de contrôle
Téléchargement
Virtualisation
Anti-surveillance

+ RAINBOWCRACK
Le CRACK des MOTS DE PASSE

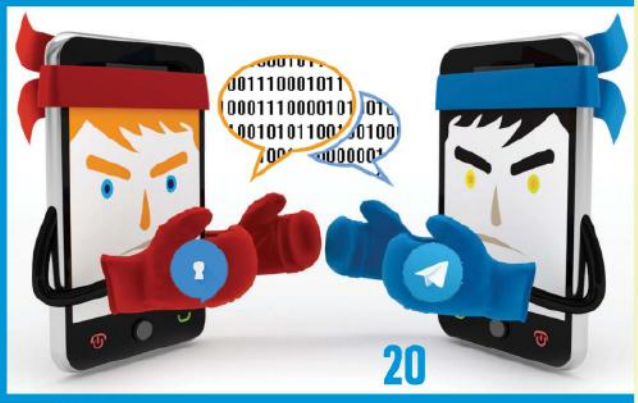
RÉSEAU SOCIAL
PIRATAGES & CLONAGES DE COMPTES FACEBOOK

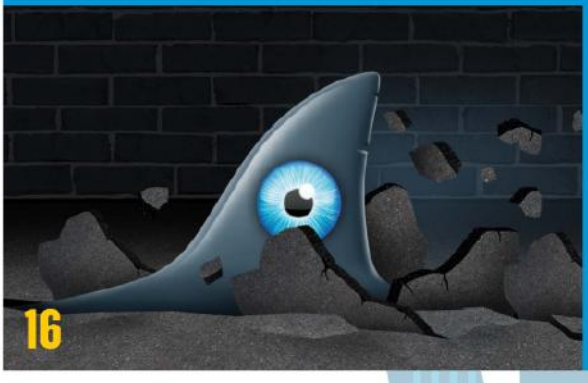
SMARTPHONE
SIGNAL VS TELEGRAM : LE CHOC DES MESSAGERIES CRYPTÉES

PROTECTION
DÉJOUER ET DÉBLOQUER UN RANSOMWARE

SOMMAIRE

PROTECTION/ANONYMAT



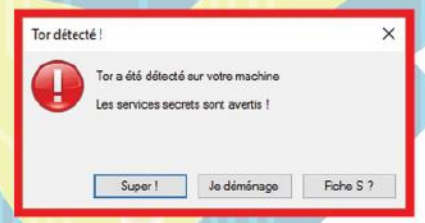


HACKING

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°31 – Nov 2016 - Jan 2017

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

Directeur de la publication :
David Côme
The Dude : Benoît BAILLEUL
Maude, Walter & Donnie : Émilie Lapierre, Yann Peyrot & Michaël Couvret
L'invité surprise : Jonathan Defer
Brandt & Bunny : Sergueï Afanasiuk & Stéphanie Compain
Correctrice :
Virginie Bouillon

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

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

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

ÉDITO

BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Comme vous avez été nombreux à vous intéresser à Tails, nous avons décidé de vous proposer de découvrir un nouvel OS dans ce numéro. Qubes OS n'est certes pas destiné à tout le monde, mais il préfigure peut-être ce qui sera le futur de l'informatique. Ça ne coûte rien d'essayer pas vrai ? Pour ce numéro 31 nous vous présentons aussi les Rainbow Tables : un formidable moyen de gagner du temps lors de la récupération de vos mots de passe ou, pour d'autres, un excellent outil pour vérifier si vos sésames sont bien solides. Comme nous ne mettons pas de côté l'actu, nous avons aussi décidé de faire le point sur les fraudes sur Facebook avec tous les moyens de se protéger d'un piratage ou d'un clonage de compte. Wireshark vous intéresse ? Nous avons déniché un spécialiste de ce logiciel qui reviendra pour un prochain numéro si l'article vous a intéressé. Mais vous le savez, *Pirate Informatique* serait bien démuni sans ses fidèles lecteurs qui, non seulement donnent des idées d'articles, mais envoient carrément des sujets complets à la rédaction. C'est ainsi que pour la première fois en plus de 7 ans, un lecteur apparaît dans l'ours du magazine après nous avoir soumis un papier des plus intéressant : le contournement du sésame de Windows (rien que ça !). Continuez, vous êtes géniaux.

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

BRICE DE NICE 3 CASSE LES PIRATES

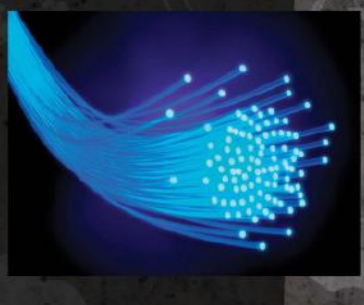
Quand on voit la politique de certaines majors en ce qui concerne le piratage de films, on ne peut que saluer le petit clin d'œil de Gaumont pour la sortie de Brice de Nice 3. À une semaine de la sortie du film, les internautes on en effet eu la surprise de voir débarquer sur YouTube une vidéo qui avait tout l'air d'un screener, un film volé destiné à la presse ou aux professionnels (à ne pas confondre avec un CAM, filmé illégalement dans un cinéma). Tout est là : le titre accrocheur (*film complet VF avec Jean Dujardin*), la qualité pas top, la mention «Propriété de Gaumont», etc. Or au bout de quelques minutes, l'acteur oscarisé habillé en Brice vient se moquer du spectateur : «*T'as cru que t'allais voir tout le film ? C'est même pas le bon début !*». Sans doute la meilleure vanne du surfeur.

USURPER UNE IDENTITÉ ? C'EST SIMPLE COMME UN COUP DE FIL !

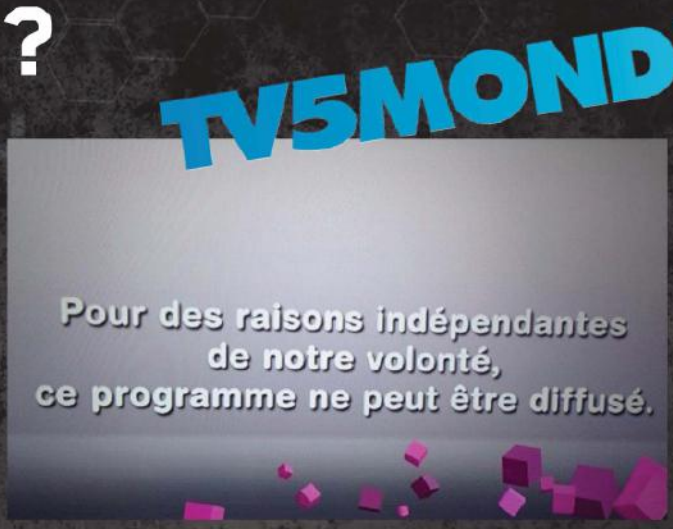
En septembre dernier, le quartier des Halles à Paris a été bouclé à cause de deux petits malins qui ont eu la bonne idée de se faire passer pour un prêtre, soi-disant attaqué dans son église. Bien sûr, sur fond d'attaques terroristes en tout genre, la police prend très au sérieux ce genre d'appels. Mais le problème c'est qu'au moment de vérifier la véracité de l'alerte, la maréchaussée a juste pu constater que le numéro correspondait bien à celui du téléphone fixe de l'église. Bien sûr, nos deux zozos ont été arrêtés après s'être vantés de leurs méfaits sur Facebook. Mais comment des pirates, tellement «expérimentés» qu'ils arrivent à se jouer de la police, se font attraper de cette manière ? Le problème c'est que ce type d'applis pullulent et qu'il n'est pas du tout nécessaire d'avoir un doctorat en mathématique pour les utiliser. La preuve c'est qu'ils sont déjà utilisés par les plates-formes de démarchage : ceux qui appellent avec un 05 ou un 01 alors qu'ils sont en Roumanie ou en Côte d'Ivoire par exemple. Le comble c'est que ce genre d'applications soit disponible facilement ou que nos forces de l'ordre se fassent posséder par des analphabètes de 15 ans équipés d'un téléphone ? Ce ne sont pas des flashballs qu'il faut à vos policiers Monsieur Cazeneuve !

LA NEUTRALITÉ DU NET SAUVÉE (POUR LE MOMENT)

Nous savions déjà que le Parlement européen, proie des lobbies, avait lâché du mou concernant la neutralité du Net. Or l'équivalent européen de l'ARCEP (l'autorité de régulation des télécoms), le BEREC, a dernièrement lancé un signal fort. Non seulement cet organe a demandé l'avis des citoyens, mais devant les quelque 500 000 contributions envoyées, le BEREC a tranché dans le vif : «*Les fournisseurs d'accès à Internet devront traiter tout trafic de la même manière, sans discrimination, restriction ou ingérence*». En bref, l'Internet à deux vitesses ce ne sera pas pour tout de suite. Les données chiffrées ne pourront pas être traitées moins favorablement que le reste et BitTorrent ou YouTube ne pourront pas être bridés à cause de leur consommation élevée de bande passante. Seule ombre au tableau : les données mobiles de certaines applications (Spotify, Netflix, etc.) qui, avec certains partenariats spécifiques, pourront ne pas être décomptées dans le forfait data. Un moindre mal.



TV5 MONDE : UNE ATTAQUE SOUS FAUX DRAPEAU ?



Même si vous n'êtes pas un lecteur assidu, vous n'avez as pu rater l'affaire du piratage de TV 5 Monde. Rappelons quand même que cette chaîne, très populaire à l'étranger auprès des francophones et des Français expatriés, représente le deuxième plus grand réseau mondial de télévision. Or en avril 2015, en plus des piratages des comptes Facebook, Twitter et YouTube de la chaîne, c'est carrément la diffusion des 12 canaux qui a été suspendue (TV 5 Europe, TV5 Afrique, etc.) Nous savons maintenant que cette attaque, préparée plus de 2 mois à l'avance, a été effectuée via une faille Java sur plusieurs ordinateurs disposants de droits étendus. Un simple fichier .vbs du nom de ISIS caché dans un document HTML a ainsi pu déclencher ce désastre en se répandant dans tout le réseau jusqu'à atteindre le serveur qui transmet les vidéos. Selon les indices, très évidents, laissés çà et là, tout portait à croire que l'attaque avait été orchestrée par des cyberdjihadistes.

Une affaire qui sent un peu le bortsch

Retournement de situation en juin dernier où les enquêteurs considèrent maintenant la piste de l'attaque sous faux drapeau. En effet, le code du virus a été tapé sur un clavier cyrillique à des moments correspondant aux fuseaux horaires de Saint-Pétersbourg et Moscou. De plus, le mode opératoire rappelle de précédents faits d'armes imputés au groupe de hacker russe APT28, très actif lorsqu'il s'agit d'ennuyer les ennemis de Voldem... Vladimir Poutine. S'agit-il de représailles au sujet de la non-livraison des deux navires Mistral ou de la position française sur le conflit ukrainien ? Pourquoi faire accuser les barbus alors ? Certains experts pensent même qu'il ne s'agit que d'une sorte d'entraînement pour attaquer une cible plus grosse encore...

CITATION

«Chacun a son idée de ce qu'est le hacking mais pour moi il s'agit de faire en sorte qu'une technologie fasse des trucs pour lesquels elle n'a pas été conçue»

Jeff Moss "Dark Tangent", fondateur de la conférence Defcon

NUMÉRO EXCEPTIONNEL

BEST OF ASTUCES POUR SMARTPHONES & TABLETTES

3,90 € seulement

CHEZ VOTRE MARCHAND DE JOURNAUX

NOUVEAU !

INSCRIVEZ-VOUS GRATUITEMENT !

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

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

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

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

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

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

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

TROIS BONNES RAISONS DE S'INSCRIRE :

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

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

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

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

DAVFI, UHURU, ARMADITO : 3 NOMS POUR UN ÉCHEC À 5 MILLIONS D'€

Souveraineté et informatique ne font pas bon ménage, en tout cas en France. L'antivirus DAVFI, financé en partie par vos impôts est un échec avant même sa sortie. Devenu Uhuru (pour les mobiles) puis Armadito (pour les PC), les changements de noms et d'orientations successives ainsi que les guerres d'ego ont eu raison d'un projet dont nous avions parlé pour la première fois en 2013. Retour sur cette pitoyable histoire dont personne ne parle...

F. Dechelle sur le site NoLimitSecu : *« Notre propos n'est pas de dire aujourd'hui on va révolutionner le monde de l'antivirus. L'ambition c'est d'être un antivirus open source correct [...] qui tienne la route »*. Ça c'est de l'ambition ! On est bien loin des discours de « rupture technologique » des débuts...

DAVFI (pour Démonstrateurs d'Antivirus Français et Internationaux) est à l'origine un projet d'antivirus réalisé par des sociétés françaises à destination des particuliers et des professionnels. Financé à 50 % par le Fonds national pour la Société Numérique dans le cadre du programme des investissements d'avenir, l'idée de départ est de proposer une solution souveraine d'antivirus open source, et donc sans « backdoor » permettant le vol de données par des puissances étrangères. C'est d'ailleurs Jérôme Notin qui nous l'avait expliqué dans une interview parue en 2013 dans notre seul et unique numéro hors-série. Monsieur Notin était à l'époque Président de la société Nov'IT et chef de file du consortium en charge de la bonne conduite des opérations. Nous avions été séduits par ce Monsieur qui avait tout l'air d'être investi par sa mission. Il était d'ailleurs très fier de compter sur le concours d'Eric Filiol. Car l'autre figure du projet initial, c'est Eric Filiol. Docteur en mathématiques appliquées et en informatique, ingénieur en cryptologie, Monsieur Filiol devait fournir le code du projet DAVFI ainsi qu'une équipe d'ingénieurs. Mission accomplie puisque le code est livré en septembre 2014, avec la validation de la DGA (Direction Générale de l'Armement), à la société Nov'IT chargée d'industrialiser le produit.

armadito antivirus

DAVFI

uhuru

Le début des ennuis

La lune de miel est de courte durée entre les deux hommes puisque nous savons de source sûre que très rapidement, les ennuis commencent. Notin n'est pas content du code et Filiol dénonce une phase d'industrialisation lamentable. Bref, ils font n'importe quoi avec son code : logiciel Linux, portage Windows, version Android qui devient en fait un système complet difficilement utilisable par tout un chacun, liberté prise avec le code livré, etc. Le plus beau là-dedans c'est que personne ne demande de comptes à Nov'IT qui cumule les retards, les produits, sans finaliser un seul projet. À ce jour, seule la version Android a été présentée sans pour autant passionner les constructeurs tandis qu'une version Windows devait sortir il y a presque 2 ans. Cerise sur le gâteau, Nov'IT est vendue en 2015 à Teclib. Cette société qui faisait partie du consortium hérite du projet. Depuis, Jérôme Notin ne répond plus directement à nos e-mails et fait suivre les courriers au pôle marketing (?) de Teclib. Le nouveau chef de projet, François Dechelle, n'a quant à lui pas le temps de répondre à nos sollicitations d'interview et nous renvoie vers un podcast soporifique d'une heure enregistré en août 2016 par le site NoLimitSecu. Dans cet enregistrement (nous devrions parler de monologue), Monsieur Dechelle se veut réaliste : « Je ne vais pas vous raconter des histoires, par rapport à l'ambition du projet et aux moyens il y a encore des choses à faire ».

Des bugs et une notion d'open source un peu bancale

Car le code source du projet est public sur Github depuis mai 2016 et déjà les critiques affluent. Premièrement, la communauté ne considère pas le projet comme réellement open source. Le code est bien disponible, mais seulement depuis peu or, pour les plus pointilleux, un projet open source doit être public dès le début du développement. Deuxièmement, une faille critique (possibilité d'exécution de code à distance) a été dévoilée moins d'un mois après la mise en ligne : https://goo.gl/K2v3EA. Sans compter les testeurs qui relèvent un nombre important de faux positifs, une trop forte empreinte mémoire et des crashs... Pendant ce temps, Avast reste l'antivirus préféré des Français, alors qu'on ne sait pas vraiment où sont envoyées les données recueillies. Eric Filiol n'a pas souhaité réagir dans nos colonnes. Il nous a fait part de son « écœurement » et n'a « plus envie de communiquer sur ce qu' [il considère être] une incurie d'État ». Il a depuis créé un fork du projet, OpenDAVFI, qui se veut être fidèle à l'esprit original. Comme il l'explique sur son site : « Produire un antivirus libre et ouvert a toujours été une condition sine qua non en particulier parce qu'il a été financé en partie par le contribuable français qui doit avoir son mot à dire sur la façon dont son argent a été dépensé ». Selon son profil LinkedIn, Jérôme Notin a été bombardé chef de projet à l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et ne répond toujours pas à nos e-mails. Vive la France.

COMPTE FACEBOOK : PIRATAGE ET CLONAGE

Entre les prises de possession d'un compte ou les clonages de profils, tout est bon pour faire de l'argent avec Facebook quand on est un pirate malintentionné. La détresse des victimes est réelle, car on a l'impression d'être dépossédé de toute notre vie. Comment les pirates s'y prennent-ils et comment se protéger ?

Parmi les problèmes de sécurité rencontrés par Facebook, il y a le piratage de compte. Comment font les pirates pour réussir ce tour de force ? Il y a d'abord la technique bien connue du phishing : via e-mail ou depuis un site frauduleux, vous vous retrouvez devant une page Internet qui copie en tout point le design de Facebook. La victime est donc en confiance même s'il suffit de regarder la barre d'adresse pour voir que vous n'êtes pas sur Facebook. Attention, car les pirates regorgent d'astuces pour vous tromper avec des adresses proches (**www.face-book.com**, etc.) ou trompeuses (**www.security-faceb.com**), mais ne vous faites pas avoir : cette page va permettre au pirate de récupérer vos identifiants. Il y a toujours une bonne raison qui alarmera pour rien l'utilisateur peu prudent : « *Votre compte va être effacé si vous ne vous connectez pas depuis cette page* », « *Suite à un piratage/une maintenance, nous avons besoin de vos identifiants pour sécuriser votre compte* », etc. On vous voit sourire d'ici, mais Facebook c'est 1,59 milliard d'utilisateurs dans le monde soit plus de 20 % de la population mondiale. Vous pensez que ce sont tous des gens sensibles à la sécurité informatique ?

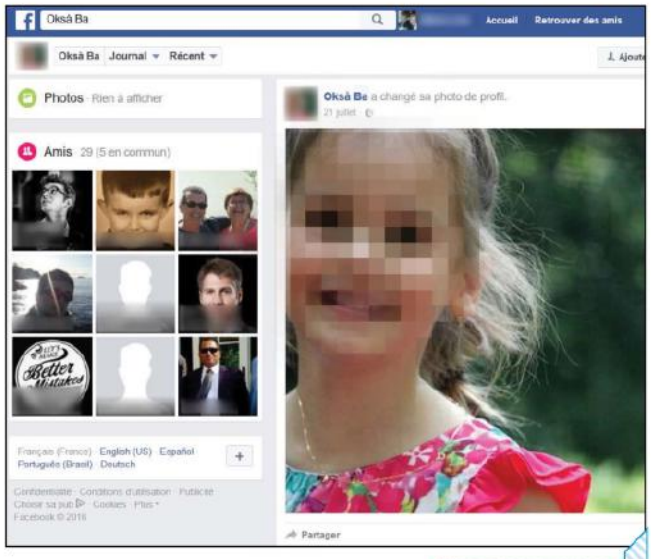
UN MOT DE PASSE UNIQUE !

Il existe aussi un autre problème qui ne touche pas que Facebook : l'utilisation du même mot de passe par les Internautes. Même si de plus en plus d'utilisateurs savent qu'il faut choisir un mot de passe solide, ne figurant dans aucun dictionnaire et mêlant chiffres, minuscules, capitales et caractères spéciaux, il est fréquent qu'une personne utilise le même (ou une version légèrement modifiée) pour tous les sites qu'il va fréquenter. Alors bien sûr, Facebook protège les sésames de ses utilisateurs comme le rédacteur en chef protège sa réserve de single malt, mais qu'en est-il des autres sites moins connus et avec peu de moyens ? Imaginons que votre mot de passe Facebook soit le même que celui que vous avez utilisé pour les sites **www.apprends-le-tricot.fr** et **www.le-gluten-c-le-mal.org**. Si ces sites sont mal sécurisés, ou pire, qu'ils ne stockent pas les sésames sous forme hashée, c'est la fin des haricots. Un hacker ira cracker le mot de passe (il n'aura peut-être même pas besoin de le faire s'ils sont « en clair ») et tenter des connexions avec le même identifiant et le même mot de passe sur les sites les plus populaires : Facebook et Gmail en tête. Heureusement, il existe la double identification pour se protéger (voir après),

mais encore une fois, on imagine mal mamy Denise activer cette option toute seule. Voilà comment on peut se faire voler son compte en quelques minutes. Mais cela demande un peu de technique. Quand on est nul, pourquoi pirater un compte quand on peut le cloner ?

LA GUERRE DES CLONES

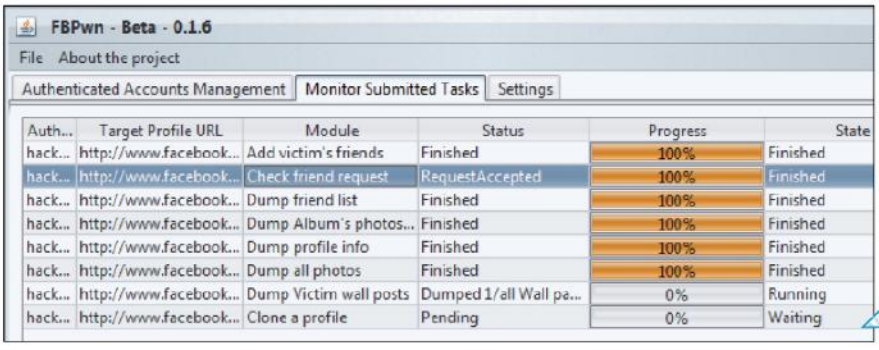
Pour un utilisateur, le clonage est un peu moins grave, mais il est aussi plus répandu, car plus facile pour le malandrin de service. Il s'agit de copier complètement un profil puis de faire basculer les amis de la victime avec un message du genre « mon compte Facebook a été piraté/effacé/disparu dans la 4e dimension, ceci est mon nouveau compte, ajoute-moi ». Pour ce faire, il existe des logiciels clé en main qui peuvent télécharger l'intégralité d'un compte « ami ». Si un de vos contacts sur Facebook s'est fait pirater, vous pouvez en être facilement victime. Dernièrement, un lecteur a eu ce problème et ce sont presque la moitié de ses amis qui se sont fait avoir. Comme Facebook refuse les mêmes noms de profil, la différence entre le compte cloné et le vrai se situe au niveau des accents ou autres petits détails de typographie. Pire, le compte de notre lecteur a été banni de Facebook ! En effet, les complices ou autres faux comptes du brigand vont alors signaler le vrai compte comme étant frauduleux ! Notre pauvre lecteur a donc dû montrer patte blanche et envoyé un scan de sa carte d'identité. Il a fallu un bon mois à Facebook pour régler le problème. Il aurait été pourtant facile de regarder la date de création des deux comptes pour reconnaître le vrai du faux, mais ce sont apparemment des robots qui prennent en charge une partie de ces requêtes...



Voici le compte cloné de notre lectrice avec une photo, volée, de sa fille en profil. La différence avec le vrai compte : un « à » au lieu d'un « a » dans son nom. Rien d'alarmant pour ses amis puisque le pirate explique qu'elle a dû créer un nouveau compte à cause d'un piratage. Un comble.

UN SEUL BUT : L'ARGENT !

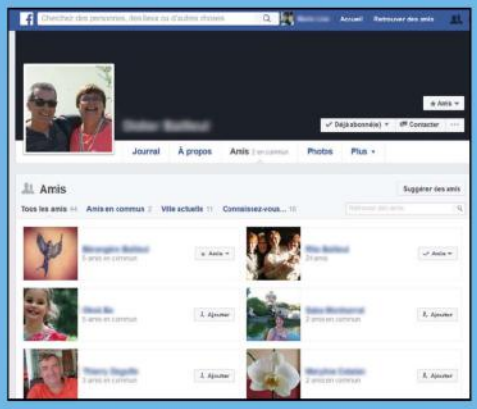
Ces attaques ont bien sûr le même but : qu'il s'agisse de piratage de compte ou de clonage, c'est l'argent qui motive les pirates ! Dès qu'un compte est piraté ou cloné, les amis de la victime sont sollicités pour différentes choses « *Je suis bloqué sans papier à Abidjan, tu te rappelles je t'avais dit que j'y serai ? Envoie-moi un mandat, je t'en prie* », ou la dernière mode en date est l'arnaque au numéro surtaxé : « *Je viens de bloquer mon téléphone si tu peux m'aider, il faut appeler ce numéro gratuit pour obtenir les codes de déblocage, mais je n'ai pas accès à un autre téléphone que le mien* ». Bien sûr, ce numéro est surtaxé et en pensant bien faire ce sont peut-être 4 ou 5 amis de votre liste qui paieront 3 ou 4 € chacun. Imaginez qu'un pirate fasse de même avec 20 comptes clonés par jour...



FBPwn, même s'il est un peu dépassé maintenant, fait partie de ces logiciels qui peuvent pomper l'intégralité des comptes Facebook pour le cloner. Depuis 2012, d'autres ont pris la relève...

COMMENT ÉVITER LES PIÈGES DE FACEBOOK ?

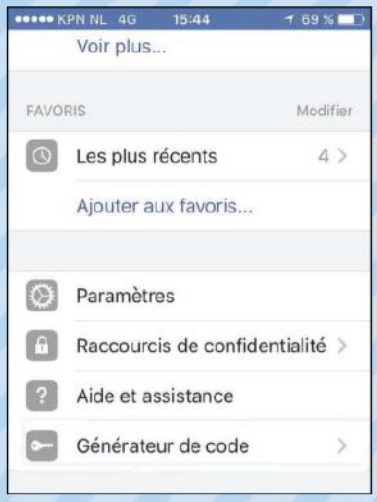
1 PRÉVENEZ LE CLONAGE DE COMPTE



Choisissez bien vos amis et supprimez ceux que vous avez ajoutés uniquement parce que X ou Y les connaît. Ces comptes ont pu être piratés. Si vous êtes victime, la première chose à faire est de poster un avertissement sur votre journal (ou «timelime») et d'envoyer des SMS à vos amis les plus proches et les moins sensibles au problème de sécurité. Le but est bien sûr d'éviter que vos amis ne quittent votre profil pour devenir amis avec le brigand. Demandez-leur de bloquer les invitations de cette personne et de signaler le compte comme étant un faux en suivant ce lien: **https://goo.gl/6UHCMT.**

2 OPTEZ POUR LA DOUBLE AUTHENTIFICATION

La double authentification va prévenir le piratage et pas le clonage. Il s'agit en fait de recevoir un code par SMS ou directement sur l'application de votre téléphone portable pour valider les changements de mots de passe et autres manipulations délicates. Sur Facebook, cliquez sur la petite flèche vers le bas en haut à droite puis allez dans **Paramètres > Sécurité > Générateur de code**, puis sur le lien **Activer le générateur de code**. Sur votre application smartphone, touchez le bouton **Menu** en bas à droite et trouvez l'option **Générateur de code**. Sur votre ordinateur, cliquez sur **Continuer** et entrez le code qui s'affiche sur votre téléphone. Vous devrez refaire cette manipulation avec tous les autres appareils que vous utilisez pour Facebook.



3 RÉGLEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ

Dans **Paramètres et outils de confidentialité** (ou depuis votre assistant de confidentialité), regardez de plus près vos réglages. Votre liste d'amis ne doit pas être publique puisque le cloneur va l'utiliser pour les contacter après vous avoir bloqué. Dressez aussi une liste d'**Amis proches** et faites en sorte que seuls ces derniers puissent voir vos publications (vous pourrez donc accepter un nouvel ami sans craindre qu'il soit un pirate). Suivez ce lien pour savoir comment faire: **https://goo.gl/sN5aeT.**

4 ATTENTION AUX IDENTIFIANTS

Comme nous vous l'avons expliqué précédemment, vos identifiants (couple nom d'utilisateur/mot de passe) sont précieux. Facebook ne vous demandera jamais de les saisir depuis un formulaire par e-mail. Le seul cas où vous devrez entrer votre sésame, c'est lors d'une nouvelle connexion ou lors d'un changement de mot de passe que vous aurez demandé. Choisissez un mot de passe solide et changez-le tous les 6 mois. N'oubliez pas non plus de vous déconnecter si vous êtes sur un ordinateur qui n'est pas le vôtre.

LES DOSSIERS DU

Pirate

DES **DOSSIERS THÉMATIQUES COMPLETS**

À DÉCOUVRIR EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ D'ASTUCES

100% Windows

Actuellement #Guide pratique

LE GUIDE PRATIQUE DE L'ANONYMAT

LES RANSOMWARES DE PLUS EN PLUS POPULAIRES

PAYE 300 € OU SINON...

Dans notre numéro 26, nous vous mettions en garde contre les ransomwares, ces virus qui prennent en otage vos données les plus chères. Force est de constater que ce type d'attaque a le vent en poupe, mais heureusement, les éditeurs d'antivirus prennent très au sérieux cette nouvelle menace...

Dans un rapport de juillet 2016, Symantec indique qu'entre janvier 2015 et avril 2016, environ 43 % des victimes de ransomware étaient des employés d'entreprises. Même si la France ne fait pas partie des pays les plus touchés (USA, Italie et Japon sur le podium), de plus en plus de personnes sont contaminées par ce genre de malware. CryptoWall a causé à lui seul un préjudice de près de 325 millions de dollars, selon la Cyber Threat Alliance. Pourquoi jouer les « gagne-petit » avec du phishing ou se lancer dans un scam nigérian de longue haleine quand on peut demander d'un coup 200, 300 ou 800 € à une maman qui fera tout pour récupérer les photos de ses enfants ?

LE «CRYPTO SHERIFF» EST DANS LA PLACE

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

Dans la saison 2 de la série TV Mr. Robot, le groupe de hacker fsociety contamine une banque avec un ransomware de leur cru. De la fiction? Pas tant que ça! L'année dernière, des pirates demandaient 3 millions de dollars pour ne pas révéler des détails concernant les clients d'une grande banque des Émirats Arabes Unis. De même, l'idée du saboteur (le «gars de l'informatique» qui travaille à la banque est aussi un membre de la fsociety) rappelle l'infection de Stuxnet en 2010... La réalité rattrape même la fiction puisqu'un nouveau ransomware appelé fsociety a dernièrement vu le jour.

LEXIQUE

***RANSOMWARE :** C'est un malware qui sera introduit par un ver informatique. Le ransomware va cibler les types de fichiers ayant une valeur sentimentale ou pratique (photo, vidéo, DOC, XLS, etc.) et les chiffrer avec une double clé très solide (RSA 2048 bits). Au bout de quelques minutes, vos fichiers deviennent inaccessibles et un message s'affiche sur votre écran. Ce dernier vous invite à payer une somme d'argent pour récupérer la clé privée ayant servi au chiffrement et ainsi retrouver vos données.

PAS À PAS

Les fonctionnalités de No More Ransom

CE QU'IL VOUS FAUT

NO MORE RANSOM

OÙ LE TROUVER ? :
www.nomoreransom.org

DIFFICULTÉ :

01 L'ANALYSE

Si vous avez été contaminé par un ransomware et que vous avez gardé vos fichiers, nous allons les uploader sur le site pour savoir s'il existe une solution. Il peut s'agir d'un fichier chiffré contre votre gré (une photo par exemple) ou les «notices» qui vous expliquent comment payer les malfrats (qui se trouvent souvent en vrac dans C:). Cliquez sur **Choose first file from PC** et éventuellement sur **Choose second file from PC** pour en ajouter un deuxième.

02 LA LOTERIE !

Dans notre cas, pas de chance, il s'agit de CryptoWall 3.0 un ransomware qui est pour l'instant hermétique à tous les outils de déchiffrement. Le site vous propose de faire une sauvegarde de vos fichiers inutilisables en attendant une éventuelle solution dans le futur.

03 UNE SOLUTION ?

Si vous avez de la chance, le site vous dirigera vers les 7 logiciels permettant de déchiffrer pas loin de 25 ransomwares et leurs variantes. Pour chaque cas, il suffira d'installer le programme et de suivre les instructions pour récupérer vos précieux fichiers.

02 NE FAITES PAS LE 17 MAIS...

Si ce n'est pas déjà fait, vous pouvez aussi vous signaler à la police. Suivez le lien **Report a crime** après votre analyse puis, depuis le site d'Europol, choisissez **France**. Vous pourrez déposer une préplainte ou signaler le problème à la plate-forme Pharos qui gère les cybercrimes.

LES 4 COMMANDEMENTS DU RANSOMWARE

1/ Faites des sauvegardes régulièrement sur un disque dur externe qui n'est pas branché à votre PC en permanence.

2/ Mettez votre Windows et votre antivirus à jour et ne croyez pas le vendeur de chez Auchan (oui Jean-Pierre, on parle de toi) qui vous racontera qu'un antivirus gratuit n'est pas un antivirus.

3/ Désinfectez comme il se doit votre PC. L'éradication du ransomware ne vous rendra pas vos fichiers, mais vous limiterez les dégâts.

4/ Ne payez pas ! Gardez vos fichiers cryptés par le ransomware, car les éditeurs d'antivirus pourront trouver une solution plus tard. De même, la police arrête parfois les malfaiteurs et réussit à récupérer les clés de chiffrement.

WIRESHARK

POUR INTERCEPTER LES MOTS DE PASSE

Connaissez-vous exactement les informations qui sortent de votre ordinateur lorsqu'il est connecté à Internet ? Savez-vous quel est le degré de protection de ces informations ? Wireshark est là pour répondre à ces questions. Et vous allez voir que vos mots de passe ou vos mails ne sont pas si bien protégés que cela.

Wireshark, c'est fort, très fort. Ce logiciel sous Windows ou Linux est capable d'analyser tous les paquets qui transitent sur votre réseau. Qu'il s'agisse d'un réseau domestique (une box et plusieurs appareils reliés en Wi-Fi et /ou câble Ethernet) ou professionnel (appareils reliés via hub, switch, router, etc.). Pour communiquer sur un réseau et donc sur le Web, votre ordinateur utilise des protocoles. Ces protocoles sont normés afin que votre machine puisse se faire comprendre des autres appareils. Vos informations sont donc encapsulées dans des paquets, plus ou moins sécurisés et plus ou moins complexes à traduire. Ces paquets transitent bien évidemment de manière invisible pour l'utilisateur. Wireshark, lui, intercepte ces paquets d'informations et les analyse. Il est capable de vous dire qui les a envoyés, à qui ils sont destinés, ce qu'ils contiennent et quel est le protocole utilisé.

Au premier abord, ces informations sont assez indigestes. Il s'agit de nombreuses lignes de chiffres et de lettres pas très explicites. Afin de comprendre et traduire ces données, vous devrez avant tout savoir ce que vous cherchez.

À QUOI SERT WIRESHARK ?

Car Wireshark possède une multitude d'applications. La première, c'est d'établir un audit du réseau, c'est pour ça qu'il a été créé. Lorsque vous êtes connecté à un réseau (Intranet, réseau local, Internet, etc.), vous n'êtes pas le seul à envoyer et recevoir des données, votre ordinateur le fait aussi et notamment vos logiciels. Savez-vous quelles sont les informations récupérées par Microsoft, Google ou même ce dernier petit logiciel gratuit que vous avez déniché ? Bien sûr que non. Avec Wireshark vous pourrez le savoir.

L'autre application qui en découle, c'est la recherche d'un cheval de Troie sur un réseau. Les malwares savent se cacher et même les antivirus peuvent avoir du mal à les déloger. La petite astuce consiste à étudier le trafic sortant et voir s'il n'y a pas un programme suspect qui enverrait des paquets suspects vers des serveurs suspects.

Enfin, et c'est peut-être ce qui vous intéresse le plus, Wireshark va vous aider à dresser un audit de vos connexions. En fouillant dans les paquets qui sont envoyés depuis votre ordinateur, vous allez découvrir que certains mots de passe ne sont pas chiffrés (cf. notre tutoriel), de même

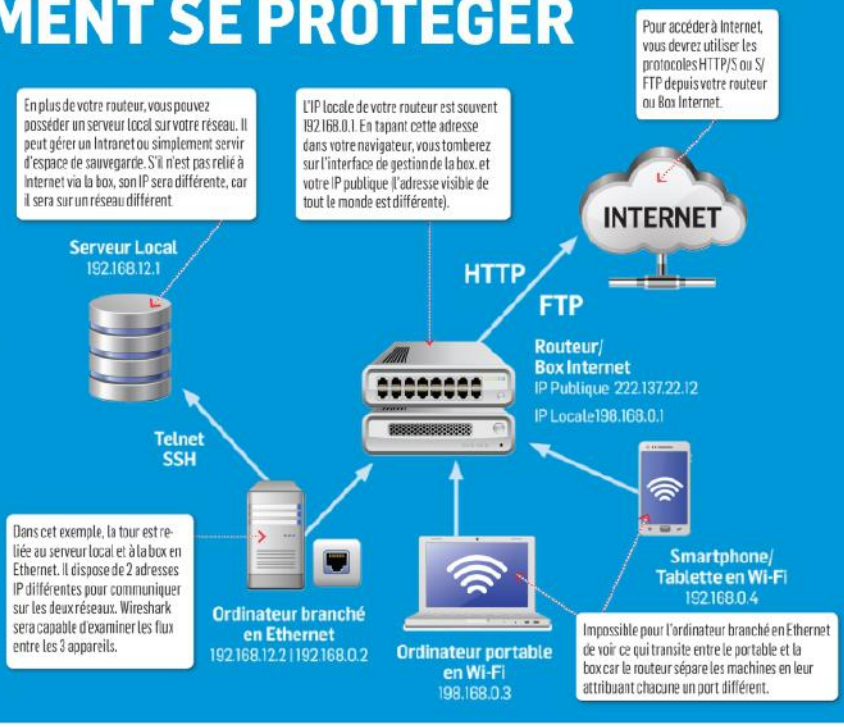
LEXIQUE

***SNIFFER :**
Un anglicisme pour l'action d'analyser les paquets d'informations qui transitent sur un réseau.

***MAN-IN-THE-MIDDLE :**
Il s'agit d'une technique consistant à intercepter des informations circulant sur un réseau sans que personne ne se doute d'une mise en écoute.

COMMENT SE PROTÉGER

Comme d'habitude, la méthode la plus efficace pour se protéger reste le bon sens. Si Wireshark vous permet de déchiffrer facilement les paquets des protocoles les plus populaires. Il ne peut rien face au chiffrement. Le SSL est donc votre meilleur allié. Optez le plus souvent possible pour des sites offrant une connexion sécurisée **HTTPS**, surtout ceux qui demandent un mot de passe. Concernant le FTP, configurez votre client pour utiliser une sécurité. Si votre serveur n'est pas compatible, sachez que FileZilla par exemple, propose un **SFTP** (SSH File Transfer Protocole). Enfin, préférez **SSH** à Telnet si vous bossez sur des serveurs UNIX, mais ça, c'est la base...



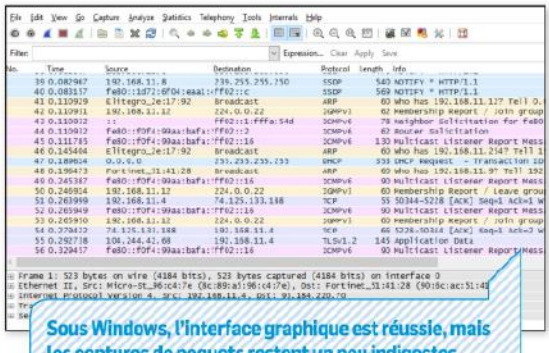
que certains mails. En effet, les protocoles HTTP, FTP et Telnet, pour ne citer qu'eux, ne sont pas chiffrés et ne protègent donc pas les données échangées. Il est donc potentiellement possible d'accéder à tous les mots de passe des sites dont l'adresse commence par HTTP ainsi qu'aux mots de passe des connexions vers un serveur FTP. De même, les services de mail en ligne qui utilisent HTTP permettent aux utilisateurs de Wireshark d'accéder au contenu des conversations. Ceci n'est pas la vocation première de Wireshark, mais nous vous conseillons d'essayer de retrouver vos mots de passe afin de savoir si, oui ou non, ils sont bien protégés lorsque vous naviguez sur le Web ou sur un réseau privé.

QUEL EST LE DANGER ?

Si vous arrivez à intercepter vos mots de passe, sachez que d'autres pourront le faire également. Même si ce n'est pas si simple que cela. En effet, lorsque vous faites tourner Wireshark sur un ordinateur, vous ne pourrez analyser que le trafic relatif à cet appareil. Impossible donc d'intercepter les mots de passe des autres ordinateurs du réseau. Pour faire simple, c'est comme si vous preniez l'avion entre Paris et Madrid et que vous aimeriez savoir quel temps il fait à Oslo. Cependant, il y a des cas de figure qui permettent d'accéder à ces données sensibles et donc de savoir quel temps il fait à Oslo...

Le premier, c'est le cas de l'homme du milieu. L'attaque Man-in-the-middle permet à un hacker de s'introduire sur un réseau et de se positionner entre votre poste et le routeur/switch. Il est donc capable d'analyser les paquets d'informations qui partent de votre ordinateur vers le Web. L'autre scénario catastrophe, c'est le cas où le hacker a réussi à installer Wireshark sur le serveur que vous interrogez ou sur un switch. L'exemple le plus concret, ce sont les points d'accès Wi-Fi. Vous êtes à la gare ou dans un restaurant de malbouffe et vous vous connectez au premier réseau Wi-Fi que vous trouvez. Malheureusement, c'est un Honey Pot installé sur la machine d'un hacker. Il intercepte alors tous les paquets sortant de votre ordinateur et peut les analyser avec Wireshark. Danger.

Wireshark est un outil très puissant, relativement facile d'accès qui vous permettra de vous rendre rapidement compte de ce qui sort de votre ordinateur. N'espérez pas récupérer les mots de passe des autres membres de la famille ou du réseau, ce n'est pas le but de Wireshark. Wireshark est un outil pédagogique qui vous aidera d'abord à mieux vous protéger.



Sous Windows, l'interface graphique est réussie, mais les captures de paquets restent un peu indigestes.

PAS À PAS

Comment sniffer un mot de passe ?

CE QU'IL VOUS FAUT

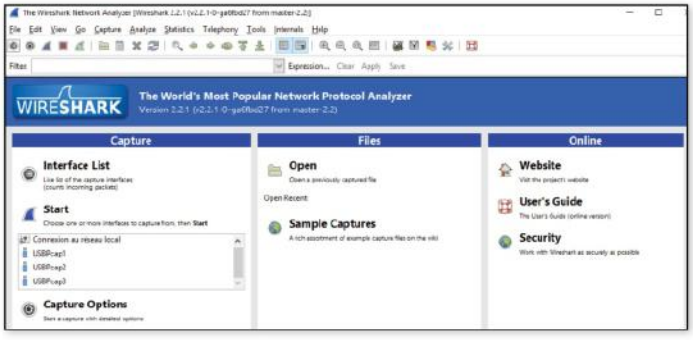
WIRESHARK

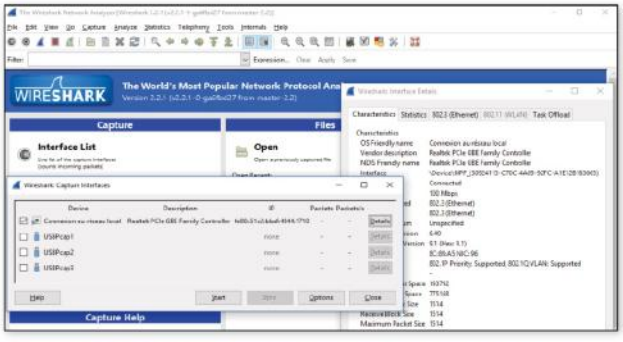
OÙ LE TROUVER ? : **https://goo.gl/hRNFXo**

DIFFICULTÉ : ☠☠☠

01 INSTALLATION

Le processus d'installation de Wireshark est très simple. Si vous êtes sous Windows, veillez à bien faire l'installation de Winpcap proposée également. Ceci permet d'installer les fichiers .dll nécessaires à la capture des paquets. Redémarrez votre ordinateur et lancez Wireshark. Vous êtes maintenant prêt à démarrer une capture de paquets. Notez que Kali Linux intègre de base ce logiciel.



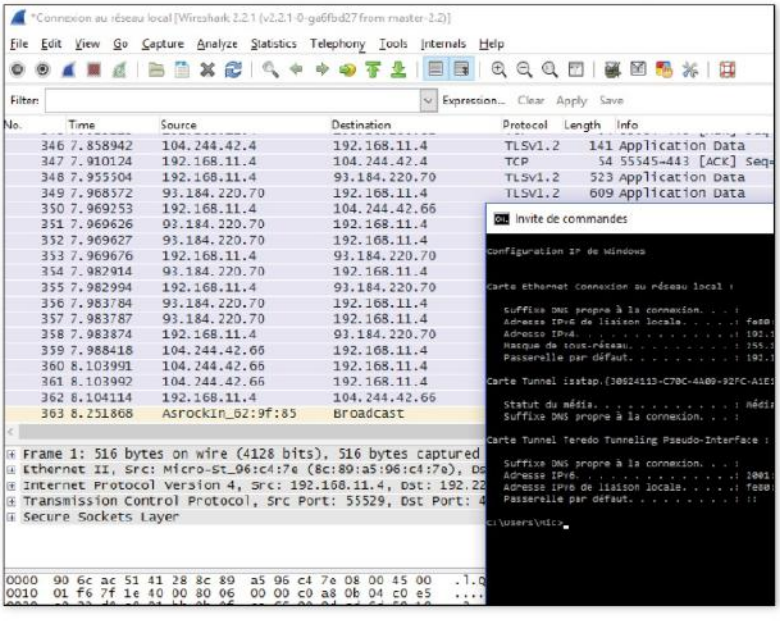


02 DÉMARRER UNE CAPTURE

Lors de chaque démarrage, Wireshark va vous demander de choisir une interface. Comprenez qu'il vous demande de choisir, quel périphérique réseau il doit observer. Si vous avez plusieurs cartes réseau, vous devrez faire votre choix ici. Vous avez 3 options pour sélectionner l'interface. Soit dans le menu **Interface List**, soit dans l'encadré sous le bouton **Start**, soit dans le menu déroulant de **Capture Options**. Tous les chemins mènent à Rome.

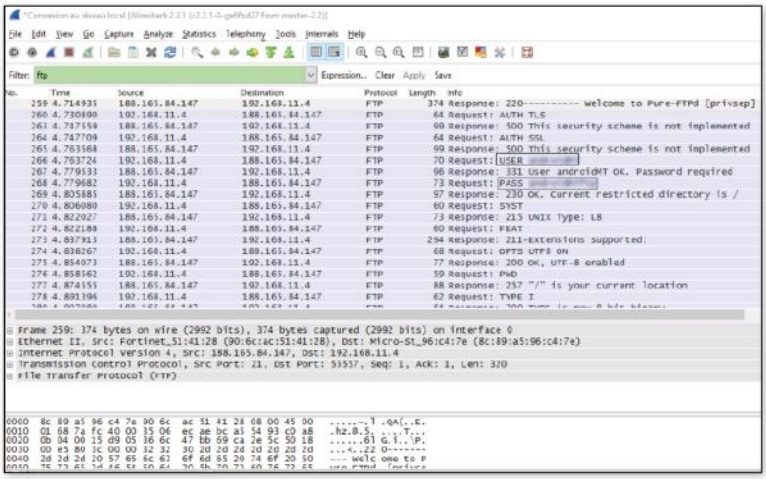
03 RETROUVER UN MOT DE PASSE FTP (1/2)

Une fois l'interface sélectionnée, cliquez sur le bouton **Start** pour lancer la capture de paquets. Vous allez alors voir apparaître des lignes et des lignes de données. Connectez vous ensuite à un site via un client FTP (ici FileZilla) et stoppez la capture. Avant d'aller à la recherche du mot de passe, vous devez connaître le nom de votre machine sur le réseau. Ouvrez l'**Invite de commandes** de Windows (tapez cmd dans la barre de Cortana). Entrez ensuite **IPCONFIG** et appuyez sur la touche **Entrée**. Récupérez les 4 nombres en face de **Adresse Ipv4**. Ici: 192.168.11.4.



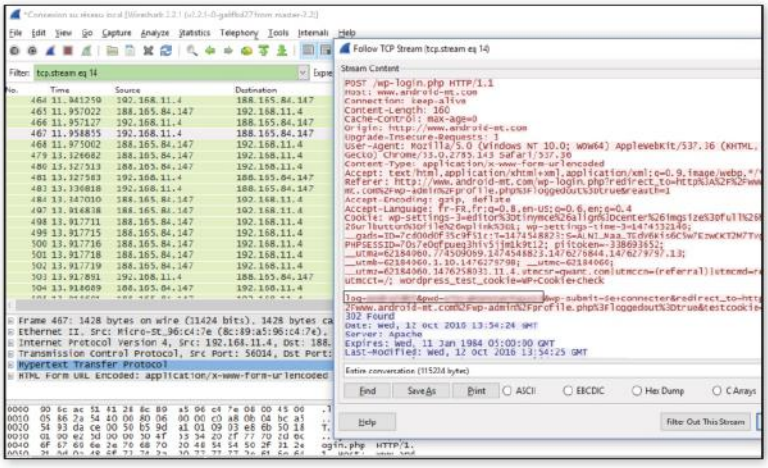
04 RETROUVER UN MOT DE PASSE FTP (2/2)

Le plus simple pour retrouver les paquets qui vous intéressent, c'est d'utiliser l'outil de filtre. Allez dans la barre **Filter** et tapez **FTP**. Vous allez voir apparaître les paquets uniquement concernés par ce protocole. Dans la colonne **Source** de votre première ligne, vous devez retrouver le serveur distant. Dans la colonne **Destination**, votre adresse IP, ici: 192.168.11.4. Vous verrez ensuite qu'un dialogue s'est instauré entre les deux machines. Dans la colonne **Info**, vous aurez la (mauvaise) surprise de voir que vos identifiants et mots de passe apparaissent en clair.



05 RETROUVER UN MOT DE PASSE WORDPRESS

Pour retrouver un mot de passe sur un site Web, le procédé est sensiblement identique. Lancez la capture et connectez-vous sur un site, ici un Wordpress. Filtrer le protocole HTTP peut ne pas suffire à cause du trop grand nombre de résultats. Il faut un filtre plus efficace. Tapez l'expression suivante: **ip.src==192.168.11.4 and ip.dst==XXX.XXX.XX.XX**. Vous cherchez les résultats qui concernent votre machine en source et le serveur du site en machine distante. Faites ensuite un clic droit sur la première ligne et choisissez **Follow TCP Stream**. Surprise, vous allez voir que les identifiants apparaissent en clair...



LES 5 MEILLEURS FILTRES

Voici une sélection de filtres qui vous aideront à trouver votre bonheur dans les résultats de Wireshark.

ip.addr == XX.XX.XX.X: pour sélectionner les résultats concernant une adresse IP.

ip.src==XX.XX.XX.X and ip.dst==XX.XX.XX.X: pour sélectionner un dialogue entre deux machines spécifiques

tcp contains facebook/gmail/twitter: pour accéder aux paquets concernant un site en particulier.

tcp.analysis.flags: permet de faire ressortir les trames ayant été marquées comme problématiques. Pratique vous vérifier l'intégrité d'un réseau.

http.response.code==404: pour analyser les éventuels problèmes de connexions vers un site.

SIGNAL VS TELEGRAM

Depuis les attentats sur le sol français et ailleurs, on entend beaucoup parler de Telegram et un peu moins de Signal. Pourtant, ces deux applications mobiles sont au centre de plusieurs débats idéologiques : lutte contre la surveillance opposée à la lutte contre le terrorisme et, plus confidentiellement, code ouvert contre code fermé.

Dans notre numéro 29, nous avions fait un comparatif des meilleures solutions de tchat privé et anonyme avec le point commun d'être tous au moins sous Windows. Mais comme de nombreux lecteurs nous l'ont signalé, le tchat est de plus en plus utilisé sur mobile. Cela tombe bien puisque les deux solutions qui s'affrontent en ce moment sont disponibles sur iOS et Android. Cerise sur le gâteau, Signal qui ne disposait pas d'interface pour ordinateur, s'est doté d'une solution Web. Faisons l'historique de ces deux applications et distribuons les bons points....

SIGNAL, LE CHOUCHOU DE SNOWDEN

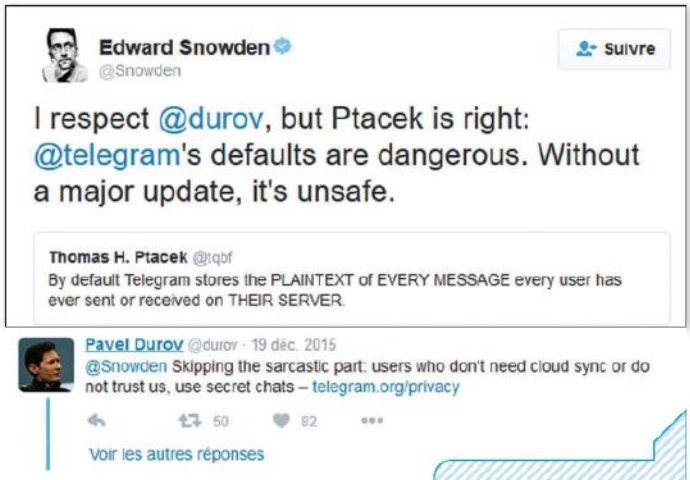
Signal Private Messenger est issu de l'application TextSecure (qui a donné naissance à SMS Secure puis Silence lorsque Open Whisper Systems a abandonné la possibilité de chiffrer les SMS). Disponible sur iOS et Android, Signal est une appli adoubée par l'ami Snowden lui-même. Gratuite, sans pub et open source, difficile de faire mieux que cette dernière. Signal propose pourtant d'activer la conversation téléphonique à la manière de WhatsApp. On note aussi la possibilité

LEXIQUE

***CHIFFREMENT BOUT EN BOUT :**
Le chiffrement (message, pièce jointe, etc.) est réalisé localement sur l'appareil qui le est seul à détenir la clé privée. Le serveur qui relaye l'information est donc totalement aveugle.

***BACKDOOR :**
Ou « porte dérobée » en français. Il s'agit d'une faille sciemment laissée dans un logiciel pour donner un accès spécial à celui qui l'a laissé. Avec un code source fermé, impossible de savoir si un logiciel ne laisse pas en clair vos informations à une entité gouvernementale ou des pirates.

d'importer les SMS pour envoyer des textos depuis la même interface, mais attention, ces derniers ne seront pas chiffrés. Et c'est justement ce qui nous intéresse ici, puisque Signal propose un chiffrement de bout en bout. Pour ce type de protection, impossible pour l'utilisateur de commencer une conversation sur un appareil (mobile) pour la finir sur un autre (ordinateur) et vice-versa. Pour plus de portabilité, les développeurs de Signal ont tout de même pensé à une solution. Il faudra passer par une extension du navigateur Chrome que l'on associera au téléphone pour profiter du bout en bout sur votre PC/Mac (voir notre prise en main).



TELEGRAM, LE CONTROVERSÉ

Pointée du doigt pour avoir le malheur d'être utilisée par des djihadistes, Telegram est une application de tchat pour mobile et ordinateur. Lorsqu'on installe Signal et Telegram, on se rend compte que les applis sont très similaires : la création d'un compte se fait à la manière de WhatsApp avec une vérification par numéro de téléphone. Si vos contacts téléphoniques disposent de Telegram ou de Signal vous serez alors aussitôt au courant. Telegram ne propose pas de conversation téléphonique, mais, comme son concurrent, il intègre un chiffrement de bout en bout. Le problème, que relèveront les anti-Telegram, est que cette fonctionnalité n'est pas activée par défaut. Il faut en effet aller dans le menu, puis faire New Secret Chat pour

Snowden a dénoncé le fait que Telegram ne propose pas le chiffrement par défaut et que les messages sont donc quelque part en clair sur les serveurs. Bien sûr, cela n'a pas plu à Durov qui a juste commenté « *Ceux qui n'ont pas besoin de synchronisation sur plusieurs appareils ou ceux qui ne nous font pas confiance peuvent utiliser le tchat secret* ». Snowden est revenu sur ses déclarations (les messages ne sont pas « en clair » sur les serveurs), mais le débat a longtemps été animé entre le whistleblower invité de Moscou et le Russe, qui a préféré fuir son pays.

	SIGNAL	TELEGRAM
Chiffrement	Curve25519 + AES 256 bits et HMAC-SHA256	AES 256 bits + RSA 2048 bits avec un échange de clé Diffie–Hellman
SMS	Oui (peut remplacer l'appli SMS par défaut sous Android, mais sans chiffrement)	Oui (propose d'importer les SMS existants, mais sans chiffrement)
Appel téléphonique chiffré	Oui	Non, mais on peut laisser un message vocal
Pièces jointes chiffrées	Oui, mais pas de communication sur la taille maximale	Jusqu'à 1,5Go
Disponible sur ordinateur	Oui, mais il faudra l'extension Chrome et une petite manipulation (voir plus loin)	Oui, mais il est impossible de continuer sur un appareil une conversation chiffrée de bout en bout commencée sur un autre
Version en ligne	Non	Oui, mais il est impossible de continuer sur un appareil une conversation chiffrée commencée sur un autre: **https://web.telegram.org**
Autodestruction des messages	Oui, au bout d'un certain nombre de messages (chiffre défini par l'utilisateur)	Oui, de 1 seconde à une semaine
Nombre d'utilisateurs actifs	Pas de communication sur le nombre, mais sans doute moins de 10 millions	100 millions

initier une conversation privée (voir notre prise en main). Avec cette précaution, vous ne laisserez aucune trace de vos messages sur les serveurs de Telegram et il sera impossible d'avoir une trace sur l'application PC/Mac. Sans cela, les messages envoyés sont tout de même chiffrés, mais ils reposent sur les serveurs de Telegram. L'autre problème qui hérisse les poils des adversaires de Telegram c'est la notion d'open source. Le client est en effet ouvert, comme Signal, et on peut donc vérifier qu'aucune backdoor n'ira compromettre vos messages. Par contre au niveau de la partie serveur, le logiciel est propriétaire. Impossible donc d'être sûr que les messages ne sont pas lus. Pour le créateur de Telegram la solution est simple : utilisez le tchat secret si vous ne faites pas confiance à Telegram !

CONCLUSION :

Si vous utilisez déjà Telegram, ne changez pas de crèmerie. Pensez simplement à activer le Secret Chat ! Si vous n'avez aucune de ces solutions (ou que vous utilisez WhatsApp), vous pouvez opter pour Signal qui propose les conversations téléphoniques chiffrées. Au final, vous seriez peut-être tenté d'opter pour la messagerie où vous comptez le plus d'amis, mais rien ne vous empêche de faire du prosélytisme ou de simplement convaincre vos contacts de changer.

PAS À PAS

Un Secret Chat avec Telegram

CE QU'IL VOUS FAUT

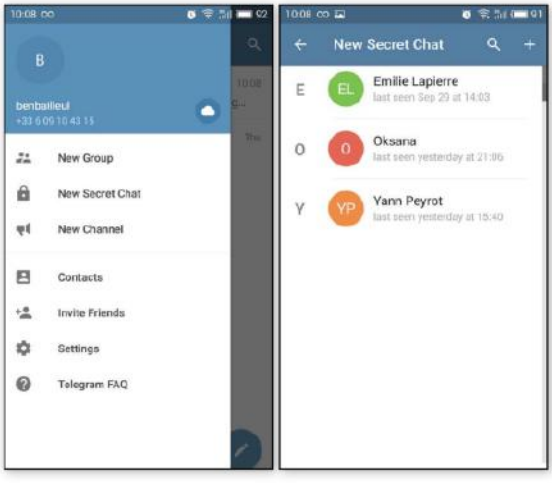
TELEGRAM

OÙ LE TROUVER ? :
https://telegram.org

DIFFICULTÉ :

01 INITIEZ LE TCHAT

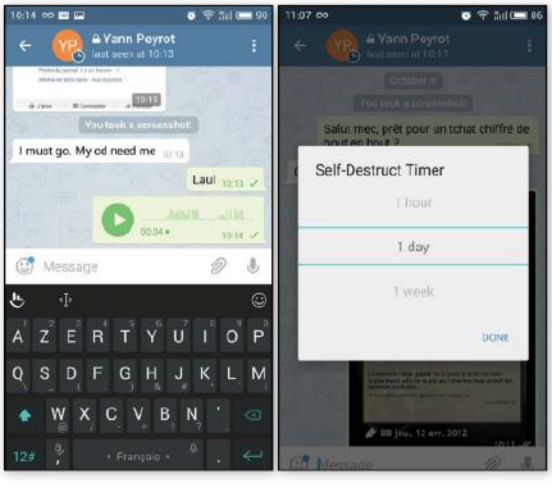
Pour être sûr de chiffrer ses communications avec Telegram, sélectionnez les trois barres horizontales et faites **New Secret Chat**. Choisissez alors le contact que vous voulez joindre. Libre



à vous d'envoyer des pièces jointes, des messages vocaux (pas de téléphonie sur Telegram!). Attention, ces activités ne seront pas visibles par la suite sur l'appli desktop puisque le bout en bout est à l'honneur.

02 LES MESURES DE PROTECTION

Si vous prenez une capture, l'appli vous le notifiera. Cela permet à l'utilisateur de savoir si une capture a été faite sans son consentement (par un espion ou un malware). Sur Signal, les captures sont presque impossibles à faire.En cliquant sur les trois petits points en haut à droite, vous pouvez effacer le tchat, supprimer l'historique et mettre un compte à rebours permettant d'effacer le tchat après un certain temps. (**Set self-destruct timer**).



PAS À PAS

Synchroniser Signal avec votre PC

CE QU'IL VOUS FAUT

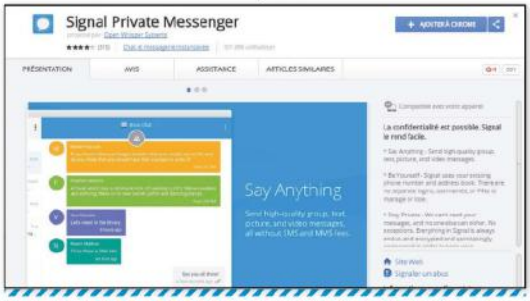
SIGNAL PRIVATE MESSENGER

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

DIFFICULTÉ :

01 INSTALLATION

Depuis Google Chrome, cliquez dans les trois petits points en haut à droite puis faites **Plus d'outils>Extensions>Plus d'extensions**. Dans la barre de recherche, tapez signal et cliquez sur **Ajouter à Chrome>Ajouter l'application**. Faites un autre clic sur **Commencer** puis **Got It**.

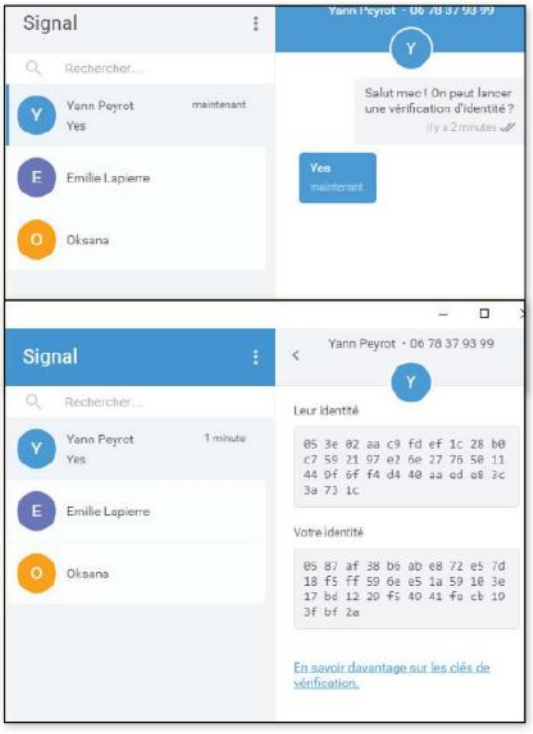


02 SYNCHRONISATION

Utilisez votre smartphone pour scanner le QR Code et synchroniser l'extension avec le mobile. Au bout de quelques secondes, vous devriez voir votre numéro de téléphone s'afficher dans une fenêtre. Validez pour voir vos contacts et converser avec eux. Les messages seront aussi contenus dans votre mobile et le chiffrement sera de bout en bout.

03 VÉRIFIER L'IDENTITÉ DE VOTRE CORRESPONDANT

Libre à vous de vérifier l'identité de votre correspondant avec la clé publique. Sur mobile, initiez une conversation et faites **Préférences de conversation>Vérifier l'identité** tandis que sur PC, il faudra cliquer sur les trois petits point verticaux puis **Vérifier l'identité**.



POURQUOI NE PAS PARLER DE WHATSAPP ?

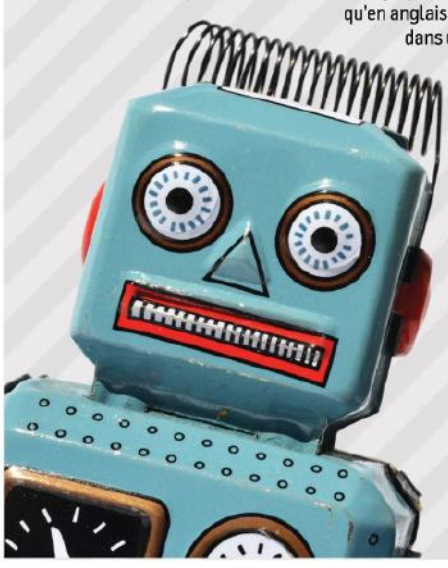
WhatsApp est utilisé par un milliard d'utilisateurs et est de loin la solution de messagerie n°1. En ajoutant une couche de chiffrement en début d'année, l'appli a suivi le mouvement de nombreuses messageries. Par la suite, Facebook a flairé la bonne affaire en achetant l'application pour 19 milliards de dollars. Seulement, voilà, le réseau social tentaculaire souhaite utiliser WhatsApp pour faire de la publicité ciblée en se servant de l'énorme base de données que constituent les numéros de téléphone des utilisateurs. Même avec un chiffrement solide, comment peut-on encore faire confiance à cette application pour respecter votre vie privée ? On peut aussi se demander pourquoi certains gouvernements font la guerre à Telegram, qui possède 10 fois moins d'utilisateurs, et pas à WhatsApp. Y'aurait-il des trous dans le fromage ? C'est un lièvre que Durov a récemment soulevé dans un Tweet.

▲ **« Vous ne vous êtes jamais demandé pourquoi les régimes totalitaires comme la Chine ou le Bahreïn bloquent Telegram, mais laissent WhatsApp tranquille ? »**

#1 Troller les arnaqueurs du Web

AVEC MLOOPER

Si vous en avez marre de recevoir des e-mails d'une princesse nigériane vous réclamant 500€ (pour en toucher 1000 fois plus) ou de ce monsieur prêt à se séparer d'un bien d'une grande valeur en échange d'un mandat, le script de Brian Weinreich est fait pour vous! Ce dernier va répondre automatiquement aux arnaqueurs qui vous sollicitent. Le bot est tellement convaincant que les malandrins peuvent répondre plusieurs fois avant de se rendre compte qu'ils parlent dans le vide. Le seul problème de ce robot si sympa, c'est qu'il ne parle qu'en anglais et doit s'installer dans un cloud via une base MySQL. Pas très accessible, mais si vous désirez faire des modifications, le code est libre ! Cela nous a rappelé la vidéo de Mozinor sur les Mugu et les Brouteurs : **https://goo.gl/nkzRTn**



Lien : **https://github.com/beweinreich/mlooper**

#2 De l'Open VPN

AVEC IPJETABLE

IPjetable, le service de VPN basé aux Pays-Bas est depuis peu passé au protocole OpenVPN. Encore en version béta, ce dernier remplacera peu à peu les connexions PPTP vieillissantes et peu sûres. Les clients peuvent se rendre dans leur espace et suivre le lien **OpenVPN BETA** pour trouver l'ensemble des explications nécessaires à la configuration de leur VPN sur leurs appareils préférés (Windows, Mac OS, iPhone, etc.). Ce n'est pas tout puisque prochainement, d'autres pays d'emprunt seront disponibles...

Notez que IPjetable ne garde aucune donnée puisque la loi néerlandaise l'y autorise et qu'il est possible de profiter d'une période d'essai de quelques jours avant de payer 15€/trimestre si vous êtes convaincu.

Merci à Pierre G. Pour cette information !

#3 Du chiffrement natif sur Android

AVEC OVERSEC

Vous le savez bien, lorsqu'il s'agit de chiffrer des communications, il faut que les correspondants utilisent le même logiciel/protocole pour que cela fonctionne. Cela peut décourager le plus motivé des utilisateurs puisqu'il faudra «convertir» vos amis et contacts à telle ou telle solution de chiffrement (voir notre article sur Signal et Telegram à la page 20). Sur Android, la solution pourrait s'appeler Oversec: une application qui ajoute une couche de chiffrement de bout en bout à toutes les autres applications. A vous les SMS, Facebook, Twitter, Skype, ou Gmail entièrement chiffrés! Alors certes, ici aussi vos correspondants devront posséder Oversec, mais ils pourront l'utiliser avec toutes les applications en leur possession. Si X, Y et Z utilisent l'appli, X peut parler avec Y via Gmail chiffré. Y de son côté peut envoyer des SMS chiffré à X puisque X n'a pas Facebook, etc. Oversec n'est donc pas restrictif et s'applique potentiellement à chacune de vos applications. Il est même possible d'afficher de faux textes qui s'afficheront en clair sur le réseau pour détourner l'attention des espions/pirates! Un petit tuto pour le prochain numéro?

Lien : **www.oversec.io**

#4 Anonymat sur Internet

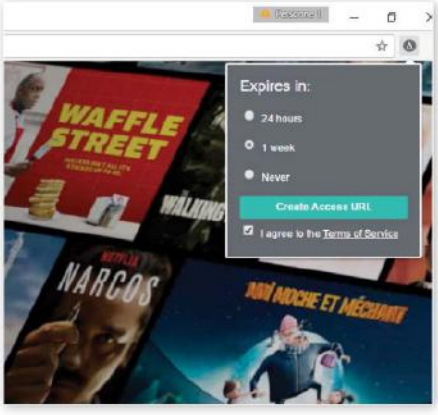
avec Tor Browser 6.0

Vous utilisez Tor pour masquer vos activités sur le Net ou éviter les curieux? Vous avez bien raison. N'oubliez cependant pas de mettre à jour votre **Tor Browser** pour disposer des dernières fonctionnalités ! C'est le moment où jamais avec cette version 6 qui reprend les bases de Firefox 45 et ajoute donc la prise en charge du HTML5 tout en corrigeant les dernières failles et quelques bugs. N'oubliez pas de n'installer aucune extension supplémentaire sur ce navigateur !

#5 Partagez un accès sans compromettre son mot de passe

avec Access URL et Chrome

Vous voulez partager un accès à Netflix, Canal+, T411 ou n'importe quel autre site réclamant des identifiants? Au lieu de donner votre vrai mot de passe, vous pouvez très bien opter pour l'extension Chrome Access URL. Il suffit de s'identifier sur un site et de cliquer sur l'icône d'**AccessURL** pour générer un cookie qui sera expédié à votre ami. Ce dernier, lui aussi utilisateur de l'extension, recevra un lien pour accéder à votre espace. Il ne pourra cependant pas le partager avec d'autres personnes. Vous avez même la possibilité de paramétrer une durée de validité.



Lien : **www.wireshark.org**

#6 Expulsez les squatteurs de Wi-Fi

avec Fing Network Tools

Rien de plus rageant que de voir son réseau Wi-Fi complètement aux fraises, sans aucune raison. Vous ne le savez peut-être pas, mais il est possible que certains voisins mal intentionnés ne se privent pas d'utiliser votre connexion. Avec l'application Android Fing Network Tools, dénichez les squatteurs et expulsez-les par la même occasion. Il est aussi possible de «signer» vos appareils domestiques pour être immédiatement averti d'une intrusion.

Lien : **https://goo.gl/0MRB3p**

TABLES ARC-EN-CIEL: UN VRAI TRÉSOR!

Avec l'article sur Hashcat de notre numéro précédent, vous vous sentez très fort et prêt à vous attaquer à n'importe quel mot de passe ? Et si nous vous disions qu'il est encore possible de faire mieux avec les rainbow tables, ces chaînes de mots de passe « prémâchées » ? Voyons comment cela fonctionne...

Lorsque vous possédez le hash d'un mot de passe et que vous voulez retrouver le sésame, il existe plusieurs méthodes. La première consiste à regarder sur des bases de données comme **https://crackstation.net** ou **https://hashkiller.co.uk**, si le hash n'est pas déjà connu ou se réfère à un mot de passe tellement facile qu'il est connu comme le loup blanc (**ab4f63f9ac65152575886860dde480a1** pour **azerty** en MD5 par exemple). La seconde solution consiste à attaquer par « dictionnaire » en essayant des millions de mots issus d'un fichier texte (par exemple **nirvana**, **Windows** ou **Porsche911** ont de grandes chances de s'y trouver). Lorsque cela échoue, il reste encore le « brute force » : essayer des combinaisons de caractères plus ou moins longs en espérant glaner des indices permettant de gagner du temps. On peut par exemple tenter d'en savoir plus sur les dates de naissance de la personne qui a créé le mot de passe.

DANS LES ÉPISODES PRÉCÉDENTS

Dans notre précédent numéro, nous vous avions parlé du logiciel hashcat et de ses fonctions « hybrides », comme le fait de pouvoir mixer une attaque dictionnaire avec un brute force. Si le mot de passe est **Skywalker001**, il ne sera pas trouvé avec une attaque par dictionnaire si le dico ne contient que **skywalker**. Il faudra demander

au logiciel d'ajouter des suffixes paramétrables (ici 3 chiffres) et de mettre une majuscule au début à chaque essai. L'attaque par combinaison permute quant à elle les différents mots du dico (**jesuspass**, **1234pass** ou **passjesus1234** à partir de **jesus**, **pass** et **1234**). Une telle entreprise demande de la réflexion pour bien utiliser le logiciel et entrer les bonnes commandes, mais aussi un temps de calcul qui peut durer des siècles dans les cas les plus extrêmes. Mais il existe une ultime solution que nous n'avons jamais abordée : les rainbow tables, ou tables arc-en-ciel.

UNE NOUVELLE TECHNIQUE

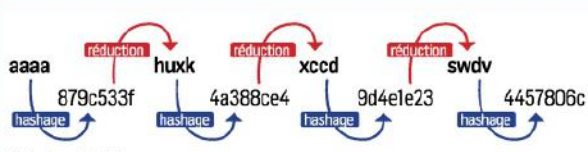
Au lieu de vérifier si tel mot de passe correspond au hash de départ, puis de refaire la même opération jusqu'à trouver le bon sésame, le principe de rainbow table diffère quelque peu. Il s'agit d'une technique de « compromis temps-mémoire » réduisant considérablement le temps nécessaire pour casser un mot de passe. Une rainbow table, c'est une sorte de tableau avec un mot de passe de départ dans la première colonne et un mot de passe d'arrivée dans la dernière. Dans les colonnes du milieu, on va trouver des mots de passe intermédiaires qui sont obtenus avec des calculs appelés fonction de réduction. Une fonction de réduction transforme une empreinte de mot de passe en un nouveau mot de passe. Au final, on ne va garder que le premier et le dernier mot de passe généré puisque le reste de la chaîne (les colonnes du milieu) peut être retrouvé en refaisant des calculs beaucoup plus rapides que tout le processus d'un brute force. L'inconvénient, c'est qu'il vous faut générer ces fichiers rainbow tables en amont. En fonction de la complexité du mot de passe que vous souhaitez retrouver ces derniers peuvent peser de 500 Mo à plus d'un To ! Il faut donc de la place sur un disque dur et beaucoup de temps pour les générer (comptez 3 heures pour 1 Go avec un PC standard). Heureusement, vous pouvez télécharger ces tables, les acheter et bien sûr les garder pour d'autres tentatives de crackage si vous avez eu le courage de les générer vous même. Nous allons donc voir comment générer ces tables et les utiliser avec RainbowCrack, un logiciel qui en plus d'être compatible avec un grand nombre de hash, supporte le multicoeur et l'accélération graphique (le CUDA de nVidia ou le OpenCL de ATI/AMD comme Crarck, voir *Pirate Informatique* n°29). Pas de jaloux pour cette démonstration puisque RainbowCrack est disponible sur Windows et Linux.

Si vous avez raté des numéros...

Si certains aspects de ces pages vous échappent nous avons pensé à vous en regroupant dans le CD tous les précédents articles où nous avons abordé les cracks de mots de passe et les hash : John The Ripper (n°19 & 20), hashTag.py (n°24), PDFCrack (n°26 & 27), fcrackzip (n°28), Crarck (n°29) et Hashcat (n°30).

COMMENT ÇA MARCHE ?

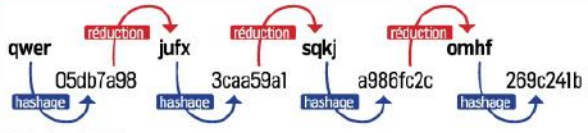
Le principe des rainbow tables consiste à calculer un mot de passe à partir d'une empreinte. Pas « le » mot de passe qui correspond à l'empreinte, mais « un » mot de passe. On dit que l'on « réduit l'empreinte » grâce à une fonction de réduction qui doit systématiquement toujours redonner le même mot de passe quand on lui donne la même empreinte. Pour générer une rainbow table, on part d'un mot de passe, on calcule son empreinte puis on calcule un nouveau mot de passe à partir de l'empreinte, on calcule l'empreinte de ce mot de passe, etc. À la fin, on stocke dans la table le mot de passe initial et l'empreinte finale.



Rainbow Table

aaaa	4457806c

On recommence ensuite le processus avec un nouveau mot de passe pour construire une nouvelle « chaîne ».



Rainbow Table

aaaa	4457806c
qwer	269c241b

La rainbow table ainsi générée contient 2 lignes où chaque ligne représente une chaîne de 4 mots de passe (chaîne de longueur 4). Pour utiliser cette table, RainbowCrack va essayer de cracker l'empreinte 269c241b. Cette empreinte figure directement dans la table, à la seconde ligne, et est associée avec le mot de passe **qwer**. On sait donc que le mot de passe qui correspond à cette empreinte est le 4ème de la chaîne. Malheureusement, on ne l'a pas stocké dans la table pour gagner de la place, mais on peut le retrouver à partir du mot de passe initial. On fait passer ce dernier dans la fonction de hachage, ce qui donne 05db7a98. Ensuite, on fait passer cette empreinte dans la même fonction de réduction que celle qui a servi à générer la table. Elle retourne donc le 2e mot de passe de la chaîne (**jufx**) que l'on hache puis réduit pour trouver le 3e mot de passe (**sgkj**), que l'on hache puis réduit pour donner le 4e mot de passe: **omhf**. Bingo!

Merci au site http://mieuxcoder.com.

PAS À PAS

Générez votre table arc-en-ciel

CE QU'IL VOUS FAUT

RAINBOWCRACK

OÙ LE TROUVER ? : **http://project-rainbowcrack.com**

DIFFICULTÉ : ☠☠☠

01 OÙ TROUVER LE LOGICIEL ?

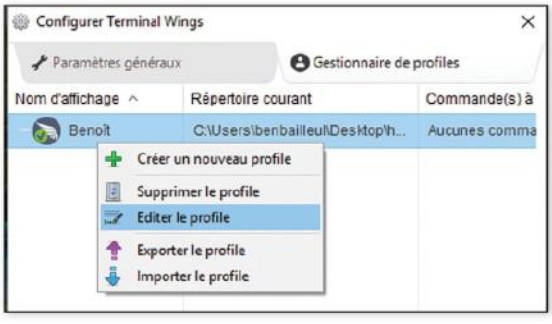
Sous Kali Linux, RainbowCrack est installé d'office. Sous d'autres distributions ou sous Windows, suivez notre lien pour le télécharger. Allez dans le menu **Applications** puis **Attaques de mots de passe** pour trouver le logiciel. Dans la fenêtre, vous verrez comment doivent être organisées les lignes de commandes ainsi que les limites pour les longueurs de mots de passe (de 0 à 15 pour le MD5, 0 à 20 pour le SHA1, etc.)

UN PEU DE SEL DANS VOTRE HASH ?

Le salage est une méthode permettant de renforcer la sécurité des mots de passe. Au lieu d'utiliser une méthode de hachage connue (MD5, etc.), on va y ajouter une valeur supplémentaire (une chaîne aléatoire) pour brouiller les pistes et éviter que le mot de passe n'ait qu'un seul hash équivalent. Le salage est une méthode éprouver pour contrer la technique de la rainbow table. Si vous êtes développeur, vous savez ce qu'il vous reste à faire...

02 PREMIÈRE TABLE

Comme nous avons vu que les fichiers peuvent peser plusieurs Go, nous allons commencer léger et créer un «set» de 6 rainbow tables. Supposons que nous cherchions un mot de passe à partir d'un hash MD5 et que nous sommes sûrs que ce dernier fait entre 4 et 7 caractères tout en minuscule. Nous allons d'abord taper **cd /usr/share/rainbowcrack** pour aller dans le répertoire de destination puis:



rtgen md5 loweralpha 4 7 0 2000 35000000 test puis **Entrée**.

03 LES DÉCLINAISONS

Le 0 correspond au numéro d'index. Si l'index change, la fonction de réduction aussi. 2000 correspond à la longueur de la chaîne. Plus elle est grande, plus la table contient de mots de passe, mais

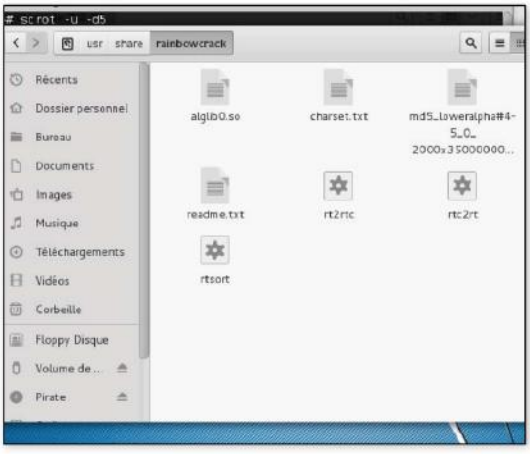
```
Copyright 2003-2015 RainbowCrack Project. All rights rese
http://project-rainbowcrack.com/

usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file
rt_files:              path to the rainbow table(s), wil
-h hash:               load single hash
-l hash_list_file:     load hashes from a file, each has
-f pwdump_file:        load lanmanager hashes from pwdum
-n pwdump_file:        load ntlm hashes from pwdump file

hash algorithms implemented in alglib0.so:
    lm, plaintext_len limit: 0 - 7
    ntlm, plaintext_len limit: 0 - 15
    md5, plaintext_len limit: 0 - 15
    sha1, plaintext_len limit: 0 - 20
    sha256, plaintext_len limit: 0 - 20

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rcrack *.rt -l hash.txt
root@kali:~# rtgen md5 mixalpha-numeric 4 7 0 2000 50000
```

plus elle sera longue à générer. Enfin, 35000000 se rapporte au nombre de chaînes (les lignes du tableau). Comme chaque ligne fait 16 bits, on peut savoir combien pèsera la table en faisant 35 000 000x16=560000000 bits. Environ 560Mo par table donc. Nous allons ensuite taper:

rtgen md5 loweralpha 4 7 1 2000 35000000 test
rtgen md5 loweralpha 4 7 2 2000 35000000 test

04 NOM ET EMPLACEMENT

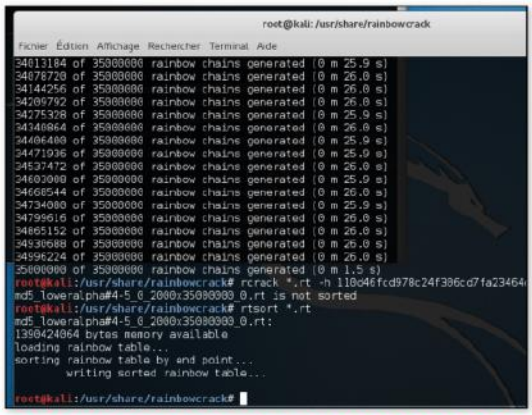
Continuez jusqu'à l'index **5** ce qui nous fera 6 tables en tout appelées **md5_loweralpha # 3-7_0_2000x80000_test.rt**, etc. Ces opérations vont prendre énormément de temps



alors, imaginez si nous prenions en compte les mots de passe mixtes (voir le fichier **charset.txt** pour changer le paramètre **loweralpha**) de 3 à 15 caractères! Vous comprenez maintenant pourquoi certaines tables font plus de 1To. L'avantage, c'est que cette technique va vous faire gagner des heures, des jours et même des années!

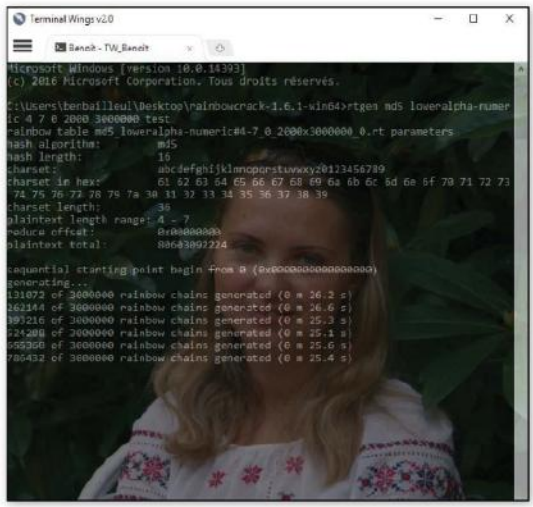
05 LE TRI

Une fois vos tables générées, il va falloir encore faire une opération pour les rendre exploitables: c'est le tri. La commande rtsort va «retourner» la table pour commencer la recherche par la dernière empreinte et donc remonter le fil de la table (voir notre schéma). Toujours dans **/usr/share/rainbowcrack**, faites **rtsort *.rt** pour trier vos 6 tables qui se trouvent dans le dossier de travail. N'interrompez surtout pas le processus!



06 ET SOUS WINDOWS ?

Sous Windows, RainbowCrack s'opère en ligne de commande lorsqu'il s'agit de générer et trier les tables. Pour plus de confort, nous avons choisi d'utiliser le logiciel Terminal Wings



(**www.phrozensoft.com**). L'avantage de ce dernier réside dans la gestion d'un profil avec un répertoire d'usage. Si vous ne souhaitez pas l'utiliser, restez appuyé sur **Shift** (ou **Maj**), faites un clic droit dans le dossier de RainbowCrack faites **Ouvrir une fenêtre de commande ici**. Au niveau des commandes, c'est exactement la même chose.

TÉLÉCHARGER DES RAINBOW TABLES ?

Il est devenu tellement difficile de trouver des rainbow tables gratuites sur Internet que nous nous sommes résignés à créer les nôtres. Si cela vous intéresse, sachez que les développeurs de RainbowCrack proposent des Go de tables à la vente pour les hash LM/NTLM, MD5 et SHA1. Il vous en coûtera la bagatelle de 1 000 dollars par catégorie ou 2 700 $ pour le tout !

PAS À PAS

Crackez avec votre table

CE QU'IL VOUS FAUT

RAINBOWCRACK

OÙ LE TROUVER ? :
http://project-rainbowcrack.com

DIFFICULTÉ : ☠☠☠

01 PRÉPARATIFS

Votre belle rainbow table est prête? Il est temps de l'utiliser! N'oubliez pas que dans notre exemple, nous avons choisi de créer une table permettant de cracker un mot de passe hashé en MD5 de 4 à 7 caractères de long uniquement constitué de minuscule. Allons sur **www.md5.cz** et notons les hash correspondant à **0000**, **jesus** (vous avez appris la bonne nouvelle? Il est ressuscité!) et **bidul**. Bien sûr, ces mots de passe sont très faibles, mais avec la table que nous avons générée il ne faut pas s'attendre à des miracles

02 CRACK !

Depuis le répertoire de travail, tapez: **rcrack *.rt -h 110d46fcd978c24f306cd7fa23464d73**

Ce hash est celui correspondant au sésame **jesus**. Si vous en avez plusieurs, mettez-les dans un fichier TXT (toujours dans le même répertoire) et faites **rcrack *.rt -l hash.txt**

L'argument ***.rt** va prendre en compte toutes les tables dans le dossier de travail, faites donc attention si vous en avez plusieurs (rangez-les dans des dossiers séparés).

```
total time:                                  0.93 s
  time of chain traverse:                    0.84 s
  time of alarm check:                       0.00 s
  time of wait:                              0.08 s
  time of other operation:                   0.01 s
time of disk read:                           0.92 s
hash & reduce calculation of chain traverse: 1998000
hash & reduce calculation of alarm check:    320
number of alarm:                             320
speed of chain traverse:                     2.38 million/s
speed of alarm check:                        0.32 million/s

result
---------------------------------------------------------
110d46fcd978c24f306cd7fa23464d73  jesus  hex:6a65737573
root@kali:/usr/share/rainbowcrack#
```

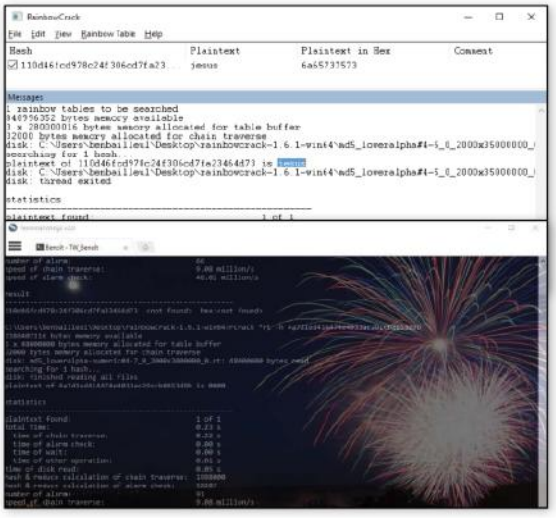
03 AVANTAGES ET LIMITES

En fonction de différents paramètres (taille du mot de passe, de la table, puissance du PC, etc.), le processus peut prendre longtemps, mais rien de comparable avec le brute force. **00000**, **jesus** et **bidul** ont été trouvé en quelques secondes (le résultat s'affiche en bas avec l'équivalent hexadécimal du mot de passe (c'est important pour les caractères accentués, voir notre encadré). N'espérez pas des résultats aussi rapides avec un sésame comme **Tf5Jç5d_cc23dx^$** par exemple. Mais avec les rainbow tables, vous avez une chance. Avec le brute force... aucune.

```
  time of alarm check:                       0.00 s
  time of wait:                              0.07 s
  time of other operation:                   0.01 s
time of disk read:                           0.90 s
hash & reduce calculation of chain traverse: 1998000
hash & reduce calculation of alarm check:    192
number of alarm:                             192
speed of chain traverse:                     2.41 million/s
speed of alarm check:                        0.19 million/s

result
---------------------------------------------------------
8551819a762771e56d6ad74facc3022  bidul  hex:626964756c
root@kali:/usr/share/rainbowcrack#
```

04 ET SOUS WINDOWS ?

Sous Windows, la partie «crack» peut s'effectuer en ligne de commande ou via une interface graphique (GUI). Notez qu'il est possible de tirer parti des accélérateurs graphiques CUDA ou OpenCL. Si cela ne fonctionne pas avec votre matériel, utilisez simplement **rcrack_gui.exe**, allez dans **File** puis **Add Hashes...**



pour coller votre hash. Dans le menu **Rainbow Table**, allez dans **Search Rainbow Table...** pour choisir votre table. Les calculs commencent immédiatement.

ET AVEC DES CARACTÈRES ACCENTUÉS ?

Vous aurez remarqué que nous n'abordons pas le sujet des accents dans notre démonstration. Comment faire avec des mots de passe francophones alors ? C'est un peu complexe, car cela dépend de votre système d'exploitation et du codage hexadécimal que celui-ci utilise pour chaque caractère. Heureusement, RainbowCrack peut être patché pour faciliter la lecture. Pour ceux qui s'y intéressent, consultez le chapitre 3 et 4 de ce document signé Guillaume Lehembre : **www.hsc.fr/ressources/breves/rainbowtables.html.fr**

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3€

Chez votre marchand de journaux

QUBES OS : LE SYSTÈME «CLOISONNÉ»

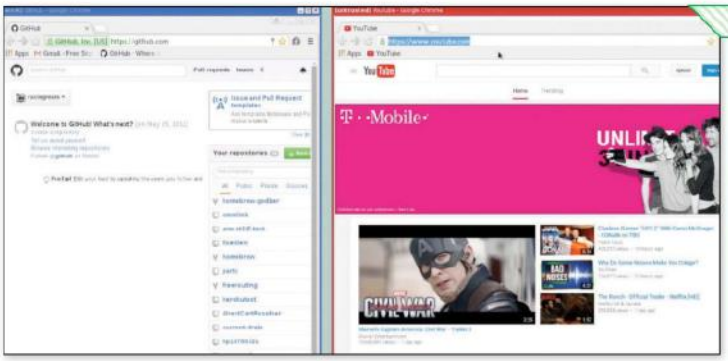
LEXIQUE

***SANDBOX :**
Littéralement «bac à sable». Il s'agit d'un espace virtuel coupé du système qui permet d'être sûr que vos activités n'iront pas le polluer.

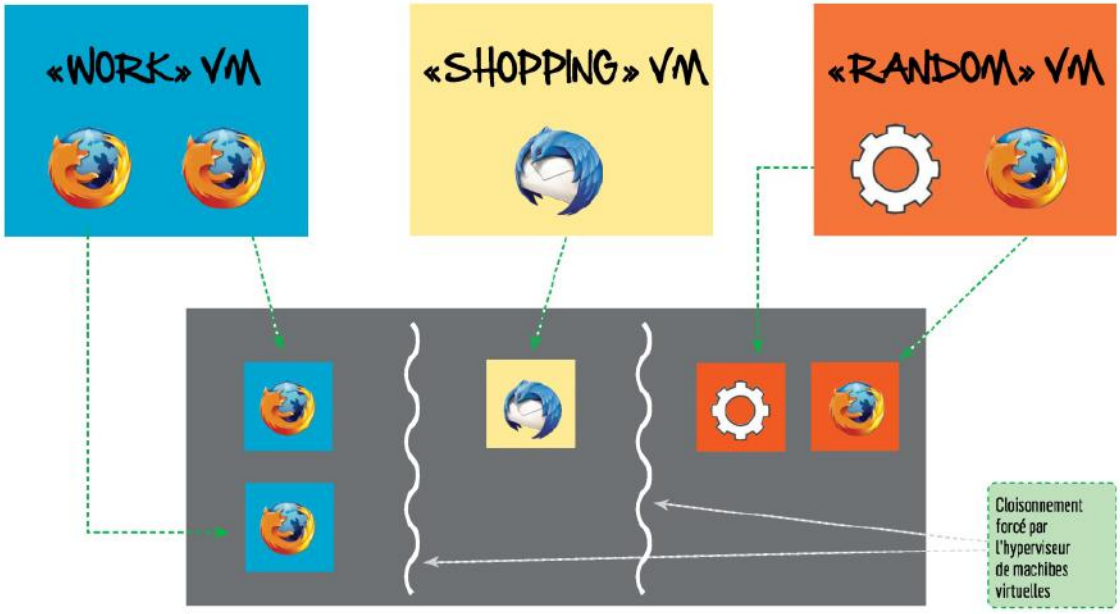
Basé sur l'architecture virtuelle Xen, Qubes OS est un système qui va créer autant de « bacs à sable » que vous voudrez. Vous pourrez par exemple disposer d'un navigateur contenant toutes vos données de connexions et un autre que vous utiliserez pour aller sur un site louche ou non sécurisé. Ce site contient un malware ou tente une intrusion ? Pas de problème, puisque tout est déployé dans la RAM : l'infection s'arrêtera nette sans compromettre le reste du système. Cela vous évitera des ennuis si par exemple, vous ouvrez la pièce jointe qu'il ne fallait pas ou si vous lancez un programme dont vous n'êtes pas sûr. C'est comme si toutes vos actions s'exécutaient sur des machines différentes. Car Qubes OS permet de créer autant de machines virtuelles (appelé « qube » ou AppVM) que d'utilisateurs ou types d'utilisation : achat en ligne, travail, etc.

DIFFÉRENTS COMPARTIMENTS

À moins d'opter pour l'installation sur une clé USB, il faudra faire en sorte de faire cohabiter l'OS avec votre Windows ou votre distribution Linux pour le tester (voir notre pas-à-pas). Et avec Qubes OS, c'est



Travail, achat en ligne ou simple navigation, toutes vos activités sont compartimentées. Le Firefox de la machine virtuelle «Work» en bleue connaît vos mots de passe tandis que celui de la zone «Random», utilisée pour les sites peu sûrs, ne les connaît pas. Même chose pour les fichiers qui peuvent être placés dans des domaines différents.



BUREAU DE L'UTILISATEUR

l'utilisateur qui a la lourde responsabilité de prendre toutes les décisions concernant la sécurité. Et malgré le code couleur permettant de s'y retrouver dans les différentes machines virtuelles, il n'est pas souvent aisé de comprendre où le système veut en venir. En effet, certains messages ou menus restent en anglais. Les linuxiens partiront avec une longueur d'avance puisque le système est basé sur Unix et qu'il est possible de commencer avec des « templates » (des groupes de « qubes ») Fedora, Debian ou Whonix. Notons enfin que l'implémentation de Tor est de la partie, même s'il ne s'agit pour le moment que d'une phase expérimentale.

QUELLE CONFIGURATION ?

Pas question d'installer Qubes OS sur un vieux coucou. Il vous faudra absolument un processeur 64 bits, 4Go de RAM et 32Go d'espace sur le disque dur pour l'installation. La liste de matériels compatibles est disponible ici : **www.qubes-os.org/hcl**.

PAS À PAS

Installation et premiers pas

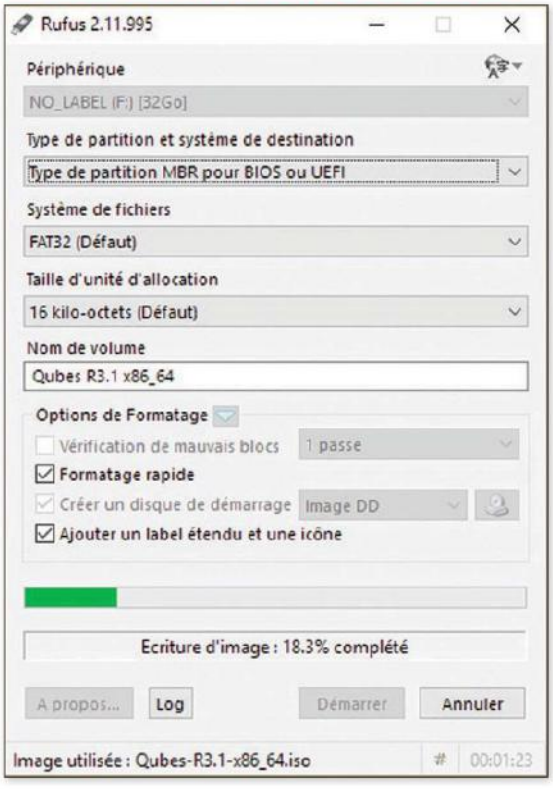
CE QU'IL VOUS FAUT

QUBES OS
OÙ LE TROUVER ? : **www.qubes-os.org**

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

DIFFICULTÉ :

01 LES FICHIERS NÉCESSAIRES

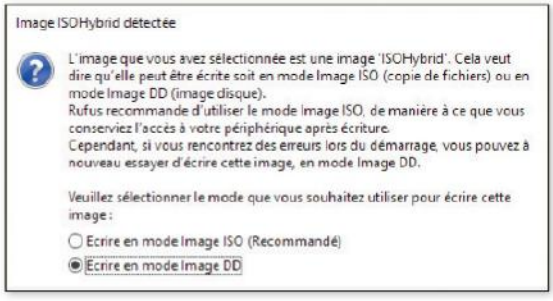


Commencez par télécharger l'image de Qubes OS au format ISO (5 Go) et vérifiez son intégrité avec sa signature PGP. Notez que si vous optez pour l'installation depuis une clé USB, il vous en faudra une de 32 Go. Téléchargez aussi le logiciel Rufus. Pour l'image DVD, faites un tour ici : **https://ftp.qubes-os.org/iso** et gravez simplement l'image sur la galette. Attention, dans la liste vous trouverez aussi des versions Live CD. Choisissez-en une faisant moins de 4,2 Go où vous serez obligé de passer par un DVD double densité. Lancez Rufus et choisissez l'option **Image DD** dans **Créer un disque de démarrage**.

DANS LE PROCHAIN NUMÉRO

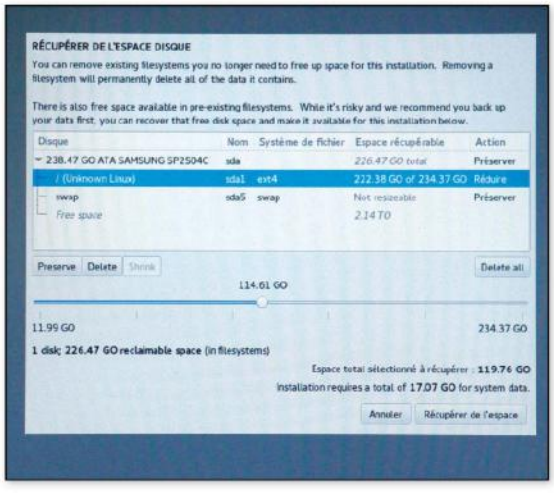
Des difficultés avec Qubes OS ? Envie d'approfondir les possibilités du système (Tor, VPN, etc.) ou de découvrir un autre système alternatif ? Dites-nous ce que vous voulez pour le prochain numéro : **benbailleul@idpresse.com** !

02 AVEC WINDOWS OU LINUX



Retrouvez l'ISO dans l'arborescence en choisissant **Tous les fichiers** dans la fenêtre **Ouvrir**. Rufus vous demandera bien la confirmation que vous souhaitez une Image DD. Faites **OK** puis **Démarrer**. Les fichiers nécessaires iront dans la clé USB. Notez que QubesOS n'est pas compatible avec les BIOS UEFI. Sous Linux, il faudra faire **dd if=Qubes-R3-x86_64.iso of=/dev/sdX** (en prenant soin de changer le nom de l'ISO si celui-ci a changé et la partition également, **sda1** par exemple).

03 MULTIBOOT ?

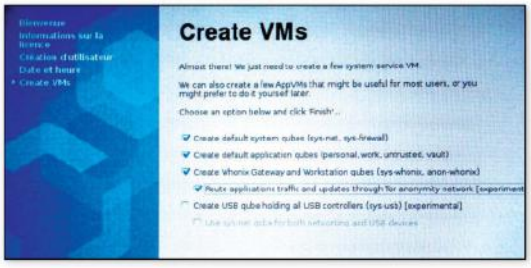


En ce qui concerne l'installation (ou le lancement du Live CD), pas de surprise, il faudra booter sur la clé USB ou le lecteur optique depuis le BIOS. Vous pouvez très bien opter pour le multiboot au démarrage, mais sachez que cela est peu sécurisé. En effet, un malware pourra accéder à **/boot** ce qui pourrait contaminer Qubes OS depuis le Windows ou le Linux déjà présent. Il est donc

préférable d'installer uniquement Qubes OS sur un PC si vous souhaitez vraiment l'utiliser de manière régulière. Si vous souhaitez juste le tester, suivez ce lien pour savoir comment activer le multiboot : **www.qubes-os.org/doc/multiboot**

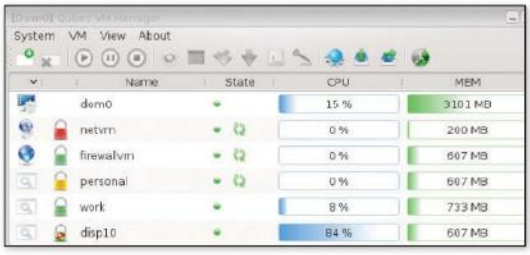
04 OPTIONS D'INSTALLATION

Lors de l'installation vous aurez à choisir la langue, le mot de passe pour le chiffrement du disque et vous aurez aussi accès à un module permettant de créer une partition dans **Installation destination**. Vous pouvez en effet choisir de **Récupérer de l'espace** sur un disque (32 Go seront nécessaires). Après avoir entré à nouveau votre mot de passe, vous devrez choisir les options de départ. Cochez les 4 premières cases pour activer le support de Tor dans le même temps.



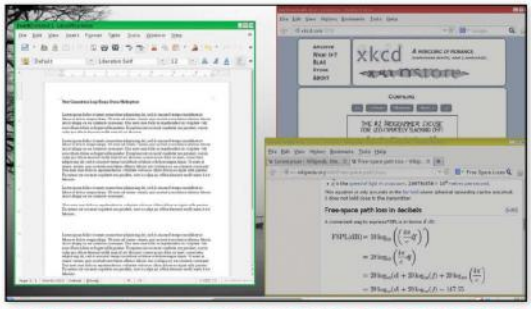
05 VOTRE BUREAU

Une fois que les fichiers seront copiés, authentifiez-vous et découvrez le bureau. La seule fenêtre qui va s'afficher concerne les qubes présents au démarrage : **dom0** (qui correspond au domaine initial, le père de tous les autres) ainsi que **sys-net** (gestion du réseau) et **sys-firewall** (pour le pare-feu). Le bureau est très sobre, juste quelques options dans **Desktop** en haut à droite et une barre des tâches en bas. Si le Wi-Fi n'est pas pris en compte, branchez le PC avec un câble Ethernet.



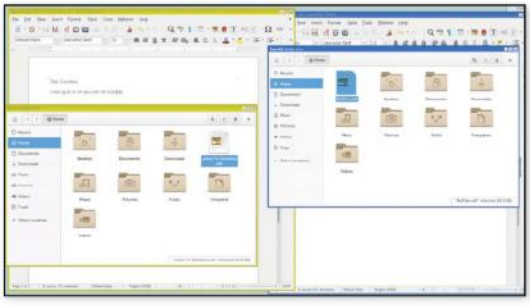
06 VOTRE PREMIER « QUBE »

Depuis le bouton en forme de logo Qubes en bas à gauche, vous allez pouvoir accéder aux différents «domaines» : **vault, personal, work** et **untrusted** correspondant à quatre niveaux de sécurité. Commençons par ouvrir un navigateur depuis un de ces domaines ou depuis le menu **Disposable VM** qui va ouvrir un navigateur «jetable». Dans le menu **anon-whonix**, vous aurez la possibilité de faire fonctionner votre navigateur avec Tor.



07 POUR LES FICHIERS AUSSI...

Dans chaque domaine, vous aurez la possibilité d'ajouter des raccourcis (**Add more shortcuts**...). Pour les fichiers c'est la même chose, vous pouvez très bien sauvegarder un document dans un domaine sans que les autres ne le «voient» dans leur propre arborescence. Idéal pour de pas mélanger vos activités personnelles avec vos activités professionnelles. Ce sont de nouvelles habitudes à prendre, mais au final vous serez gagnant.



Interview de Andrew David Wong, documentaliste et community manager du projet Qubes OS

Dans notre dernier numéro nous avons fait un sujet complet sur Tails. Nous nous demandons si avec l'implémentation de Tor vous voulez faire de Qubes OS plus qu'un système sécurisé.

Notre but est de laisser le choix à l'utilisateur. Ce dernier peut en effet installer Whonix Vms qui permet d'utiliser Internet de manière anonyme avec Tor, mais nous avons aussi le projet d'ajouter des fonctionnalités présentes dans Tails comme l'effacement de la RAM à l'extinction ou la compatibilité avec Gnome et les BIOS UEFI.

Qubes OS est un système pour les utilisateurs avancés, voire experts, pensez-vous faire une version un plus facile à prendre en main ?

Oui, nous faisons actuellement beaucoup d'efforts pour faire en sorte de simplifier Qubes OS particulièrement au niveau de l'interface utilisateur et de l'expérience utilisateur (UI/UX) [NDLR : un très bon article pour tout comprendre ici : https://goo.gl/3Nne6o]. Dans la prochaine version 4 de Qubes OS, nous avons repensé notre approche du Qubes Manager. Notre but est de prendre les fonctions de l'actuel Qubes Manager et de les intégrer de manière plus transparente au bureau pour rendre le tout plus intuitif et facile à utiliser.

Dans votre rubrique Download, nous avons vu un fichier Qubes Live USB. Qu'est-ce que c'est ?

Qubes Live USB est une version permettant de ne rien installer sur le PC cible, mais elle est encore en version alpha et n'a pas été mise à jour depuis un certain temps. La plupart des utilisateurs préféreront installer une version normale de Qubes OS. Notez cependant que même les versions normales peuvent être installées sur une simple clé USB [NDLR : en branchant une clé de 32 Go sur le PC et en installant les fichiers depuis le DVD]. C'est un moyen efficace pour créer une installation « portable » et tester l'OS sur différents matériels.

Lors du lancement vous parliez de Qubes OS comme d'un système «raisonnablement sécurisé». Comment le définiriez-vous en 2016 ?

Nous définissons toujours Qubes OS comme « raisonnablement sécurisé », car nous croyons qu'un système ou un logiciel complètement et parfaitement sécurisé est actuellement impossible. Dire le contraire serait tromper l'utilisateur. C'est pour cela que nous avons sciemment choisi ce slogan modeste même si Qubes OS a été décrit comme le système le plus sécurisé du monde par le site http://motherboard.vice.com.

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

VOTRE MEILLEUR AMMYY À DISTANCE

Besoin de prendre le contrôle d'un ordinateur à distance pour aider un ami ou récupérer des données qui vous appartiennent ? Au lieu de chercher dans les logiciels compliqués ou payants (ou les deux !), essayez Ammyy Admin. Simple et gratuit, ce dernier est en plus sécurisé...

Limité à 15 heures d'utilisation par mois, Ammyy Admin est la solution idéale si vous souhaitez accéder à un ordinateur à distance. Rien à voir ici avec un logiciel comme DarkComet (voir Pirate Informatique n°25) puisqu'il s'agit d'un programme « légitime », impossible à utiliser de manière malicieuse. Ammyy Admin vous permettra aussi bien de régler un problème sur le PC de tata Lydie que de récupérer un fichier important sur votre PC à la maison pendant vos vacances. Il faudra simplement que le poste cible soit allumé et qu'un ami accepte la connexion en cliquant sur un simple bouton.

UN LOGICIEL SÛR ?

Alors bien sûr, lorsqu'il s'agit d'un logiciel de contrôle à distance type VNC, on se pose toujours la question de la sécurité. Tout d'abord Ammyy est un programme russe et pas du tout open source, ce qui sera rédhibitoire pour certains utilisateurs (ceux-là préféreront sans doute www.tightvnc.com). Il est donc déconseillé de l'utiliser pour le travail même si des géants comme nVidia, General Motors ou Nokia figurent parmi les clients. Ensuite au niveau de l'interception des données par des tiers, le logiciel s'est doté du classique « combo » d'algorithmes AES 256 bits + RSA 2048 bits ainsi que d'un système de permissions (accès total, uniquement aux fichiers ou au bureau, etc.). Bien sûr, tout cela est automatique et très simple à prendre en main. Chose rare, vous ne serez pas embêté par votre antivirus ou votre pare-feu lors d'une connexion. La personne qui souhaite être aidée n'a qu'à lancer le programme sans installation (et même depuis une clé USB) et donner un code unique à son « sauveur » par téléphone par exemple.

LEXIQUE

***VNC :** **Pour Virtual Network Computing** ou «informatique virtuelle en réseau» dans la langue de Cyril Hanouna. C'est un système de visualisation et de contrôle d'un ordinateur à distance. Il est séparé en deux morceaux (même si Ammyy regroupe les deux dans son EXE): un client sur l'ordinateur «maître» et un serveur sur l'ordinateur «esclave».

Ammyy Admin est idéal pour aider une personne en difficulté sur son PC. Qu'il s'agisse d'un problème à régler depuis le Panneau de configuration ou une mise à jour de l'antivirus, Tata Lydie peut compter sur vous.

PAS À PAS

Première connexion avec Ammyy Admin

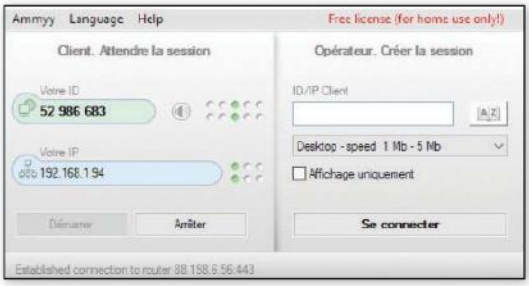
CE QU'IL VOUS FAUT

AMMYY ADMIN

OÙ LE TROUVER ? :
www.ammyy.com

DIFFICULTÉ :

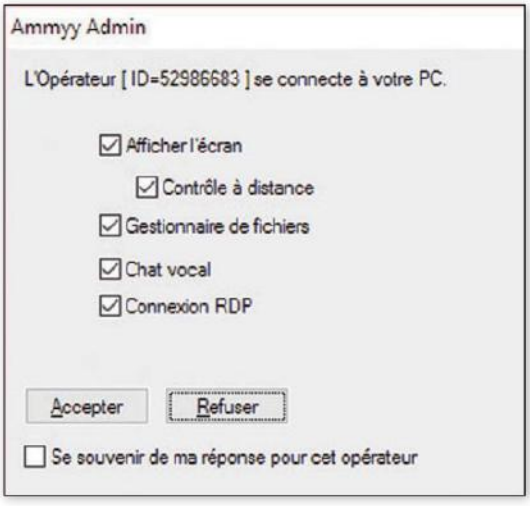
01 LE CODE UNIQUE



Commencez par lancer le programme sur les deux ordinateurs. Sur le PC cible, il faudra bien sûr que quelqu'un fasse la manipulation. Notez que le programme ne s'installe pas et peut très bien se lancer depuis une clé USB. L'opérateur devant l'ordinateur cible doit alors donner son code (celui de la partie gauche) pour que vous puissiez le taper das la partie droite du logiciel. Sur un réseau local, il est possible d'utiliser l'IP pour plus de réactivité.

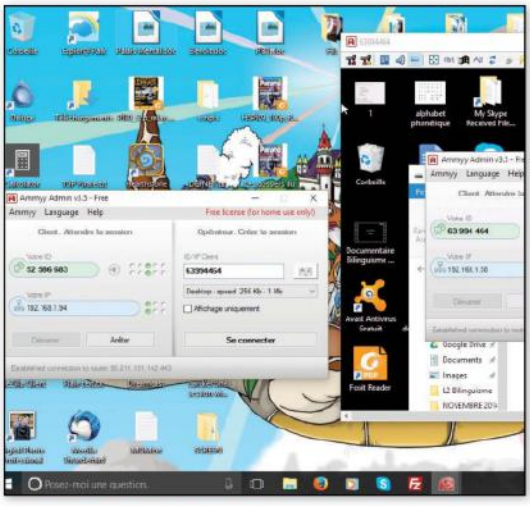
02 LA CONNEXION

Réglez ensuite la vitesse de votre connexion Internet (**<5Mb** par exemple) dans le menu déroulant et faites Se connecter. Un message demandant la permission va alors s'afficher sur le PC cible pour accepter ou non la connexion ainsi que de spécifier les autorisations (affichage de l'écran, accès aux fichiers, etc.) En quelques secondes, le bureau du PC cible va s'afficher dans le bureau du PC maître en mode fenêtré.



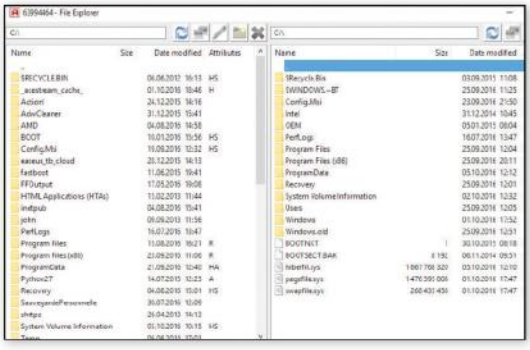
03 LES OPTIONS

Ne vous en faites pas pour le fond d'écran qui disparaît, il s'agit d'économiser la bande passante, il reviendra automatiquement. Dans cette fenêtre, vous pourrez faire comme si le bureau distant était le vôtre, mais aussi passer en mode plein écran, activer le tchat vocal, régler les paramètres du presse-papier, les options graphiques, etc.



04 UN GESTIONNAIRE DE FICHIERS

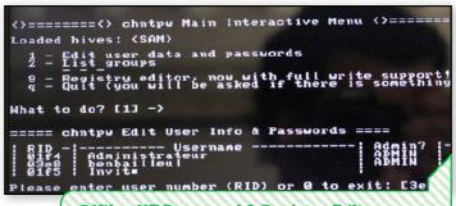
Mais vous pouvez aussi accéder à un gestionnaire de fichiers avec à gauche l'arborescence de votre PC et à droite, celui du PC cible. Pratique pour rapatrier des fichiers sans utiliser le mode graphique. Car comme tous les logiciels de ce genre, vous constaterez un petit temps de latence entre le moment de votre clic de souris et le moment où celui-ci est pris en compte.



OUTREPASSER LE MOT DE PASSE DE WINDOWS

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

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



Offline NT Password & Registry Editor permet aussi de réinitialiser le mot de passe de Windows, mais il s'avère un peu dur à prendre en main

DÉBLOQUER VOTRE WINDOWS

Dans notre n°26, nous vous avions parlé de Offline NT Password & Registry Editor, un logiciel permettant de réinitialiser le mot de passe des comptes utilisateurs de tous les Windows de NT jusqu'à 10 en passant par XP. Plutôt rugueux à prendre en main, un lecteur nous a fait parvenir une solution plus simple qui fonctionne à merveille avec tous les Windows récents. Bien sûr, cette astuce ne fonctionnera qu'avec un compte local et pas avec le mot de passe du compte Microsoft (solution que nous déconseillons), mais cela vous permettra de vous sortir d'un mauvais pas.

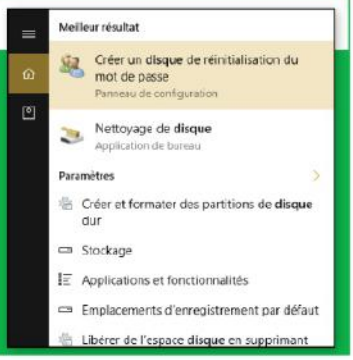
Merci à Jonathan Defer pour cette idée d'article et pour ses captures !

LEXIQUE

***COMPTE MICROSOFT :** Depuis Windows 8, Microsoft propose deux solutions pour ouvrir votre session : le mot de « passe local », le classique et le mot de passe Microsoft. Ce dernier permet de synchroniser vos données avec d'autres appareils Microsoft par exemple, mais savoir que son mot de passe repose dans les serveurs de Microsoft ne nous enchante pas.

LA CLÉ USB «PENSE-BÊTE»

Si vous n'avez pas envie de retenir votre mot de passe, il est possible de créer une clé USB qui fera office de «pense-bête» si vous oubliez votre mot de passe Windows. Dans le champ **Rechercher** de votre Windows, tapez **mot de passe** et sélectionnez **Modifier votre mot de passe Windows**. Sur la nouvelle fenêtre, cliquez à gauche dans **Créer un disque de réinitialisation de mot de passe** (pour Windows 10, il sera plus simple de taper **disque** dans le champ de recherche). Faites deux fois **Suivant**, tapez votre mot de passe et laissez Windows opérer. Un fichier PSW sera présent sur votre support amovible. Mettez cette clé en lieu sûr...



PAS À PAS

Windows ouvre-toi !

CE QU'IL VOUS FAUT

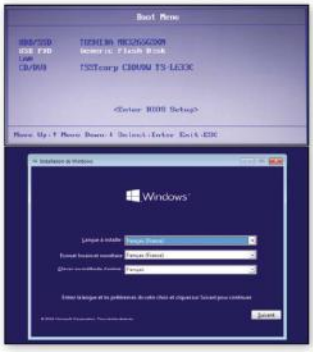
LE CD D'INSTALLATION DE WINDOWS

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

DIFFICULTÉ :

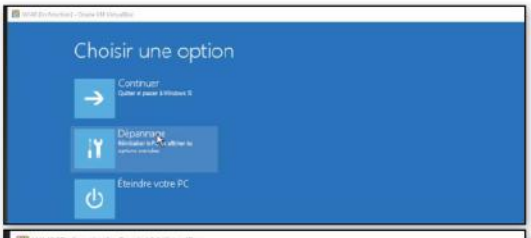
01 LE DVD D'INSTALLATION

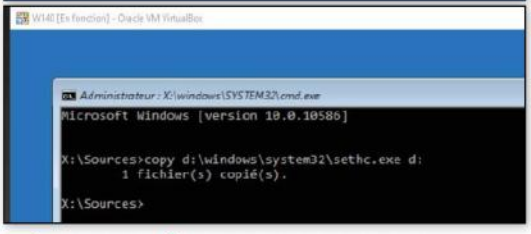
Notre tuto concerne Windows 10, mais vous pouvez faire cette manipulation avec tous les Windows récents. Il faudra vous munir du CD d'installation de Windows. Si vous ne l'avez pas (version OEM) ou si vous l'avez perdu, vous pouvez toujours télécharger une version «pirate» de Windows puisque vous l'avez acheté, mais vous pouvez aussi créer un DVD de réparation depuis un Windows identique au vôtre. Bootez votre PC depuis le lecteur optique en modifiant les paramètres de votre BIOS.



02 LES TOUCHES RÉMANENTES

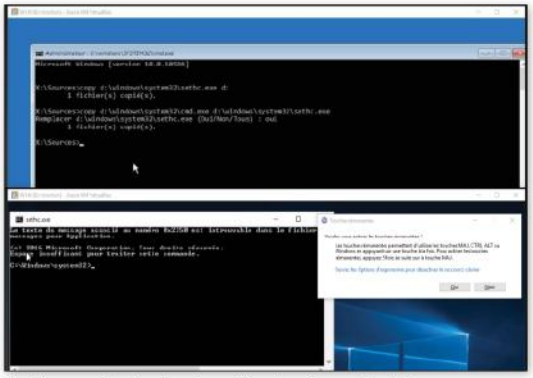
Choisissez la langue du système, mais ne faites pas **Installer maintenant**, choisissez plutôt **Réparer l'ordinateur**. Dans **Dépannage**, sélectionnez **Options avancées** puis **Invite de commande**. Le but est de copier le fichier des touches rémanentes (sethc) qui se trouve dans C: (l'emplacement de Windows). Tapez la commande suivante: **copy c:\windows\system32\sethc.exe c:**





03 DERNIÈRE MANIPULATION

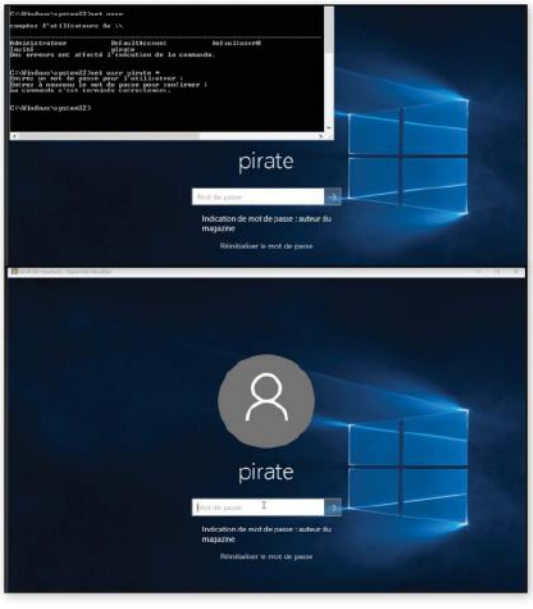
Ensuite, nous allons remplacer le fichier copié par le fichier contenant l'invite de commande en faisant **c:\windows\system32\cmd.exe c:\windows\syetem32\sethc.exe** Validez et tapez **Oui** (ou **y** si vous avez une version anglaise).



Redémarrez l'ordinateur jusqu'à voir votre session (si vous ne voyez pas de bouton, tapez **exit**). À l'affichage de votre nom et du mot de passe, tapez 5 ou 6 fois de suite sur la touche **Shift** (ou **Maj**) pour accéder à l'invite de commande.

04 CHANGEZ VOTRE MOT DE PASSE

Pour terminer, il suffit de taper la commande suivante pour enregistrer votre nouveau mot de passe: net user [votre nom de session] [votre nouveau mot de passe], par exemple **netuserpirateFh8&Pjk58n@p^**. Après avoir validé, faites **exit** pour fermer la console. Vous n'avez plus qu'à entrer votre nouveau mot de passe pour accéder à votre session. Bravo, vous avez récupéré votre environnement sans avoir perdu de fichiers!

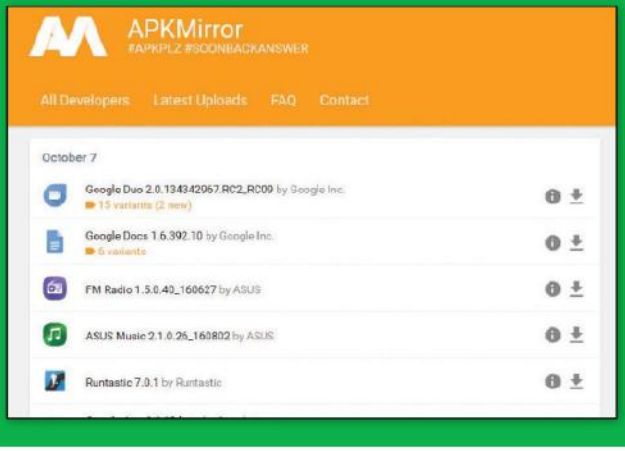


#1 L'ancienne version d'une appli Android

AVEC APKMIRROR

Une ou plusieurs de vos applis Android refusent de fonctionner ou ne proposent plus les fonctionnalités que vous aimiez bien? C'est parfois le problème avec ces mises à jour automatiques! Il se peut que votre version d'Android soit un peu vieille (à moins qu'il ne s'agisse d'une Custom ROM?), mais parfois ce type de problème arrive sans raison. La solution? Remonter dans le temps et télécharger une version de cette appli au format APK sur APKMirror! N'oubliez pas d'activer l'installation depuis les sources inconnues sur votre appareil. Attention, les mises à jour permettent de corriger des bugs ou des failles. A utiliser à vos risques et périls...

Lien : **www.apkmirror.com**



#2 Une Pirate Box facile

AVEC PIRATEBOXLIVE

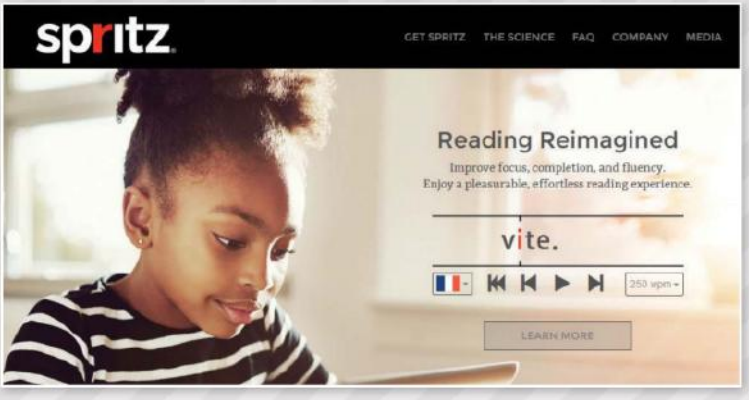
Une Pirate Box est une machine indépendante d'Internet permettant de s'échanger des fichiers sans restriction avec ceux qui veulent s'y connecter. Une sorte de disque dur couplé à un routeur. L'idée a germé en 2011, mais elle a su évoluer: pour arroser un quartier ou une résidence étudiante de contenus multimédia, fournir à des villages reclus de quoi échanger des données, mais aussi stocker des livres ou des bulletins d'information, etc. Si vous souhaitez vous faire une Pirate Box pourquoi ne pas le faire simplement avec ce Live CD et un vieux PC? Si vous souhaitez en savoir plus sur ces appareils et savoir comment cela fonctionne, demandez-nous un tuto pour le prochain numéro : benbailleul@idpresse.com

Lien : **https://goo.gl/P38WDu**

#3 Hackez votre cerveau

AVEC SPRITZ

Il y a bien longtemps, nous vous avions parlé de différentes techniques de biohacking (*Pirate Informatique n°11*), mais ici il s'agirait plutôt de dompter votre cerveau pour apprendre à lire plus rapidement. Une personne normale lit environ 200 mots par minutes, mais avec Spritz, vous pourrez essayer de lire jusqu'à 700 mots/minutes avec une facilité déconcertante et bien plus efficacement. Il s'agit en fait d'un logiciel qui va afficher les mots un par un en les «alignant» grâce à une lettre rouge placée au milieu. Fini les micros temps morts lorsqu'il s'agit de bouger les yeux pour atteindre le prochain mot. Le système est très au point (essayez vous-même sur la page d'accueil en français avec 350 mots/minutes et augmentez au fur et à mesure !) et les applis compatibles sont disponibles sur iOS, Android et Windows Phone.
Merci à Korben.info pour le tuyau !



Lien : **http://spritzinc.com**

#4 Centralisez vos données confidentielles

AVEC ENPASS

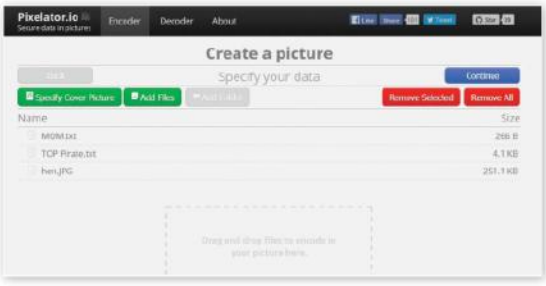
Si vous souhaitez éviter de stocker vos mots de passe en ligne sur un cloud chiffré comme Lastpass ou Dashlane, Enpasse devrait vous combler. Tout se fait en local dans une base SQLite chiffrée en AES 256 bits. Vous pouvez y placer vos identifiants, mais aussi vos codes de cartes bancaires ou n'importe quelles autres données sensibles. Pour y accéder depuis vos autres appareils, vous pouvez vous y connecter en utilisant Webdav ou un service de cloud comme Dropbox, Google Drive, etc. Bien sûr, l'appli permet un remplissage automatique des formulaires, un générateur de mot de passe et un nettoyeur de presse-papier.

Lien : **www.enpass.io**

#5 Cachez des documents dans une photo

AVEC PIXELATOR

Si vous avez l'habitude de nous lire, vous savez que nous aimons la stéganographie. Cette technique consiste à cacher des documents dans une photo par exemple. Les .jpeg peuvent en effet facilement intégrer des fichiers sans éveiller les soupçons, puisqu'avec un APN récent on peut maintenant trouver des clichés de plus de 10 Mo. Faites **Specify Cover Picture**, sélectionnez votre image puis un ou plusieurs documents avec **Add Files**. Cliquez sur **Continue** et mettez un mot de passe si le coeur vous en dit.



Lien : **https://pixelator.io**

#6 Kali Linux sur votre navigateur

AVEC KALIBROWSER

Envie de voir ce que donne Kali Linux? Au lieu de l'installer ou de l'utiliser en mode LiveCD, le spécialiste réseau Jerry Gamblin a créé KaliBrowser, une version permettant d'être lancée dans un simple navigateur, même sous Windows. Pour en profiter, il faudra utiliser les outils de virtualisation Kali Docker, OpenBox ou NoVNC, mais la performance mérite d'être saluée. Suivez notre lien pour en savoir plus sur les méthodes de déploiement...

Lien : **https://goo.gl/xzqe7z**

#7 Partagez en P2P

AVEC REEP.IO

Vous avez un gros fichier à envoyer, mais vous n'avez pas de cloud et votre client mail refuse de prendre en charge les pièces jointes si lourdes ? Pas de problème avec Reep.io qui permet d'envoyer n'importe quel fichier à un camarade via WebRTC. Il suffit de spécifier votre document puis d'envoyer le lien à votre ami. Votre PC devra rester allumé pendant le transfert. Bien sûr, tout cela est chiffré !

Lien : **https://reep.io**

NOUVEAU FORMAT, NOUVEAU DESIGN

ENCORE PLUS DE TUTOS, DE TESTS, DE CONSEILS, DE TRUCS ET D'ASTUCES !

DÉJÀ EN KIOSQUES

CACHEZ CES VISAGES...

Créée par le Guardian Project, ObscuraCam est une application photo pour les appareils Android. Cette dernière peut reconnaître et brouiller les visages sur les photos et vidéos dans le but de protéger l'identité des personnes.

Project Guardian est une association faisant la promotion de logiciels open source dans le domaine du respect de la vie privée. Parmi leurs applications on se souvient notamment de Orbot (Tor pour Android) ou ChatSecure. Cette fois, nous allons vous parler d'ObscuraCam, une app permettant de masquer automatiquement les visages sur vos clichés ou vidéos. Par pousser le concept encore plus loin, ObscuraCam va aussi effacer les métadonnées concernant la position géographique et le type d'appareil qui a été utilisé. Que vous soyez un citoyen lambda, un activiste ou une organisation humanitaire, ce type d'appli, comme toutes les applis de Project Guardian, vous aidera à faire respecter votre vie privée et à protéger vos proches. Le système de reconnaissance faciale d'ObscuraCam ne fonctionne pas toujours bien, mais vous pouvez faire des modifications à la main et sélectionner le type de masque que vous désirez. Si c'est le lieu où se déroule l'action qui doit être masqué, c'est aussi possible.

PAS À PAS

Les options d'ObscuraCam

OBSCURACAM

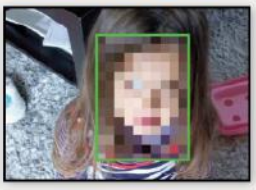
OÙ LE TROUVER ? : **https://guardianproject.info**

DIFFICULTÉ :

01 LE MENU

L'appli ne nécessite pas l'accès root. Dans le menu vous aurez le choix entre prendre une nouvelle photo (qui sera automatiquement traitée par ObscuraCam) ou ouvrir une photo/vidéo déjà existante. Commençons par une photo...

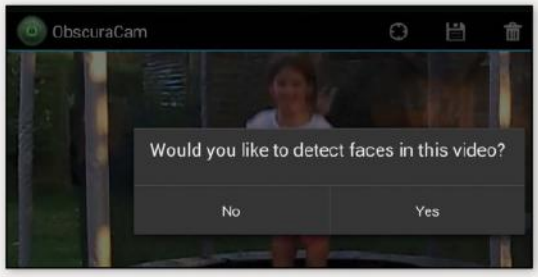
02 LA DÉTECTION DES VISAGES



L'appli 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 2 différents masques: une pixellisation forcée ou une sorte de postiche virtuel (lunette + gros nez).

03 ET POUR LES VIDÉOS ?

Pour les vidéos, le processus est un peu plus compliqué puisqu'il faudra que l'appli calcule la position des visages à chaque frame. Pour les vidéos un peu longues, cela peut prendre un certain temps mais cela fonctionne très bien...



UN PLAYER POUR TOUS LES RÉUNIR

Vous êtes inscrit à plusieurs services de streaming et vous en avez assez de switcher à chaque fois que vous voulez écouter une chanson ? Harmony propose de regrouper vos comptes Spotify, Sound Cloud Google Music et vos MP3 en local sur une même interface.

Si vous êtes un cœur d'artichaut et que vous n'arrivez pas à choisir un seul et unique service de streaming, Harmony pourrait être la solution. Il unifie différents services de streaming sur une même plate-forme. Vous pourrez profiter de vos comptes Spotify, SoundClound, Google Music et comme tout bon player qui se respecte, vos MP3 stockés en local. Petit point non négligeable : Harmony récupère vos playlists déjà créées sur les services de streaming. Il peut afficher vos musiques à la manière CoverFlow d'iTunes. En parlant d'iTunes, nous pouvons regretter qu'Apple Music ne soit pas encore disponible sur Harmony. Précisons tout de même que quand vous écoutez une musique sur Harmony, vous ne streamez pas via vos comptes. Le soft joue les musiques en provenance de YouTube. Mais le son reste tout à fait correct. Quant au service Lastfm pour ceux qui ne connaissent pas, c'est surtout un service de recommandations musicales. Il va vous fournir des statistiques sur vos habitudes d'écoute et sera à même de vous conseiller de nouveaux artistes.

PAS À PAS

Utiliser Harmony

HARMONY
OÙ LE TROUVER ? : **http://getharmony.xyz**
DIFFICULTÉ :

01 CONNECTER SES COMPTES

La connexion sur Spotify et SoundCloud se fait de manière classique avec vos identifiants. Mais pour utiliser Google Music, il faudra vous rendre à **https://goo.gl/Nt7SrF** et générer un mot de passe d'application. C'est ce dernier qui vous permettra de vous connecter à votre compte Google Music sur Harmony. Pour activer le mode CoverFlow, cochez **Enable CoverFlow (beta).**

02 VOS PLAYLISTS UNIFIÉES

Peu importe le nombre de playlists que vous avez sur chaque serveur de streaming, vous pourrez les retrouver sur Harmony. Chaque playlist possède un petit logo qui permet de reconnaître à quel site de streaming elle est associée. Quelque que soit la playlist jouée, vous pouvez basculer entre le mode liste et le mode CoverFlow.

03 LES PLAYLISTS INTELLIGENTES

Si vous êtes abonné à des playlists intelligentes, elles se retrouveront également sur Harmony. Mais malgré tout, la fonction reste sommaire. Impossible d'ajouter ou de supprimer un titre ou une playlist. Il faudra vous rendre sur le site du service concerné pour effectuer vos changements. S'ils ne se répercutent pas sur Harmony, cliquez sur la roue crantée puis sur **Reset cache and settings**.

WEBTORRENT DESKTOP, LE POP-CORN TIME ULTIME ?

Le streaming a ça de bien qu'on peut profiter de son contenu immédiatement. Mais il ne permet pas de garder ledit contenu sur son ordinateur. WebTorrent Desktop réunit les deux procédés et pour tous les formats : vidéos, musiques, livres....

Vous qui êtes friand de téléchargements, l'attente est parfois trop longue pour obtenir vos précieux fichiers. Le streaming peut être la solution, mais pas possible de les garder sur son ordinateur. Pourquoi ne pas profiter de son contenu immédiatement et laisser le téléchargement se faire en arrière-plan ? WebTorrent Desktop permet tout ça. Lancez votre téléchargement et profitez tranquillement du début de votre série, film ou chanson en attendant que le reste se télécharge. Bien entendu, la fluidité dépend de la connexion, mais ça marche plutôt pas mal même s'il est toujours en bêta. Et comme tout bon client torrent, vous continuez à seeder pour les copains tant que le soft reste en arrière-plan. Et cerise sur le streaming, WebTorrent Desktop est compatible AirPlay, Chromecast et DNLA. Il est gratuit, sans aucune publicité et le code source est disponible sur Github. De plus, vous pouvez créer vos propres torrents très facilement et commencer à les seeder.

PAS À PAS

Maîtriser WebTorrent Desktop

WEBTORRENT DESKTOP

DÙ LE TROUVER ? : **https://webtorrent.io/desktop**

DIFFICULTÉ :

01 TÉLÉCHARGER-STREAMER

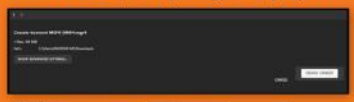
Comme tout client torrent classique, WebTorrent récupère les fichiers torrent et magnet. Faites glisser le fichier sur la fenêtre et le téléchargement débute automatiquement. Vous commencez immédiatement à seeder. Si vous en avez marre, vous pouvez supprimer le torrent via la petite croix qui apparaît en passant la souris sur ledit torrent. Le clic droit apporte d'autres options comme copier le lien du magnet (**Copy Magnet Link to Clipboard**) ou afficher le dossier du torrent (**Show in Folder**).

02 LIRE PENDANT LE TÉLÉCHARGEMENT

Dès que le téléchargement commence, vous pouvez le lire. Cliquez sur l'icône Play et c'est parti. Bon, pour nos tests, le soft a échoué à lire nos vidéos. Il nous bascule sur VLC. Mais VLC ou WebTorrent, c'est pareil: vous pouvez vous balader à loisir dans la vidéo même si ce n'est pas téléchargé. Le logiciel va simplement télécharger la partie que vous voulez voir en priorité. C'est fluide et assez efficace. En revanche, pour les musiques (un album entier), aucun souci: il se lit via WebTorrent et vous pouvez changer de chanson à loisir également.

03 CRÉER SES TORRENTS

Quoi de mieux pour la communauté que de partager ses propres torrents? C'est très simple à réaliser avec le soft. Cliquez sur File puis Create New Torrent from File, choisissez votre fichier et c'est parti. Faites un clic droit sur le torrent fraîchement créé et copiez le lien magnet ou enregistrez le torrent pour le partager via **Save Torrent File As...**

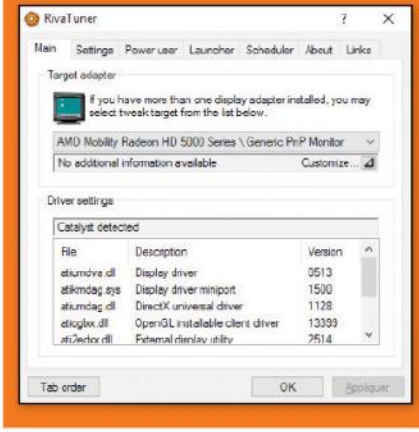


#1 Overclockez votre carte graphique

avec RivaTuner

Vous avez aimé notre article sur l'overclocking dans *Pirate Informatique n°28* ? Peut-être aimeriez-vous aller plus loin et overcocker votre carte graphique? Eh oui, croyez-le ou non, mais la plupart des gens utilisent leur GeForce ou Radeon pour jouer et pas pour cracker des mots de passe! RivaTuner ne se limite pas aux cartes nVidia et permet aussi d'overclocker les cartes AMD. Le logiciel permet d'outrepasser les fréquences normales et de modifier indépendamment le cadencement des shaders et celle du GPU. De l'overclocking pour les utilisateurs exigeants...

Lien : **www.guru3d.com**

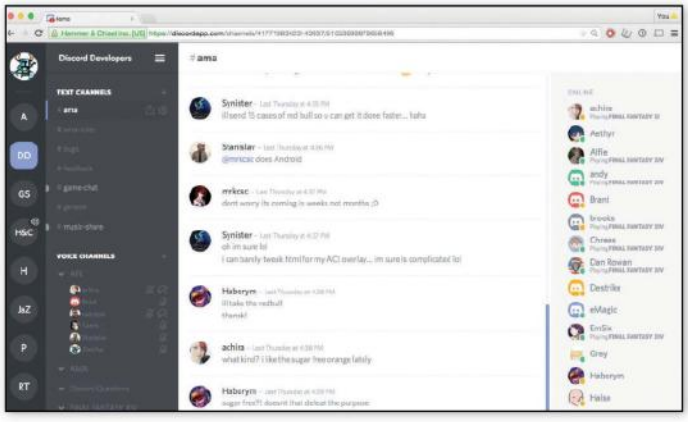


#2 Tchat pour gamer

avec Discord

Discord va vous faire oublier Teamspeak. Disponible pour presque toutes les plateformes, ce logiciel permet de converser lors de parties en réseau tout en s'intégrant parfaitement dans l'environnement. Pas besoin de basculer vers le bureau de Windows pour faire des ajustements de son ou ajouter un retardataire.Bien sûr, vous n'êtes pas obligé de jouer pour appeler vos amis. Plus fort, Discord est aussi disponible via le navigateur et comporte une couche de chiffrement. Seul point noir (sauf pour les gamers), le service ne permet pas la visio.

Lien : **https://discordapp.com**



#3 Un clone de Spotify gratuit

avec NoiseQ

Nous ne sommes pas peu fiers de notre découverte! Dans la longue liste des «clones de Spotify gratuits qui vont se servir dans les vidéos de YouTube», voici NoiseQ. Ce service en ligne va chercher les chansons et les clips de votre choix dans les différentes bases de données dont elle dispose. Vous pouvez paramétrer des playlists, avoir accès à des radios ou à des artistes similaires à ceux que vous aimez. L'interface est jolie et réactive. Le sans-faute pour les mélomanes.

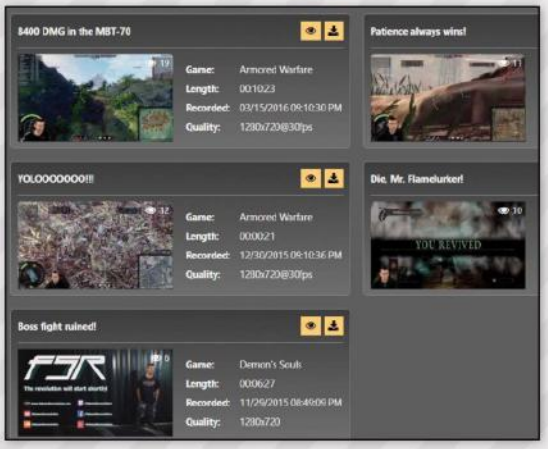
Lien : **http://noiseq.com**

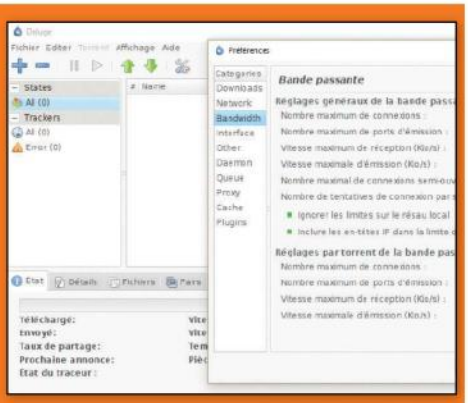
#4 Enregistrer des émissions sur Twitch

AVEC TWITCH LEECHER

Vous aimez regarder les autres jouer aux jeux vidéo sur Twitch (comme Nagui)? Vous aimez les émissions qui sont diffusées sur cette plate-forme? Alors, Twitch Leecher est fait pour vous. Faites les recherches directement depuis l'interface et téléchargez tout le contenu que vous souhaitez. Les abonnés qui payent peuvent même entrer leurs identifiants pour récupérer les vidéos associées à leur compte. Comme au temps des magnétoscopes, on peut même programmer les enregistrements pour ne rien rater.

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





#5 Un client Torrent léger comme l'air

AVEC DELUGE

Très populaire auprès des utilisateurs de seedbox, Deluge conviendra parfaitement à ceux qui sont devenus allergiques à µTorrent ou qBitorrent. Il propose aussi un grand nombre de plugins permettant d'ajouter des fonctionnalités et d'automatiser de nombreuses opérations (renommer, récupérer des métadonnées, copier, etc.) Depuis le menu **Daemon** des **Paramètres**, il est possible de régler un port de connexion pour pouvoir agir à distance sur vos Torrents avec un navigateur et NoIP ou avec l'application Android Transdroid.

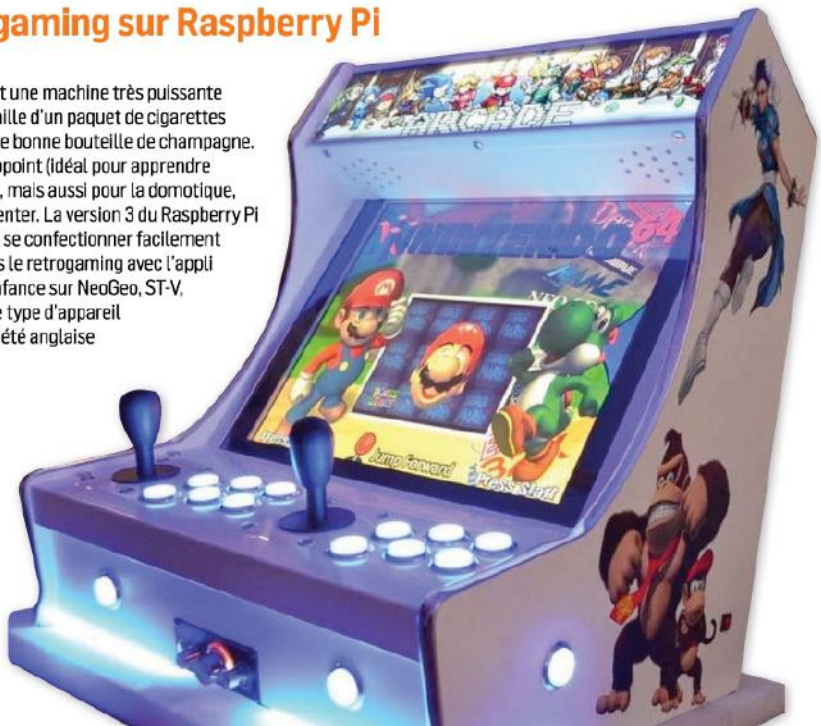
Lien : **http://deluge-torrent.org**

#6 Du retrogaming sur Raspberry Pi

AVEC RETROPIE

Le Raspberry Pi est une machine très puissante pour un PC de la taille d'un paquet de cigarettes et pour le prix d'une bonne bouteille de champagne. On peut l'utiliser comme un PC d'appoint (idéal pour apprendre Linux avec la distribution Raspbian), mais aussi pour la domotique, la robotique ou en tant que mediacenter. La version 3 du Raspberry Pi est tellement puissante, qu'on peut se confectionner facilement une borne d'arcade spécialisée dans le retrogaming avec l'appli Retropie. À vous les jeux de votre enfance sur NeoGeo, ST-V, CPS-2, N64, Super Nintendo, etc. Ce type d'appareil est tellement à la mode qu'une société anglaise vend des bornes toutes faites : www.tinyarcademachines.com. Ce n'est pas donné (plus de 700€ pour une borne deux joueurs), mais c'est la classe !

Lien : **https://retropie.org.uk**



X-MATÉRIELS

> Gablys Lockit

Gablys Lockit est un petit dispositif utilisant la technologie Bluetooth 4.0 pour verrouiller automatiquement votre ordinateur lorsque vous vous éloignez de lui. Plus besoin de taper votre mot de passe à votre retour ou à se soucier de la confidentialité de vos données. Idéal pour les parents qui craignent la curiosité de leurs tout petits, des professionnels qui veulent éviter les fuites de données ou même pour Monsieur Tout-le-Monde qui veut s'assurer que ses données ne sont pas laissées sans surveillance. L'appareil est très léger (13 g) et peut s'accrocher en pendentif ou en porte-clés. Il fonctionne avec une pile plate CR2032 qui procure une autonomie d'un an selon le constructeur. Votre PC n'est pas compatible avec le Bluetooth? Pas de problème, puisqu'un dongle (compatible uniquement avec les Windows 7 et supérieur) est fourni dans la boîte. Depuis l'interface, il est possible de paramétrer la distance à laquelle votre écran se verrouillera (maximum 30 mètres), de visualiser rapidement si le cadenas est connecté ou hors ligne et de consulter le niveau de batterie. Très fort : si quelqu'un touche à votre ordinateur quand il est verrouillé, une photo de l'importun est automatiquement prise et vous êtes averti de la tentative d'intrusion par une notification !

Prix : **45 €** www.gablys.com

Kingston Ironkey D300, PAS LA CLÉ USB DE MONSIEUR TOUT-LE-MONDE

Vous aimez ça les clés USB permettant un chiffrement de vos données ? Et bien, voici la D300 de chez Ironkey (récemment racheté par Kingston). Vu son prix, elle ne s'adresse pas au grand public, mais si vous êtes un professionnel qui doit stocker des données confidentielles, c'est le top du top. Compatible avec la norme USB 3.0, cette gamme de clés dispose d'une coque en zinc ultra résistante et étanche. Immunisée contre les attaques de type BadUSB, la D300 est certifiée FIPS 140-2 Level 3. En pratique, cela signifie que la clé est capable d'encoder les données stockées (AES 256 bits), mais également de détruire les données stockées en cas d'intrusion détectée.

Prix : **de 125€ (8Go) à 512€ (128Go)**
www.kingston.com

Raspberry Pi 3 In-a-Box Kit Officiel, TOUT-EN-UN !

Si vous avez l'habitude de nous lire, vous connaissez notre amour pour le Raspberry Pi, ce micro-ordinateur créé dans le but d'encourager l'apprentissage de l'informatique aux personnes avec peu de moyens. PC d'appoint pour certains, carte programmable et media center pour d'autres, le Raspberry Pi peut tout faire. Pour fêter le 10 000 000e Raspberry vendu dans le monde, la boutique Kubii propose un kit avec tout le nécessaire pour pleinement profiter de votre appareil: le Raspberry Pi 3, une carte micro-SD de 16 Go avec différents systèmes, un boîtier de protection, l'alimentation officielle 2,5 A, un câble HDMI de 1 mètre, un clavier (malheureusement QWERTY), une souris et le livre *Adventures in Raspberry Pi* dans la langue de Kim Kardashian. Si vous avez de la chance, vous pourrez tomber sur une promotion...

Prix : **150 €** www.kubii.fr

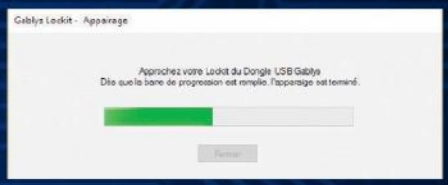
NOTRE TEST EXCLUSIF

Gablys Lockit
Un cadenas virtuel sur votre PC

Connue pour ses appareils connectés, la société Bordelaise Gablys présente son Lockit : un cadenas virtuel permettant de verrouiller son ordinateur lorsque vous vous en éloignez...

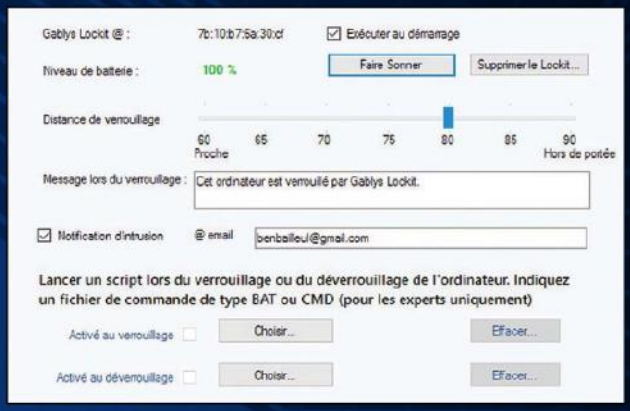
#1 LES PRÉSENTATIONS

Le Gablys Lockit est livré dans une petite boîte contenant aussi le dongle Bluetooth 4.0 et la pile que vous devrez insérer dans le dispositif. Par contre, pas de logiciel (pourquoi pas un mini CD de 8 cm ? Il y avait la place!), il faudra le télécharger sur le site officiel. Rien de sorcier lors de l'installation, il suffit de suivre les instructions à l'écran et de redémarrer sans oublier de brancher le dongle dans un port USB libre. Si vous ne voyez pas la fenêtre qui montre la progression de l'appairage, redémarrez et rebranchez le dongle.



#2 LES PARAMÈTRES

Dans la zone de notification de Windows, vous verrez un pentagone en faisant un clic droit dessus, choisissez **Paramètres**... Depuis cette fenêtre, il est possible de faire sonner le Gablys (si vous l'avez égaré) de cocher la case permettant son exécution au démarrage de Windows et d'autres options comme la distance de verrouillage. Attention, l'unité de mesure est bizarrement le... pouce (80 pouces = environ 2 m). Plus bas, vous aurez aussi le choix d'activer des scripts au format BAT ou CMD. Vous pourrez par exemple planifier des tâches au verrouillage ou au déverrouillage (effacer la RAM, l'historique, afficher un journal, etc.)



#3 MAIS QUE FAIT LA POLICE ?

Enfin, si quelqu'un essaie de taper quelque chose sur votre clavier ou tente une intrusion, il sera pris en photo par la webcam ! Le cliché sera stocké dans le dossier **Images** de votre session, mais vous pouvez aussi être averti par e-mail ! Rentrez votre adresse dans le champ de la fenêtre **Paramètres**... et faites **Enregistrer**. Rien de mieux pour savoir s'il s'agit d'un brigand ou de la femme de ménage qui a passé un chiffon sur votre souris.

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

HACKING
ANONYMAT
PROTECTION

Le GUIDE 100% PRATIQUE du Pirate

- Tous les tutoriels
- Toutes les solutions

IDPRESSE
L 12730 - 31 - 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