+ EN CADEAU : 2 magazines complets offerts SUR LE CD

LES CAHIERS DU HACKER

PIRATE [INFORMATIQUE] // 29

PIRATE [INFORMATIQUE]

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

Les MEILLEURES RECETTES & ASTUCES SECRÈTES DES HACKERS

+ ZERONET, le nouveau réseau ANONYME

INTERNET
PROTÉGEZ VOTRE WI-FI DES SQUATTERS

ANONYMAT
MESSAGERIES INSTANTANÉES SÉCURISÉES

MATÉRIEL
DÉCOUVREZ LE NOUVEAU RASPBERRY PI 3

SOMMAIRE

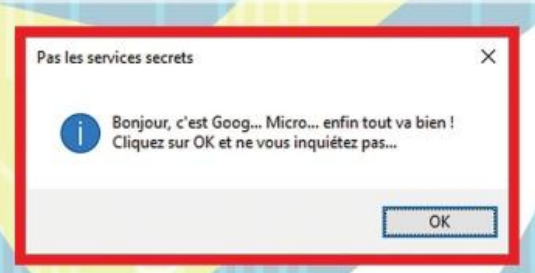
PROTECTION/ANONYMAT

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°29 – Mai/Juil. 2016

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

Directeur de la publication : David Côme
Emile A-239 : Benoît BAILLEUL
Jun A-266 : Yann Peyrot
Carter A-259 & Kat B-320 : Sergueï Afanasiuk & Stéphanie Compain
Correctrices : Claire Moynier & 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 ET AUX NOUVEAUX VENUS !

L'heure est plus que jamais au chiffrement ! Jusqu'alors réservées aux geeks, c'est dorénavant Monsieur et Madame Tout-le-Monde qui ont accès à ces technologies : WhatsApp et Viber proposent du chiffrement tandis qu'Apple se bat bec et ongles contre le gouvernement américain pour les données de ses clients. Ne nous y trompons pas, il s'agit d'un argument commercial plus que d'une vraie prise de conscience des grosses sociétés du Web, mais ne ne pouvons que nous réjouir de cette évolution. Ceux qui n'ont rien à cacher peuvent toujours étaler leurs vies sur la place publique, les autres sont de plus en plus protégés contre les pirates, les curieux ou les services secrets (de plus en plus indiscrets).

Dans ce numéro, nous avons donc décidé de vous proposer un comparatif des solutions de tchats chiffrés (avant d'attaquer le chiffrement de données à la volée dans le prochain magazine), mais aussi de faire le point sur le chiffrement des téléphones portables. Nous continuons aussi nos séries sur la récupération de mots de passe et sur l'univers Kali Linux. Enfin, de nombreux lecteurs nous ont demandé des explications sur les notions de «social engineering» et de «chiffrement asymétrique» (clé publique/clé privée) ? Nous avons donc décidé de leur dédier un article.

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

Bonne lecture !

Benoît BAILLEUL.

HACKTUALITÉS

LE FBI GARDE SES RECETTES SECRÈTES

C'est bien connu, les services secrets et la police américaine n'aiment pas Tor. Ce «réseau en oignon» décentralisé permettant d'anonymiser les échanges sur Internet est en effet très complexe à casser et même si des attaques type «man-in-the-middle» existent, le réseau est sans cesse mis à jour pour colmater les brèches. Pourtant le FBI a dernièrement fait de gros progrès : un site pédopornographique caché a été mis sous surveillance par la police pour tenter de récupérer le maximum d'informations sur ses visiteurs. Cette opération a été un succès, mais les accusés et la justice américaine demandent des détails concernant la méthode utilisée. Refus catégorique du FBI qui n'aime pas trop donner ses petits secrets. En effet, ces données pourraient servir à colmater les failles et même à mettre en danger des enquêtes en cours ! Selon le FBI, les avocats ont suffisamment de détails pour permettre la défense des accusés, mais selon la justice, une erreur est vite arrivée. Et dans les 1300 adresses IP collectées, il ne faudrait pas accuser à tort un innocent...

CITATION

«C'est grâce à un lanceur d'alerte que nous avons maintenant ces informations. Ces lanceurs d'alerte font un travail utile pour la communauté internationale, ils prennent des risques, ils doivent être protégés»

- François Hollande, concernant les révélations des «Panama papers».

[NDLR : On raconte qu'Edward Snowden est tombé de sa chaise en entendant le Président français. Julian Assange s'est déboîté le zygomatique au même moment.]

WHATSAPP : CHIFFREMENT POUR TOUT LE MONDE !

Après avoir adopté une stratégie «tout gratuit» au début de l'année, WhatsApp propose maintenant le «tout chiffré». En effet, les utilisateurs de la très populaire application de messagerie détenue par Facebook peuvent maintenant profiter d'une fonctionnalité permettant de chiffrer les messages et pièces jointes échangés. Il s'agit en fait du même système de chiffrement bout à bout déployé dès 2014 et dérivé du protocole Signal (le chouchou d'Edward Snowden) sauf qu'il est maintenant disponible sur toutes les versions et en «cross platform». L'idée a fait son chemin puisque la messagerie concurrente Viber a annoncé le déploiement d'un chiffrement sur son service. Quelque chose nous dit que ce ne sera pas le dernier...

Un paradoxe américain, par notre ami Matt Bors

MEGA.NZ : LA FIN ?

Lancé il y a un peu plus de trois ans, le site Mega.nz était censé remplacer Megaupload, fermé par la police pour avoir trop longtemps permis de pirater du contenu multimédia. Or, Mega.nz n'a jamais eu le petit côté illégal et sulfureux de son grand frère. Kim Dot Com avait pensé son nouveau bébé différemment en proposant du chiffrement de bout à bout pour l'utilisateur et en utilisant des mesures bannissant les utilisations illégales. Pourtant la réputation de son créateur a provoqué sa mise à l'écart par ses investisseurs chinois, mais aussi le retrait de PayPal. Et sans cet intermédiaire, cela fait presque deux ans que les utilisateurs souhaitant s'offrir un compte payant sont bloqués. Selon Kim, les caisses sont vides et le service va bientôt fermer. Il conseille donc à tout le monde de faire des sauvegardes en attendant son nouveau service. S'agit-il d'une vengeance contre ses investisseurs ou d'un subtil moyen de récupérer des utilisateurs ?

HACKTUALITÉS

Le Parti Pirate a la parole

Porte-parole du Parti Pirate français depuis deux ans, Thomas Watanabe-Vermorel a répondu à nos questions sur l'actualité : de la fulgurante montée en puissance du PP islandais à la loi sur le renseignement en passant par l'affaire Apple contre FBI...

Le Parti Pirate (PP) français a-t-il des contacts avec les autres PP à l'étranger?

Sur le plan « institutionnel », le PP est membre du PP EU — fondé un peu avant les dernières élections européennes — et du PP international. Sur le plan humain, les connexions se font de façon diffuse et organique, et beaucoup sur Internet. J'ai par exemple d'excellents et nombreux contacts avec le PP du Brésil du fait de mon histoire particulière. La Belgique et l'Allemagne sont aussi très bien connues de nos militants. Nous recevons régulièrement les pirates au hasard de leurs voyages, Grecs, Américains, Colombiens...

Les PP d'Islande et de France partagent beaucoup de convictions communes (réforme du droit d'auteur, démocratie directe, protection de la vie privée, etc.) alors qu'est-ce qui manque à la France pour avoir un Parti Pirate fort?

Le modèle de la Vᵉ République est extrêmement bien conçu pour empêcher les nouvelles formations d'émerger. Rick Falvingue [NDLR : le fondateur du PP suédois] le rappelait d'ailleurs : l'absence de proportionnelle à tous les niveaux rend la Grande-Bretagne et la France particulièrement, terres ingrates, pour nos mouvements. Si vous souhaitez connaître la liste des entraves démocratiques que nous subissons, il vous faudra écrire un article tout entier !

Même si le Premier ministre islandais a été inquiété par l'affaire des Panama Papers, nous avons, en France aussi, des affaires comme ça...

Et de bien pires à mon avis ! La caste politique est très attentive à se protéger, y compris en dehors de ses propres camps. En Islande, ils ont mis en tôle leurs banquiers à la suite de 2008. En France, malgré le 4 août, nous restons très tolérants avec les privilèges des puissants. Mais on peut espérer que cette patience va toucher à sa fin.

On connaît la position du PP sur la loi sur le renseignement votée en mai suite aux événements de janvier. Non seulement cela n'a pas empêché le 13 novembre, mais cela laisse une porte ouverte à l'espionnage de masse.

Il est urgent de modifier en profondeur cette loi pour permettre une protection efficace des citoyens et lutter contre le terrorisme. Lorsque Cazeneuve commence à parler de darknet comme de Tor, on voit où il veut en venir. Faire passer des idées fascistes sous couvert de protection de la population. Cette loi est nécessaire puisqu'auparavant ce type de pratique officieuse était placé sous le coup du secret-défense et que personne n'avait son mot à dire. Avec cette loi ils ont validé l'intégralité des pratiques sans penser à la notion de sûreté. Cette notion, chère aux droits de l'homme, donne normalement la possibilité à un citoyen de se défendre contre l'État. Mais cette notion a disparu. Certes il existe des terroristes, certes il faut faire du renseignement, mais nous devons avoir le droit de nous défendre contre les institutions. Sans intervention d'un juge ou d'un organisme judiciaire, cette loi fait office de lettre de cachet.

Ne trouvez-vous pas les politiques dépassés au niveau technique lorsqu'on propose la suppression des WiFi ouverts, la suppression de Tor ou d'autres annonces à chaud? Cazeneuve ou Ciotti par exemple. N'ont-ils pas de conseillers ou ne peuvent-ils pas réfléchir un peu avant de parler?

Cela dépend. Cazeneuve sait très bien de quoi il parle mais il ment aux citoyens et aux députés qui eux n'ont pas les connaissances techniques. Mais il ne s'agit pas uniquement de technique, ils passent clairement à côté de ce qu'est l'essence d'Internet. C'est à la fois une barrière générationnelle, mais aussi une incompétence conceptuelle. Lorsqu'on en entend parler certains, on imagine que derrière une « fiche » a été mal digérée et recrachée.

Que pensez-vous de la posture d'Apple sur le chiffrement? Courageux ou opportuniste?

Il ne faut pas se leurrer : ils s'opposent à l'ingérence dans les données personnelles mais cette posture hypocrite est celle d'une mégacompagnie paranoïaque. Apple désire juste avoir la mainmise sur le maximum de données possible sans pour autant les partager avec un gouvernement. C'est une subtile campagne de communication. De toute façon, si vous souhaitez garantir des droits aux utilisateurs, il faut opter pour de l'open source. Apple c'est exactement le contraire.

Et pour les prochaines échéances électorales, avez-vous besoin de renforts?

Bien sûr, nous cherchons à grandir et nous souhaitons plus que jamais être présents aux législatives de 2017. Nous espérons faire mieux qu'en 2012 où nous étions présents dans 101 circonscriptions. En ce qui concerne d'éventuelles alliances, nous désirons co-construire avec des petits mouvements citoyens sans étiquette et sincères même si ce terme est souvent employé à tort et à travers par les grands partis.

OFFRE SPÉCIALE

Clés USB

Toute la collection de votre magazine préféré en **ÉDITION LIMITÉE**

34 MAGAZINES !

+ 7 Go de stockage offerts

Valeur : ~~145~~ euros

RECEVEZ VOTRE CLÉ POUR SEULEMENT

15 € (+ frais de port)

sur **www.pirate-informatique.com**

ATTENTION, LE NOMBRE DE CLÉS DISPONIBLES EST LIMITÉ

HACKTUALITÉS

FBI CONTRE APPLE : LE GRAND BLUFF

Depuis les récents attentats, «*la France a peur*». Et malheureusement la peur n'est pas bonne conseillère. Elle peut par contre servir à faire accepter n'importe quoi aux gentils moutons que nous sommes souvent. Aux USA, la peur du barbu sert de levier pour empiéter sur la vie privée des gens. Chez nous on applaudit et on veut faire pareil...

Le chiffrement des données est devenu pour les entreprises un argument commercial. Alors que la plupart des gens s'en moquaient comme de leur premier Pentium, les révélations d'Edward Snowden sur l'ampleur de l'espionnage électronique de la NSA ont commencé à faire bouger les lignes. Les solutions de chiffrement se démocratisent et ne sont plus réservées aux seuls geeks. On en parle même à la télévision et les médias traditionnels feignent de croire que le FBI n'arrive pas à pénétrer l'iPhone de Farook (le débile niveau 58 de de la tuerie de San Bernardino).

Trop content du coup de pub, le PDG d'Apple, Tim Cook, se pose en défenseur des données personnelles et refuse d'aider la police à pirater son propre matos. Le monde à l'envers.

Faire plier le plus fort...

Sachez premièrement qu'il existe des techniques permettant de pirater un iPhone (surtout une vieille version comme celle de Farook) dont le Nand Miroring qui consiste à copier une partie de la mémoire chiffrée sur un autre support pour se débarrasser de la restriction «on efface les données si 10 mauvais mots de passe sont

saisis» et ainsi faire du «brute force» les mains déliées. Bizarrement, quand ça a commencé à se savoir, le FBI a communiqué avoir déjà trouvé la solution. Alors pourquoi le FBI voudrait-il l'accès sur un téléphone qui ne pose pas de problème particulier à cracker ? Tout simplement pour faire jurisprudence et ainsi forcer Apple à avoir le droit d'accéder aux données contenues dans les futurs appareils de la marque qui, elles, seront sans doute plus compliquées à extraire. Le but pour le gouvernement américain est de placer une porte dérobée permettant un accès plus rapide, plus facile sur les téléphones du monde entier, car s'ils font plier Apple, qui d'autre s'opposera ? Le problème avec cette éventuelle porte dérobée (ou backdoor) c'est que si un pirate y a un jour accès, les données ne seront plus protégées du tout. Dans le camp d'en face on met dans la balance qu'*«aucun lieu ou coffre-fort n'est à l'abri d'un mandat ou d'un juge alors pourquoi un téléphone ?»*. Sauf que, fabriquez une clé pour un téléphone et c'est tous les autres que vous mettez en péril. En outre si Apple affaiblit son chiffrement, d'autres solutions vont émerger et ces chiffrements solides ne seront peut-être pas à la portée du grand public.

Les réactions en France?

Depuis cette histoire rocambolesque, en France, c'est l'effervescence. Le procureur de la République de Paris, François Molins, a cosigné une tribune dans le New York Times en parlant *«d'entrave à la justice»* concernant le refus d'Apple. Il ajoute : *«Avec tous ces logiciels de chiffrement, nous ne pouvons pas pénétrer dans certaines conversations, nous nous retrouvons face à un grand trou noir»*. Nous l'invitons à relire la Déclaration des droits de l'homme et du citoyen (article II), la Déclaration universelle de 1948, l'article 9 du Code civil, l'article 8 de la Convention européenne des droits de l'homme et le Journal de Mickey. Bernard Cazeneuve, de son côté, a apporté tout son soutien à l'administration de Barack Obama en disant qu'*«il faut impérativement trouver des procédures sous le contrôle de l'autorité du juge»*. Mais comment ?

Une mise sous séquestre des clés de chiffrement ? C'est le même problème si un jour ces clés tombent entre de mauvaises mains. Retour à la case départ. Et nous terminons par le meilleur, Eric Ciotti, député, président des Alpes-Maritimes et intellectuel de niveau -15 payé par vos impôts, propose un amendement pour forcer les constructeurs de smartphones à fournir les moyens de déchiffrer les appareils aux forces de l'ordre dans les affaires de terrorisme. En cas de refus : une amende de 2 millions avec interdiction de vendre leur came sur le territoire. Encore un qui a trop regardé le JT de Pernaut et qui n'y connaît absolument rien en ce qui concerne les nouvelles technologies. Son idée géniale est-elle même légale ? Ciotti s'en moque, les caméras sont sur lui.

Ils ont dit...

«Un ordinateur ne va jamais vous donner le nom d'un terroriste. C'est l'implication de la communauté et les enquêtes traditionnelles qui donnent des résultats.»

- Ed Davis, chef de la police de Boston (après l'attentat)

«Le FBI nous demande de fabriquer une nouvelle version de notre système d'exploitation afin de contourner des mesures de sécurité importantes. Entre les mauvaises mains, ce logiciel permettrait de débloquer n'importe quel iPhone. Cela reviendrait à créer une porte secrète, et même si le gouvernement promet qu'elle ne serait utilisée que dans ce cas, nous n'en avons aucune garantie.»

- Tim Cook, PDG de Apple

«Si Apple s'exécute, le gouvernement va demander la même chose à tous ceux qui ont l'audace de proposer une sécurité forte.»

- Extrait d'un communiqué de l'Electronic Frontier Foundation.

«On doit boycotter Apple jusqu'à ce qu'ils donnent le code de ce téléphone»

- Donald Trump, Twitté de son iPhone...

LA GRANDE MODE DU TCHAT CHIFFRÉ

Alors que nous vous parlons de la nécessité du chiffrement depuis maintenant 7 ans, les médias traditionnels ne s'en font l'écho que depuis quelques mois. Les révélations de Snowden ont en effet lancé une dynamique que les récents attentats n'ont pas freinée. Dans ce numéro nous allons donc parler des solutions de tchat chiffré avant de nous attaquer à d'autres types de chiffrement dans notre prochain numéro.

La mode est au chiffrement, on en parle même sur TF1 ! C'est devenu un vrai sujet de société et les lignes bougent. Réservées aux seuls geeks, les méthodes de chiffrement ont le vent en poupe depuis les révélations d'Edward Snowden, mais elles connaissent une popularité sans pareil depuis la loi sur le renseignement. On pensait que Monsieur et Madame Michu n'en voudraient pas («*J'ai rien à cacher moi, je paye mes impôts et j'ai ma carte à l'UMP*»), mais comme tout le monde, ce charmant couple tient à sa vie privée.

CHIFFREMENT À TOUS LES ÉTAGES !

On voit donc du chiffrement à tous les étages : sur son téléphone, son service de cloud, son PC et maintenant avec les échanges par Internet. On parle de chiffrement de bout en bout au café du coin comme on parle du dernier album de Renaud ou du charme et de la classe de Cyril Hanouna. Et les technologies évoluent vite. Les développeurs savent très bien que les services secrets de tous les pays, NSA en tête, sont à même de déchiffrer des algorithmes considérés comme indéchiffrables il y a encore 5 ans. Ils rivalisent d'ingéniosité pour proposer des systèmes à la fois complexes au niveau technique (chiffrement en plusieurs couches, décentralisation, clés de chiffrement elles-mêmes chiffrées, tunnel Tor, etc.), mais simples à mettre en place pour l'utilisateur. Nous avons donc choisi de vous proposer ce qui se fait de mieux en ce moment sur PC, même si certaines solutions sont aussi disponibles sur d'autres plates-formes. Le but de ce comparatif n'est pas de vous proposer la solution la plus sécurisée, mais que vous puissiez choisir un logiciel proche de vos attentes. Car c'est bien joli d'avoir un logiciel blindé, mais cela ne vous servira à rien si vous ne savez pas l'utiliser...

LEXIQUE

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

CHAT OU TCHAT ?

Le mot chat (prononcez «tchatte») nous vient de l'anglais et signifie «messagerie instantanée». Le terme est aussi utilisé par des francophones même si nos amis québécois préféreront le terme clavardage (clavier + bavardage). Le problème c'est qu'en voyant le mot «chat», nous allons souvent le prononcer comme l'animal, dans nos têtes. À la rédaction nous avons donc décidé d'ajouter un «t» devant pour éviter les confusions.

TCHAT CHIFFRÉ : NOTRE COMPARATIF

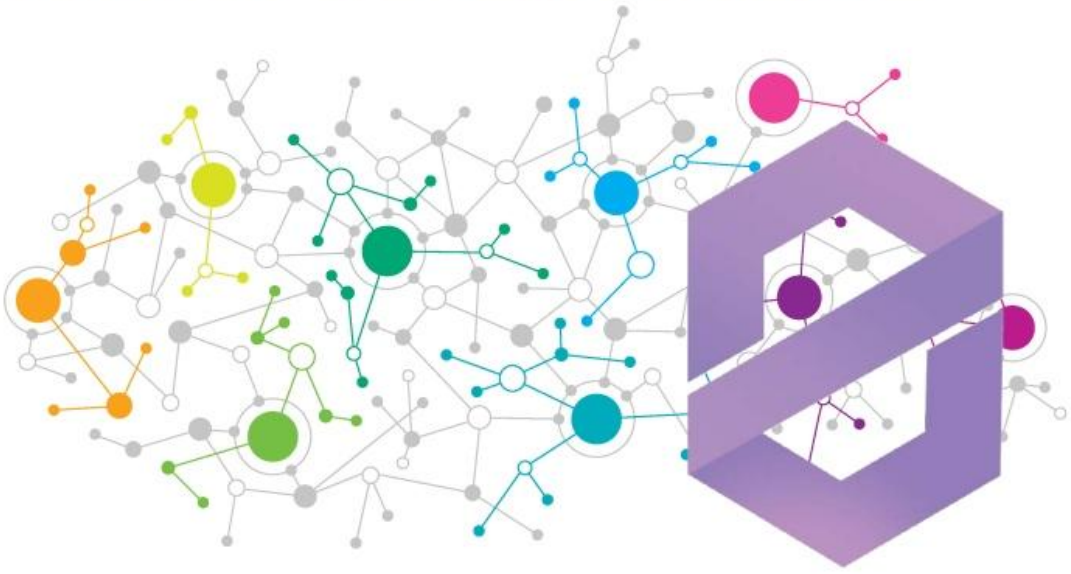
Le point commun entre toutes ces solutions est leur disponibilité sur Windows (même si certaines sont aussi déployées sur d'autres plates-formes). Si vous êtes uniquement intéressé par le chiffrement sur mobile, sachez que WhatsApp propose maintenant un chiffrement de bout à bout (voir nos Hack'tualités) et que Signal est la messagerie préférée de l'ami Snowden...

	Cryptocat	Telegram	CenoCipher	Wickr	Ricochet	TorChat 2	Off-the-record	Bitmessage	Darkwire
Fonctionnalités	Chiffrement bout à bout, partage de fichiers, tchat de groupe (bientôt), message indéchiffrable même en cas de vol de clés	Chiffrement bout à bout, partage de fichiers (jusqu'à 1,5 Go), message indéchiffrable même en cas de vol de clés), message vocal	Chiffrement bout à bout, partage de fichiers, stéganographie, pas d'installation, export des messages chiffrés via un autre mode de communication (e-mail, etc.)	Chiffrement bout à bout, partage de fichiers, tchat de groupe, message vocal	Chiffrement bout à bout, message indéchiffrable même en cas de vol de clés	Chiffrement bout à bout, partage de fichiers, pas d'installation	Chiffrement bout à bout, partage de fichiers (en fonction du client utilisé), message indéchiffrable même en cas de vol de clés	Chiffrement bout à bout, partage de fichiers, pont IMAP/POP/SMTP (pour l'utiliser comme e-mail avec Bitmessage.ch par exemple).	Chiffrement bout à bout, partage de fichiers, tchat-room éphémère, possibilité de le déployer sur son propre serveur
Plates-formes	Windows, Linux & Mac	Windows, Linux, Mac, Web, Android, iOS, Windows Mobile	Windows	Windows, Linux, Mac, Web, Android & iOS	Windows, Linux & Mac	Windows (standalone ou plugin pour Pidgin), Linux (Debian & Ubuntu)	Windows (plugin pour Pidgin, Miranda IM, etc.)	Windows, Linux & Mac	Web
Types de chiffrement	Basé sur TextSecure (AES-256 + Curve25519 + TLS/SSL + SHA256 pour le hashage)	Basé sur MTProto (AES-256 + RSA 2048 + échanges de clés Diffie-Hellman + SHA-1 salé pour le hashage	AES/Rijndael, Twofish, Serpent (256 bits) et SHA256 pour le hashage	AES-256 + ECDH51 pour le chiffrement de la clé + TLS/SLL	Basé sur les hidden services de Tor (RSA 1024 + DHE handshake + hashage SHA-1 80 bits)	Basé sur les hidden services de Tor (RSA 1024 + DHE handshake + hashage SHA-1 80 bits)	AES256, échange de clés Diffie-Hellman et hashage SHA-1 salé	AES256-CBC, échange de clés Diffie-Hellman et hashage SHA-512 avec la possibilité d'utiliser Tor ou I2P	Basé sur l'API Web Cryptography (RSA-AOEP, échange de clés Diffie-Hellman et encore bien des «couches» trop complexes à détailler ici) avec la possibilité d'utiliser Tor.
Licence	Open source Gnu/GPL v3	Partiellement Open source (la partie «serveur» reste propriétaire).	Open source Gnu/GPL v2	Propriétaire	Open source	Open source Gnu/GPL v2	Open source Gnu/GPL v2	Open source MIT	Open source
On en a parlé	Pirate Informatique n°21 (ancienne version «Web»)	Non	Non	Non	Non	Pirate Informatique n°18	Pirate Informatique n°25	Pirate Informatique n°26	Non
Difficulté	2/5	2/5	2/5	2/5	2/5	3/5	4/5	3/5	1/5
Lien	https://crypto.cat/index.html	https://telegram.org	https://gitlab.com/cenocipher/cenocipher	www.wickr.com	https://ricochet.im	https://github.com/prof7bit/TorChat/downloads	https://otr.cypherpunks.ca/index.php#downloads	https://bitmessage.org	https://darkwire.io

NOTRE VERDICT :

Bien sûr les solutions que nous vous avons proposées sont toutes sécurisées. Darkwire satisfera ceux qui n'ont pas besoin d'une solution de chiffrement tous les jours tandis que Wickr, très prometteur, est malheureusement fermé : pas moyen de vérifier la présence de backdoors. Pour une utilisation «tout terrain», Telegram semble être le grand gagnant, mais là encore, la partie «serveur» est propriétaire. Cenocipher n'est disponible que sur Windows, mais a l'avantage de ne pas nécessiter d'installation. Tout semble OK dans Ricochet puisqu'en plus de chiffrer les messages il passe par les «tuyaux» de Tor par défaut. Par contre il n'existe pas de version mobile et il n'est pas encore possible d'envoyer de pièce jointe. Off-the-record dispose de la sécurité la plus élevée, mais il est un peu plus difficile à mettre en place (il faut l'ajouter à un logiciel comme Pidgin). Bitmessage et Cryptocat ne semblent pas souffrir de défaut particulier, reste à développer des solutions mobiles...

ZERONET:
UNE EXPÉRIENCE DANS LE NET DÉCENTRALISÉ



Imaginez un réseau impossible à mettre à terre ou à censurer. Vous connaissiez déjà Freenet, I2P ou les Hidden Service de Tor (*Pirate Informatique* n°24 & 25), mais ZeroNet se veut plus convivial, plus rapide et plus simple à prendre en main. Bien sûr, les contenus sont encore peu nombreux, mais ce modèle a de l'avenir...

Dans notre numéro 27, nous vous avions présenté Maelstrom, un navigateur expérimental de la société BitTorrent permettant de développer des sites complètement décentralisés et hébergés mutuellement par tous les intervenants. N'étant pas open source et proposant peu de contenu, Maelstrom a bien du mal à décoller, mais l'idée, basée sur le principe des darknets a fait des émules.

COMPLET ET ACCESSIBLE

ZeroNet propose tous ses services depuis votre navigateur : vous n'aurez pas à installer de plugin, gérer des certificats ou des paires de clés. Tout se fait automatiquement que vous vouliez envoyer un e-mail, participer à un forum, chercher du contenu ou créer votre blog. Car à la différence avec ses petits camarades, ZeroNet supporte le contenu dynamique.

Tous les sites sous ZeroNet contiennent une liste «hashée» (SHA512) de tous les fichiers utilisés et une signature générée avec la clé privée du webmaster. Si le site est modifié, le webmaster signe une nouvelle liste et la publie pour les potentiels intéressés. Techniquement, ZeroNet utilise le réseau P2P BitTorrent pour le partage des listes et les échanges, BitCoin pour le chiffrement et Tor pour ajouter une couche d'anonymat. Bien sûr, rien n'est stocké sur un serveur. Chaque participant possède une partie des sites qu'il consulte et «seed» pour les autres. C'est grâce ce mode de fonctionnement qu'il devient impossible pour un gouvernement, un FAI ou un groupe de pirate de prendre la main ou d'en interdire l'accès. Outre les services énoncés plus haut, certains on déjà commencé à proposer des trackers (voir notre article page 46). Mais pour vos premiers pas sur ZeroNet, suivez le guide...

LEXIQUE

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

*** SEED :** «Graine» dans la langue d'Axl Rose. Dans un réseau BitTorrent, un seed est un intervenant qui dispose de l'intégralité d'un fichier et qui le partage. On dit qu'il «seede». Dans Zeronet, on seede les sites, les forums, etc.

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

*** BITCOIN :** Bitcoin est une monnaie virtuelle ne dépendant d'aucune banque centrale et qui permet anonymement de régler des achats en ligne sans taxe et sans intermédiaire. Le système pour chiffrer les transactions est utilisé dans Zeronet pour la mise en relation avec les sites.

PAS À PAS

Utilisation de ZeroNet

CE QU'IL VOUS FAUT

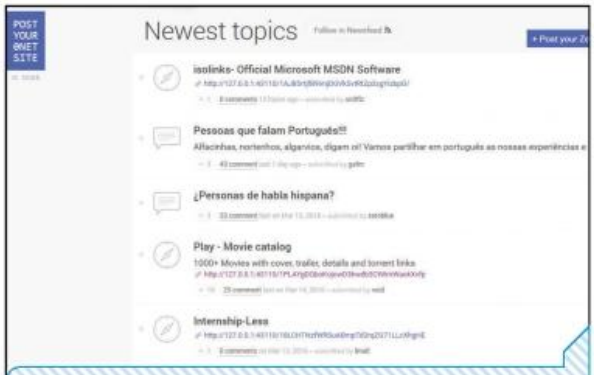
ZERONET

OÙ LE TROUVER ? :
https://zeronet.io

DIFFICULTÉ :

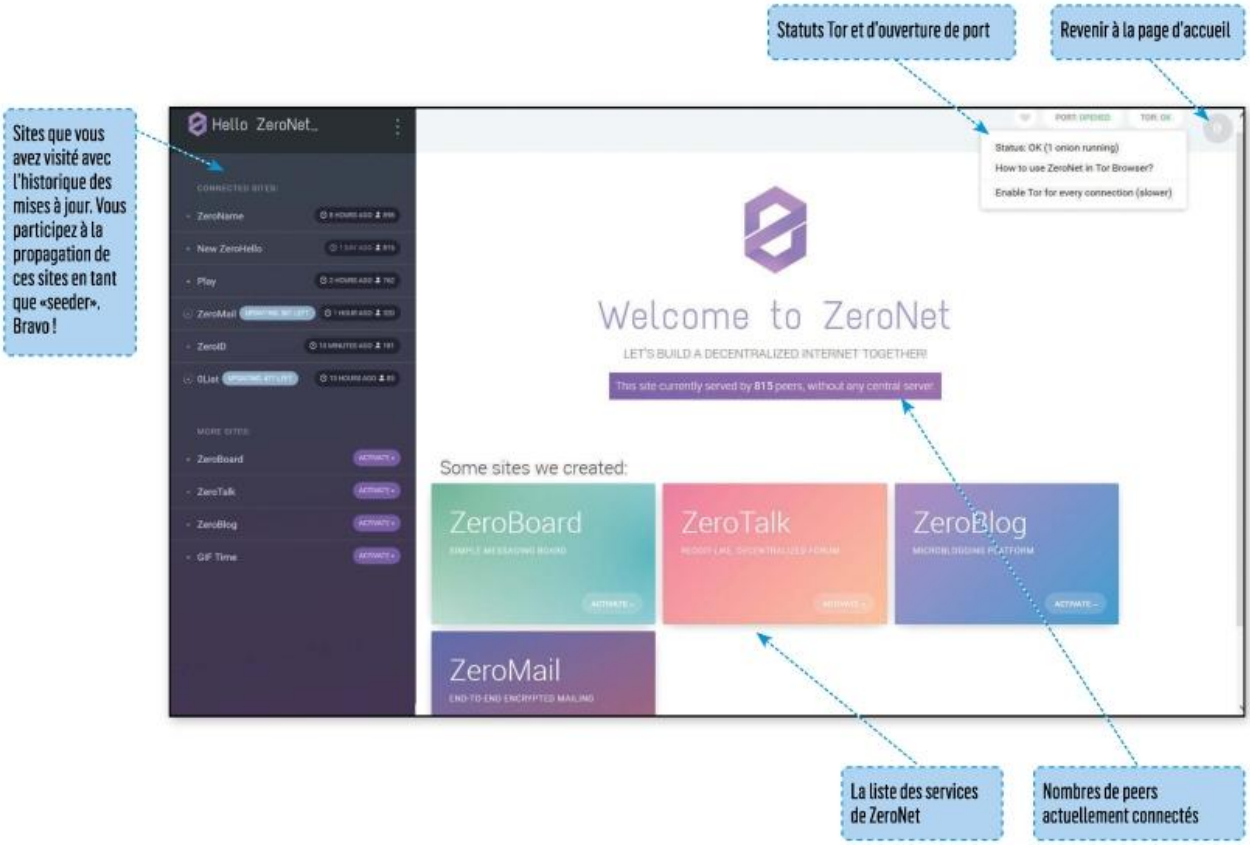
01 MISE EN PLACE

Commencez par télécharger l'archive (**Download for Windows**), dézippez-la et lancez le fichier **zeronet.cmd**. Une petite icône apparaîtra dans la zone de notification en bas à droite. Aucune installation n'est requise, vous pouvez donc emporter le dossier ZeroNet sur une clé USB. Si cela n'a pas été fait automatiquement, vous pouvez faire **Open ZeroNet** avec un clic droit dans cette icône. Vous êtes connecté !



Décentralisé et anonyme, ZeroNet est aussi dynamique ! Le contenu est facilement modifiable et permet des mises à jour. Rien à voir avec Maelstrom et ses sites statiques.

02 L'INTERFACE



03 VOTRE IDENTITÉ

Poursuivons en créant une identité certifiée **Zeroid.bit**. Cela vous permettra d'accéder à tous les services (mail, forums, etc.) sans avoir besoin de mot de passe et de communiquer avec les autres intervenants sans même connaître leur identité. Sur la page principale, cliquer sur **ZeroMail** puis **Select username**, **Get auth cert**. Tapez l'identifiant de votre choix et si ce dernier est libre, faites **Send request**. De retour dans ZeroMail, sélectionnez votre identifiant en haut depuis le **?** et faites **Create my mailbox**.

04 LE PREMIER E-MAIL

Faites un essai en envoyant un e-mail au robot echobot. En parcourant la zone de votre correspondant, vous verrez des noms au fur et à mesure que vous tapez. Il s'agit d'autres participants. C'est le point fort de ZeroNet! Rien qu'en ayant l'identifiant d'une personne, vous pouvez la joindre: pas d'échange de mots de passe ou de clé... Par contre, impossible de joindre les gens qui sont à l'extérieur du réseau. Cet e-mail ne s'utilise qu'en «interne» pour les participants. Maintenant que votre identité et votre e-mail sont configurés, explorons un peu le reste.

05 LES AUTRES SERVICES

ZeroBoard ne sert à rien (il s'agit d'un shoutbox) à part pour montrer les capacités dynamiques du système tandis que ZeroTalk est une sorte de forum style Reddit où chacun place ses posts avec la possibilité de voter pour tel ou tel sujet. ZeroBlog est le projet le plus intéressant avec la possibilité pour un citoyen lambda de créer un site complètement décentralisé interdisant la censure. Chaque site possède un identifiant sous la forme d'un hash (exemple **1HeLLo4uzjaLetFx6NH3PMwFP3qbRbTf3D**) et ne sera accessible dans votre navigateur que lorsque vous aurez démarré ZeroNet.

06 DÉCENTRALISÉ ET ANONYME

Décentralisé c'est bien, mais anonyme c'est encore mieux. Pour cela, ZeroNet intègre le protocole Tor sans qu'il soit nécessaire de l'installer. Il est néanmoins conseillé de choisir un navigateur «à part» pour le couple ZeroNet+Tor puisque certaines extensions peuvent laisser passer des informations vous concernant. Regardez en haut à droite de la page principale pour voir le statut de Tor et vérifier que le port 15441 est bien ouvert. Dans le cas contraire, il faudra ouvrir ce port manuellement dans les réglages de votre box. Pour Tor, attendez un peu ou allez ici : **http://goo.gl/lvep80**.

CRÉEZ UN SITE SUR ZERONET ET GAGNEZ UNE CLÉ USB *PIRATE INFORMATIQUE*

ZeroNet vous intéresse? Tentez de faire un site en suivant les instructions de notre lien. Envoyez-le nous et gagnez une clé USB Pirate Informatique si votre création attire notre attention (8Go avec tous les numéros du magazine inclus)...

Lien : **http://tinyurl.com/hjlqx9h** (ZeroNet requis)

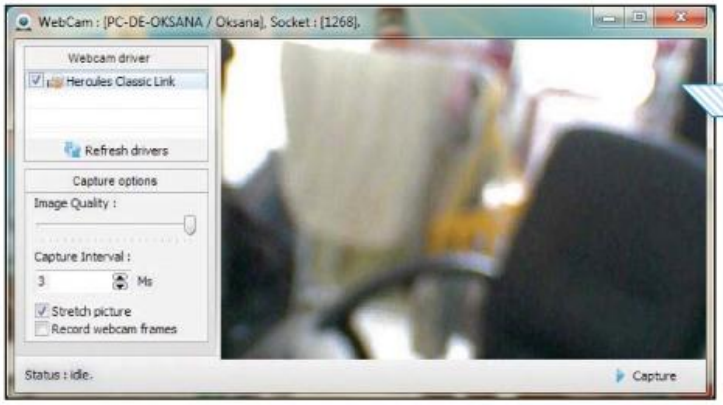
VOTRE WEBCAM VOUS ESPIONNE-T-ELLE?

Et si votre webcam servait à vous espionner à votre insu ? Ce n'est malheureusement pas de la sciencefiction puisque de nombreux spywares permettent ce tour de force. Vous pouvez bien sûr mettre un morceau de carton devant l'objectif, mais que faire lorsque vous conversez par Skype ou autre ? Pour mettre une barrière entre votre vie privée et Internet, voici Who Stalks My Cam...

Dans notre précédent numéro, nous avons vu les problèmes d'«étanchéité» des caméras IP qui fleurissent dans les commerces et chez les particuliers. Or, ce problème se rencontre aussi avec les webcams. Nous avons déjà vu dans notre numéro 25 que des RAT comme DarkComet et ses variantes permettent d'accéder au flux vidéo d'une webcam sur un PC infecté. Et tout cela sans allumer la fameuse lumière qui indique que vous êtes filmé bien sûr ! Pour se prémunir de ce genre de surprise quoi de mieux qu'un logiciel créé par le créateur de DarkComet lui-même (voir notre interview) ?

«L'ŒIL ÉTAIT DANS LA TOMBE...»

Who Stalk My Cam (WSMC) va analyser en temps réel les processus qui ont accès à votre webcam. Vous serez immédiatement notifié en cas d'accès frauduleux. À vous de choisir la marche à suivre : couper l'accès au spyware ou couper tout simplement le flux audio/vidéo. WSMC ne désinfectera pas votre ordinateur, mais vous saurez où se situe le problème quel type de malware est impliqué. Il est aussi possible de dresser une liste blanche d'applications autorisées à utiliser la webcam et de programmer le logiciel à agir suivant telle ou telle situation.



Un exemple de RAT qui va accéder à la webcam d'un utilisateur infecté. Ce type d'attaque ne relève pas de la sciencefiction ! Il est possible d'enregistrer les personnes à leur insu et imaginer qu'un maître chanteur ou qu'un cambrioleur soit de l'autre côté des tuyaux. Protégez-vous !

LEXIQUE

***DARKCOMET :**
DarkComet est un RAT qui fonctionne selon le modèle client/serveur. Le client est installé sur votre machine et le serveur (ou stub) est créé sur mesure par l'utilisateur. Il prendra la forme d'un fichier EXE (même s'il est possible de contourner cette restriction) que la cible lancera par inadvertance sur son PC. Même si les intentions du développeur n'ont jamais été de faire un logiciel pour pirater des tiers, les options pour camoufler ce fichier EXE et le rendre persistant sur la machine d'une éventuelle victime sont assez puissantes. Suite à des utilisations frauduleuses de son logiciel, son créateur a arrêté le développement en 2012.

***RAT :**
Abréviation de Remote Administration Tool ou Outil d'administration à distance en français. Il ne s'agit pas d'un malware, mais d'un programme permettant d'avoir accès au contenu d'un PC sans être physiquement présent. Ce type de logiciel peut bien sûr être utilisé à des fins malhonnêtes.

PAS À PAS

Paramétrage de Who Stalks My Cam

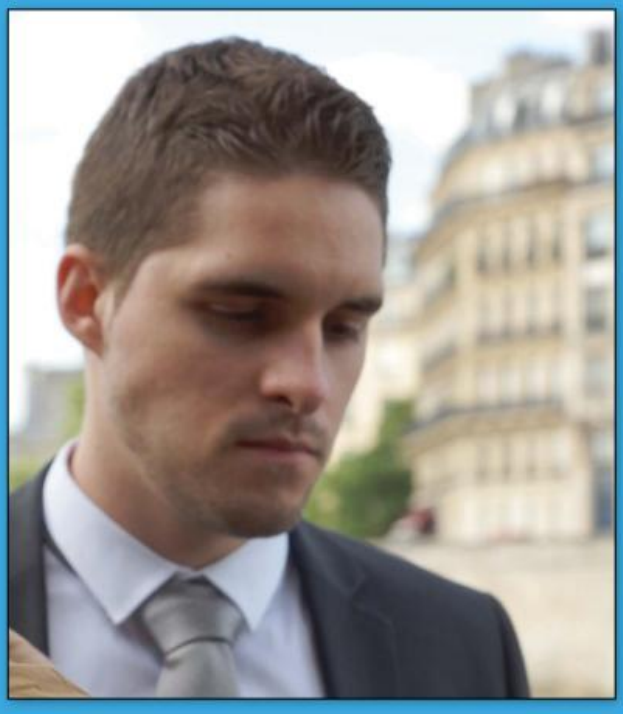
CE QU'IL VOUS FAUT
WHO STALKS MY CAM
OÙ LE TROUVER ? : **www.phrozensoft.com/freeware**
DIFFICULTÉ :

01 MISE EN PLACE

Dans le fichier Zip, vous trouverez une version portable du logiciel. Idéal pour lancer le programme sur un PC qui n'est pas le vôtre (emportez-le sur votre clé USB !), mais nous vous conseillons la version installable. Dès le lancement, allez dans l'onglet **Options** et cochez **Active Webcam Usage Detection** et **Start program with Microsoft Windows** pour activer le logiciel et le lancer à l'ouverture du système. Dans **Notifications,** ne touchez à rien pour être prévenu en temps réel.

02 RÉGLAGES

Dans **Security Policies**, nous vous invitons à cocher la première case pour intervenir lorsqu'un processus en arrière-plan tente de s'accaparer la webcam car la plupart du temps ce sont uniquement les programmes « actifs » qui utiliseront la webcam de manière légitime. La deuxième case concerne l'inactivité du PC : elle coupe la webcam lorsque l'ordinateur n'est plus utilisé depuis X secondes, minutes ou heures. La troisième case concerne la liste blanche. Pour l'instant, elle est vide bien sûr.



Interview de Jean-Pierre Lesueur,

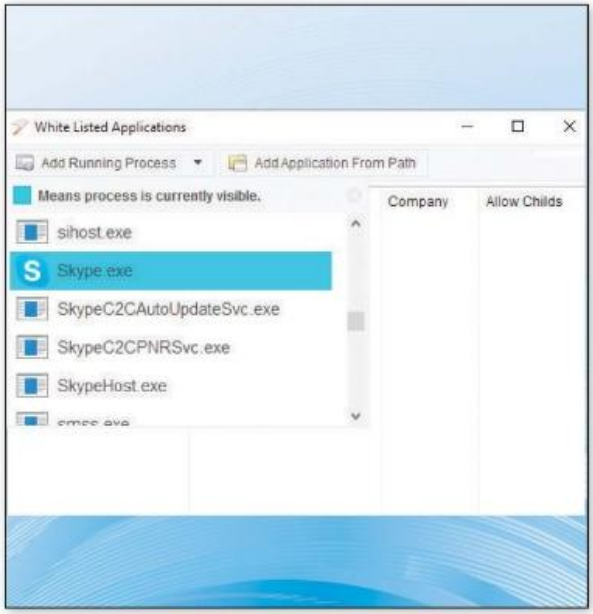
créateur de DarkComet RAT, et fondateur de la société Phrozen SASU éditrice de Who Stalks My Cam.

COMMENT AVEZ-VOUS EU L'IDÉE DE FAIRE CE LOGICIEL ? FATIGUÉ DE RETIRER LE SCOTCH DEVANT VOTRE WEBCAM AVANT DE L'UTILISER ?

Tout comme pour le programme RunPE Detector (voir *Pirate Informatique* n°26), Who Stalks My Cam est avant tout un logiciel «proof of concept» qui démontre la possibilité de détecter l'usage de la webcam par n'importe quel processus, et ce, de façon générique et en restant au sein du «user land» (ring 3*). J'en ai ensuite fait un programme complexe pour détecter la présence de potentiels malwares qui pourraient utiliser à notre insu la webcam et ainsi économiser du scotch !

03 LA LISTE BLANCHE

Cliquez sur **Configure White List** et ajoutez les programmes que vous voulez autoriser. Dans **Add Running Process**, vous trouverez les processus qui sont actuellement en train de fonctionner, mais vous pouvez trouver les autres dans **Add Application From Path**. Si vous êtes perdu, il y a plus simple. Dans le menu Phrozen en haut à gauche, faites **Webcam Testing** puis **Start**.



04 LES ÉVÉNEMENTS ENREGISTRÉS

Si vous n'avez pas touché à la liste blanche, une notification apparaîtra et la webcam sera coupée. En effet, le processus de WSMC n'est pas par défaut dans la liste blanche : l'appli elle-même se considère comme suspecte pour que le teste se déroule normalement. Pour y remédier, allez dans l'onglet **Webcam Events** pour voir les rejets. Faites un clic droit et choisissez **Add process to White List**. Faites de même pour chaque programme légitime que WSMC détectera...

Prévoyez-vous une version française du logiciel ?

Très bientôt. Tous nos derniers logiciels sortent désormais en français et anglais. Cette fonctionnalité sortira en même temps que sa nouvelle interface.

Plusieurs années après sa conception, DarkComet est toujours un des RAT les plus puissants. Comment expliquez-vous cette longévité ?

DarkComet RAT est en effet toujours un des RAT les plus utilisés dans le monde. Il est toujours très diffusé et reste le programme de référence pour les scripts kiddies. Même s'il est très détecté par les antivirus, les scripts kiddies achètent des «crypters» pour le rendre indétectable ce qui explique qu'il fonctionne toujours aujourd'hui.

Des nouvelles de DarkComet Remover? D'autres projets en cours?

DarkComet Remover n'est toujours pas disponible sur le site principal. Je n'ai toujours pas eu le temps d'adapter le programme à notre nouvelle charte graphique. L'ancien est toujours aussi efficace et se trouve facilement sur des sites de distributions de logiciels. Sinon, je travaille en ce moment sur la nouvelle version de Phrozen VirusTotal Uploader qui ne se nommera plus ainsi. C'est l'équipe de VirusTotal (Google) qui m'a encouragé à le mettre à jour. En effet, l'ancienne version a permis de scanner plusieurs millions de fichiers en seulement 1 an, ce qui aide les sociétés éditrices d'antivirus à recevoir de nouveaux échantillons et par conséquent sécuriser nos systèmes. Il devrait être disponible dans le mois et promet d'être un logiciel incontournable en complément de votre antivirus favori.

**https://fr.wikipedia.org/wiki/Anneau_de_protection*

FAILLE WPS : VOUS ÊTES CONCERNÉ !

Dans notre dernier numéro, nous vous avions parlé du logiciel WiFite intégré à la distribution Kali Linux. Ce dernier permet de faire du pentest dans votre box ou routeur, mais il faut reconnaître que tout le monde n'a pas de «Linuxette» sous la main pour faire ce genre de test à la maison... Dans les microfiches précédentes, nous avions aussi parlé de WPS Protect, mais certains lecteurs nous ont demandés de revenir dessus. Donc acte !

Commençons par rappeler que le système WPS équipé par certains routeurs ou box permet de facilement se connecter à un réseau sans fil sans avoir à taper une longue clé d'authentification. En fonction des réglages par défaut (que vous pouvez bien entendu changer), le propriétaire du matériel doit parfois appuyer sur un bouton pour autoriser un invité à se connecter (limité dans le temps) et parfois il s'agit d'un code PIN. Même s'il existe des moyens pour court-circuiter la protection du bouton (nous y reviendrons dans un prochain numéro), la vulnérabilité la plus répandue concerne ce code PIN. En effet, certains constructeurs utilisent le même PIN pour tous leurs produits et il est même parfois impossible de le changer sans modifier le firmware.

TESTEZ VOTRE MATÉRIEL !

WPS Connect est une application pour appareil Android rooté qui va tenter de se connecter sur les routeurs alentours pour voir s'ils sont vulnérables. Attention, il s'agit bien sûr de vérifier votre matériel et pas de se connecter chez le voisin ! Pour voir si vous n'avez pas un intrus sur votre réseau, allez à la page XX de ce magazine pour découvrir Wireless Network Watcher et Fing. N'oubliez pas non plus de changer régulièrement votre clé WiFi et d'éviter les sésames trop convenus.

WPS Connect a détecté une vulnérabilité sur votre réseau ? Connectez-vous aux réglages de votre routeur ou box depuis votre navigateur (avec 192.168.0.1 le plus souvent) et supprimez cette fonctionnalité !

LEXIQUE

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

PAS À PAS

Pentest de votre réseau avec WPS Connect

CE QU'IL VOUS FAUT

WPS CONNECT

OÙ LE TROUVER ? : **https://goo.gl/NZOAJ8**

DIFFICULTÉ :

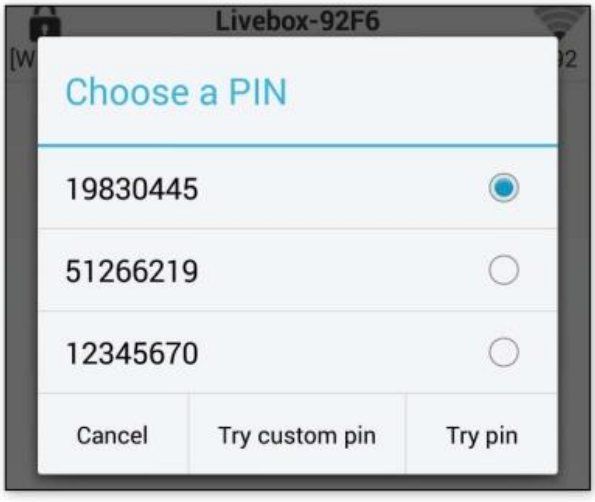
01 PREMIÈRE PRÉCAUTION

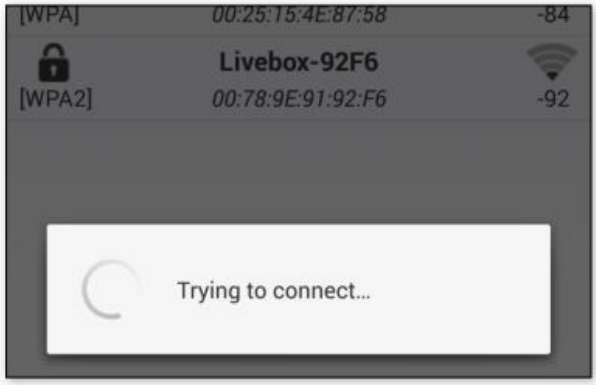
Premièrement, il ne faut pas que votre réseau WiFi soit enregistré sur votre smartphone/tablette pour le test. Allez

dans **Paramètres**>**Sans fil et réseau** ou directement depuis la zone de notification et faites **Retirer**. Vous remettrez le WiFi après. Cliquez sur les flèches en haut à droite pour afficher la liste des SSID et sélectionnez le vôtre. L'appli vous demandera alors de lui octroyer les droits superutilisateur. Votre téléphone n'est pas rooté? Retrouvez dans notre CD différents articles de notre cru pour vous aider...

02 L'ATTAQUE !

WPS Connect vous demandera ensuite de rentrer un code PIN basé sur ce qu'elle connaît de votre routeur. En faisant





Custom PIN, vous pouvez en saisir un vous-même (si vous avez des nouvelles fraîches sur une vulnérabilité), mais tentez simplement les entrées qu'on vous propose pour commencer. L'appli commencera alors à converser avec le routeur/box.

02 ÉCHEC OU SUCCÈS ?

Vous aurez ensuite deux fenêtres différentes selon la réussite ou non de la manipulation. Soit l'attaque a réussi et vous aurez le mot de passe en clair. Soit votre matériel est vulnérable:

faites toutes les mises à jour de firmware que vous pouvez et désactivez le WPS! Dans le cas contraire, l'appli vous invitera à changer de PIN ou vous rapprocher du point d'accès WiFi cible.

SURVEILLEZ VOTRE RÉSEAU WIFI

Dans notre numéro 22, nous vous avions parlé de WiFi Guard, un logiciel permettant de contrôler les périphériques présents sur votre réseau sans fil. Pratique pour déceler les intrus ! Certains lecteurs ayant eu des difficultés avec ce programme, nous avons décidé de proposer deux alternatives : Wireless Network Watcher sous Windows et Fing sur Android...

LEXIQUE

*** ADRESSE MAC :** Une adresse MAC (pour Media Access Control) est une suite de nombres (par exemple 4A:EF:23:A5:ED:14) qui identifie un périphérique sur un réseau. Il ne s'agit pas d'une identification sûre, car elle peut être changée et usurpée très facilement.

Votre réseau WiFi connaît des hauts et des bas ? Vous pensez avoir un intrus qui profite de votre forfait Internet ? Pour en avoir le cœur net, nous vous conseillons Wireless Network Watcher de Nirsoft (voir *Pirate Informatique n°27*). Ce logiciel va scanner votre routeur/box pour voir qui s'y connecte. Vous pourrez enregistrer la liste des appareils autorisés, voir les adresses MAC, les dates d'activité et le fabricant. L'interface est austère, mais l'installeur ne comporte ni toolbars, adwares ou autres mauvaises surprises.

UNE ALTERNATIVE SUR MOBILE...

Pour ceux qui souhaiteraient avoir une solution plus complète et mobile, le logiciel Fing fait exactement la même chose sur smartphone Android avec un peu plus d'options disponibles : scan de services, ping, traceroute, etc. Pratique pour auditer un réseau sans fil lorsque l'on a pas son matériel sous la main. Attention, qu'il s'agisse de WiFi Guard, Wireless Network Watcher ou Fing, il faudra faire le ménage «à la main» si vous détectez un importun...

PAS À PAS

Scan de réseau avec Wireless Network Watcher

CE QU'IL VOUS FAUT

WIRELESS NETWORK WATCHER

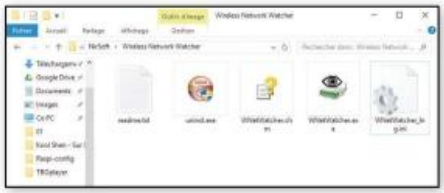
OÙ LE TROUVER ? :
http://goo.gl/uPP19S

DIFFICULTÉ :

01 INSTALLATION

Attention, comme la plupart des logiciels qui se trouvent sur notre CD, les programmes NirSoft auront tendance à faire paniquer votre antivirus. Si vous utilisez Windows 10, ce dernier va aussi vous inviter à la prudence. Cliquez sur **Informations complémentaires** puis sur **Exécuter quand même**. Pour avoir l'interface en français, téléchargez l'archive sur le site et placer le fichier **.ini** dans le dossier d'installation.

02 LES OPTIONS AVANCÉES



Dès le premier lancement, la fenêtre des options avancées va s'afficher. Notez que vous pourrez y revenir plus tard avec la touche **F9**. Normalement, la carte réseau devrait être détectée automatiquement. La plage des adresses IP est importante. Avec notre box SFR, nous avons choisi de **192.168.1.1** à **192.168.1.255**, mais il arrive que les adresses attribuées aillent de **192.168.1.1** à **192.168.1.80** par exemple. De même, on trouve des plages qui commencent à **192.168.0.1**. Dans le doute, choisissez de **192.168.0.1** à **192.168.1.255**, mais les scans seront plus longs.

03 LE SCAN DE VOTRE RÉSEAU

Au niveau de «intervalle de recherche», vous pouvez mettre **30** ou **60** secondes. Le reste des options permet de programmer des réactions en fonction de l'activité. Allez ensuite dans **Options** et cochez **Émettre un bip à la détection de nouveau périphérique**. Dans un premier temps, cliquez sur la flèche verte pour afficher tous les périphériques. Vous ne connaissez pas cet appareil? Faites bien attention à ne pas paniquer pour rien. Avec le nombre de matériels connectés dans une maison, vous pourriez déclarer la guerre à un pèse-personne !

04 L'ENREGISTREMENT DE VOTRE LISTE

Pour regarder de plus près, faites un clic droit puis **Propriétés** dans le périphérique pour avoir tous les détails. Pour garder une trace des périphériques connectés et plus facilement détecter les intrus à venir, sélectionnez tous les appareils et faites **Fichier>Enregistrer les fichiers sélectionnés** pour garder une liste au format **.txt**. En cas d'intrusion, vous pouvez relever l'adresse MAC et la bannir dans les paramètres de votre box, mais vous devez aussi changer votre clé WiFi !

05 KICKEZ LES INTRUS !

Optez pour du WPA2+AES (tout sauf du WEP dans tous les cas !) et trouvez une clé suffisamment solide: majuscules, minuscules, chiffres et caractères spéciaux. Le seul problème, c'est qu'il faudra entrer cette nouvelle clé dans tous les appareils de votre réseau domestique... Vous pouvez aussi vous renseigner des failles potentielles de votre routeur sur **http://routerpwn.com**.

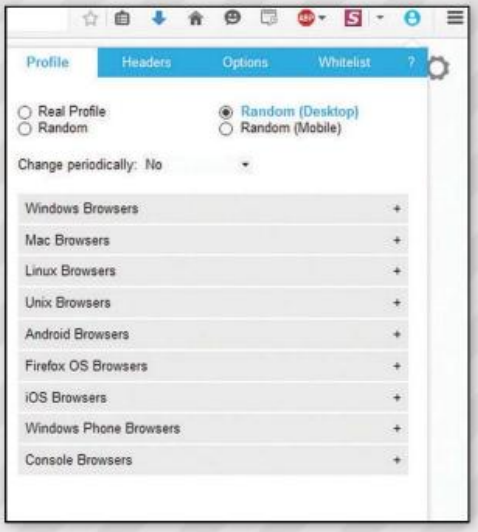
FING SOUS ANDROID

Moins puissant que cSploit, Fing a l'avantage de ne pas nécessiter un smartphone rooté. Dès l'allumage, l'appli va scanner votre point d'accès et dresser la liste de tous les périphériques connectés. Choisissez-en un pour afficher les détails: adresse MAC, IP, date de connexion, etc. En fonction du type d'appareils, vous pourrez faire appel à certaines options: scan de ports, traceroute, bidouillage DNS, etc. Dans les Tools (l'engrenage), vous aurez accès à d'autres options.

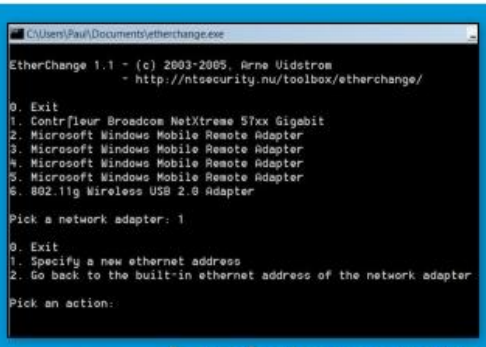
#1 Brouiller votre «empreinte» Internet

AVEC RANDOM AGENT SPOOFER

Entre les proxies, les VPN, les clients mail et les espaces de stockage chiffrés, vous êtes paré à toutes les éventualités sauf une : l'empreinte unique de votre navigateur. Même si les millions d'internautes qui se connectent chaque jour pensent se fondre dans la masse, votre navigateur «parle». Avec une simple requête, il est possible de connaître le nom de votre navigateur, sa version, le nombre et les noms des extensions, les polices installées, votre fuseau horaire, votre version de Windows, la résolution de votre écran, etc. En combinant ces différents éléments, les hackers peuvent dresser une empreinte unique : la vôtre. Random Agent Spoofer propose de brouiller encore plus les pistes sur Internet en générant de manière aléatoire des informations bidons. Vérifiez vos données sur https://panopticlick.eff.org ! Pour Chrome, essayez User-Agent Switcher.



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



#2 Jongler avec votre adresse MAC

AVEC ETHERCHANGE

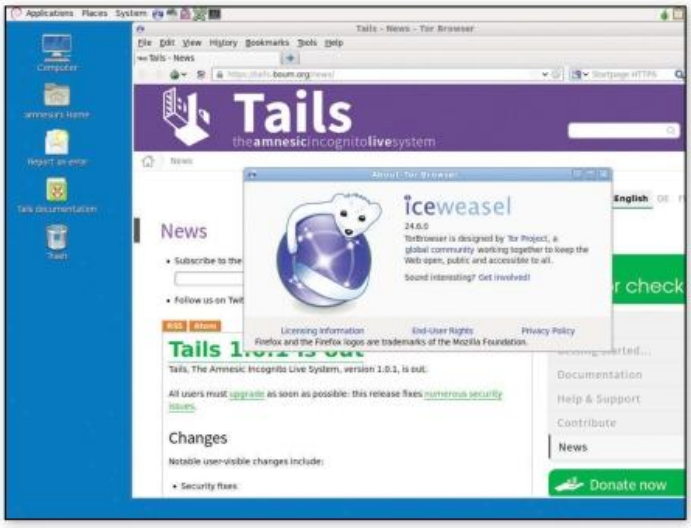
EtherChange est un programme qui vous permettra de modifier l'adresse MAC d'une carte réseau. Cela peut s'avérer utile si vous vous connectez à un réseau qui limite la connexion aux utilisateurs (aéroport, hôtel, etc.) Il fonctionne en ligne de commande, mais reste très accessible. Attention, il faudra cependant être administrateur de votre système. Maintenez la pression sur la touche **Maj** du clavier et faites un clic droit dans le dossier contenant vos fichiers et sélectionnez **Ouvrir une fenêtre de commandes ici**. Tapez ensuite **etherchange.exe** et validez. Ce logiciel ne fonctionne pas avec les versions récentes de Windows. Attention, votre navigateur peut vous mettre en garde contre le site de téléchargement. Vous pouvez y aller, il n'y a rien de dangereux. Sous Chrome, faites **Détails> Consulter ce site** ou **Ignorer cet avertissement** sous Firefox.

Lien : **http://ntsecurity.nu/toolbox/etherchange**

#3 Un OS complètement anonyme

AVEC TAILS

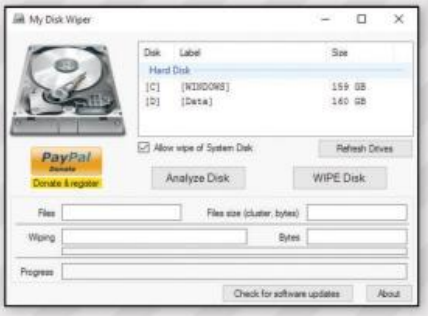
Tails, que vous avez pu voir rapidement dans la dernière saison de Homeland, est la réponse ultime aux Internautes exigeant un anonymat sans faille. Car, si vous avez déjà essayé d'utiliser Tor, vous savez qu'il est facile à installer, mais que le maintien de l'anonymat est compliqué, surtout pour les débutants qui pensent à tort être protégés quoiqu'il arrive. Ce n'est évidemment pas le cas. Il suffit d'un programme lancé malencontreusement ou d'une extension un peu trop bavarde pour mettre à mal votre identité, votre position géographique, etc. La solution réside dans un système autonome où toutes les connexions passeraient par Tor : Tails (The Amnesic Incognito Live System). Il s'agit d'une distribution GNU/Linux basée sur Debian qu'il est possible de lancer en mode Live CD. En plus d'une connexion obligatoire par Tor, Tails contient tout ce qu'il faut pour chiffrer vos e-mails, effacer vos traces, etc. La mise en place est un peu plus compliquée que pour les autres Live CD (il vous faudra posséder deux clés USB de 4 Go, créer un espace de stockage chiffré, etc.), mais tout est très bien documenté et vous pouvez le faire depuis votre PC sous Windows. Sachez enfin que la NSA considère Tails comme la pire menace contre la collecte d'information. Si vous souhaitez que nous y revenions dans le prochain numéro, envoyez un petit mail ici : benbailleul@idpresse.com



Lien : **https://tails.boum.org**

#4 Effacer les données confidentielles ou compromettantes

AVEC MY DISK WIPER



Envie de faire le grand ménage dans votre PC sans pour autant formater et tout réinstaller? My Disk Wiper va effacer toute trace de donnée sur un disque dur ou une clé USB sans espoir de récupérer quoi que ce soit. Que vous vouliez vendre ou acheter un ordinateur d'occasion, vous éviterez de voir vos données personnelles dans la nature ou au contraire, vous effacerez les informations compromettantes de votre nouvelle acquisition. Il propose moins d'options que R-Wipe&Clean (*Pirate Informatique* n°19), mais ne nécessite pas d'installation.

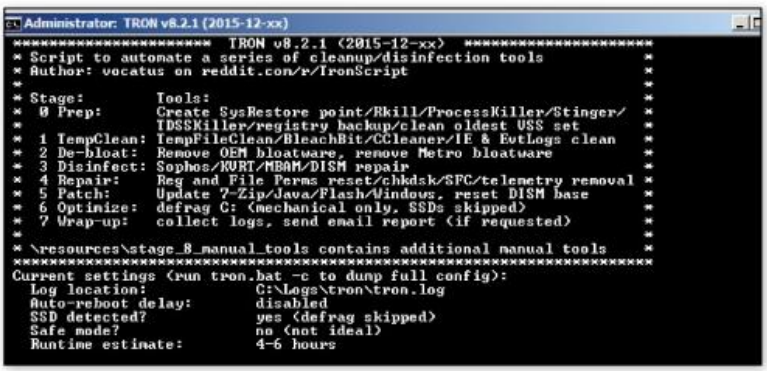
Lien : **http://goo.gl/cHMjjm**

#5 Désinfecter et réparer

AVEC TRON

Tron n'a rien à voir avec le Maître Control Principal, des motos futuristes ou Jeff Bridges. Il s'agit d'un script qui va vous permettre de récupérer un PC (de XP à Windows 10) en pleine santé. Il automatise des tâches bien connues des réparateurs de PC en herbe tout en proposant des outils bien utiles. C'est donc un total de 545 Mo de solutions de réparation/désinfection/optimisation/nettoyage qui vous sont proposés : antivirus, patch, anti-bloatware, tueur de processus, récupération d'un registre sain, etc. Vous devrez lancer l'EXE en mode sans échec à condition d'être en mode administrateur. Attention, comme la plupart des actions sont automatiques, veillez à bien sauvegarder vos documents. Si ce n'est pas possible, Tron créera un point de restauration pour ne pas partir de plus bas que vous ne l'étiez...

Lien : **www.bmrf.org/repos/tron**



#7 Récupérer vos fichiers perdus

AVEC MINITOOL POWER DATA RECOVERY

Erreur de manipulation, copier-coller malheureux ou bêtise de votre cousin/petit frère/ex-concubine: vous avez malencontreusement effacé des fichiers de votre disque dur. À moins que vous ne soyez victime d'un ransomware (puisque ces derniers chiffrent vos documents, mais effacent les originaux)? Power Data Recovery (PDR) pourrait bien vous sauver la vie. Nous ne parlons généralement pas de logiciels payants, mais ce PDR propose une version gratuite permettant de récupérer 1Go de données. Si cela ne suffit pas, la version «bootable» est disponible en démo avec la possibilité de scanner les fichiers à récupérer. Si le logiciel les voit, c'est qu'ils sont récupérables et vous pourrez alors payer les 60€ sans risque. Attention, ne téléchargez pas le logiciel sur la partition où vous voulez récupérer des données, cela pourrait les effacer à jamais. Idem pour l'installation. Notez enfin qu'il est possible de booter sur un BIOS UEFI uniquement avec les systèmes 64 bits. Bien joué, maudit UEFI !

Lien : **www.powerdatarecovery.com**

Retrouvez la première partie

Si vous avez raté nos deux derniers numéros et que vous voulez lire les premières parties de ce dossier, sachez que les PDF se trouvent dans la partie «bonus» de notre CD ! Vous y trouverez la présentation et les méthodes d'installation de Kali Linux 2 ainsi que notre tuto sur WiFite.

ARMITAGE : TESTEZ TOUS LES ORDINATEURS DE VOTRE RÉSEAU

Si vous êtes du genre à pester contre les mises à jour de sécurité, vous ne les verrez plus jamais comme avant après avoir testé Armitage. Cette interface graphique pour Metasploit permet de scanner un réseau complet et de rechercher diverses failles connues, mais pas forcément «patchées» sur tous les ordinateurs de votre environnement...

LEXIQUE

***KALI LINUX :**
Anciennement BackTrack, Kali Linux est une distribution spécialisée dans l'audit réseau, le pentesting et plus généralement le hacking. Parmi les outils inclus, vous trouverez des logiciels pour cracker des mots de passe, des logiciels de rétro-engineering, des modules pour pénétrer des réseaux sans fil, etc.

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

***SCRIPT KIDDIES :**
C'est un «pirate» qui utilise des logiciels «clé en main» sans vraiment en connaître le fonctionnement pour se faire mousser ou réaliser des méfaits. Ne soyez pas ce gars !

***EXPLOIT :**
Il s'agit d'un morceau de code qui permet d'exploiter un bug ou une faille de sécurité dans un système informatique. On le confond parfois avec la faille elle-même alors qu'il ne s'agit que du «levier».

***PAYLOAD :** Un payload est une action permise par une infection. Il s'agit de la partie «concrète» d'un malware.

Metasploit est un projet ayant pour but de réunir des informations sur les vulnérabilités de divers systèmes informatiques : Windows, Linux, Mac, FreeBSD, etc. Le but est de vérifier que votre propre système ne comprend pas de failles critiques permettant à un assaillant de prendre le contrôle de votre machine ou d'avoir accès à vos fichiers. Le problème, c'est que Metasploit ne s'utilise qu'en ligne de commandes et que tout ça est un peu «rugueux». Heureusement, Armitage ajoute une interface graphique plus conviviale. Les plus grincheux souligneront que ce type d'outil est plutôt destiné aux scripts kiddies, mais il faut bien commencer son éducation quelque part non ? Pour éviter de nous adresser aux «black hats» en herbe, nous allons simplement voir comment scanner votre réseau local à la recherche d'une faiblesse... Mais comme il faut bien s'amuser un peu nous allons contaminer et prendre le contrôle d'une de nos machines.

Microsoft édite un bulletin de sécurité dès qu'une faille est connue, il en résulte une mise à jour peu de temps après. Par exemple, le correctif KB958644 colmate la faille répertoriée sous le nom MS08-067. Nous avons choisi cet exemple, car cette faille est utilisée par le ver Conficker et reste très problématique sur XP ou sur les systèmes piratés qui ne seraient jamais mis à jour...

PAS À PAS

Comment auditer votre réseau ?

CE QU'IL VOUS FAUT

KALI LINUX 2

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

DIFFICULTÉ :

01 MISE EN PLACE

Commençons par mettre à jour les programmes, votre distribution et la liste des exploits. Si vous êtes en root tapez dans un terminal:

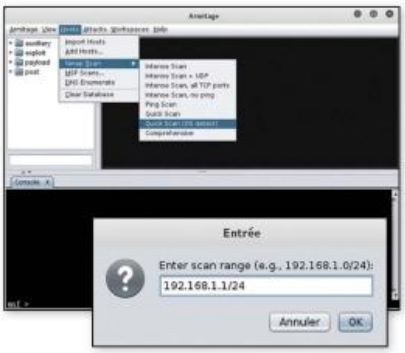
apt-get update
apt-get dist-upgrade
msfupdate

Avant de lancer le logiciel, lancez une base MySQL, car Armitage fonctionne depuis une base locale. Lancez enfin Armitage, vous le trouverez sur la barre de lancement rapide à gauche. Dans la fenêtre qui va s'afficher, faites juste **Connect** sans changer les réglages. Si vous rencontrez un problème, tapez dans un terminal:
msfdb init

Faites **Oui** lorsqu'on vous demandera de créer un serveur RPC. Attendez que la barre de progression se termine et que l'interface s'affiche.

02 LE MAPPAGE DE VOTRE RÉSEAU

Dans **Host>Nmap Scan**, faites **Quick Scan (OS Detect)** et tapez l'adresse IP locale de votre box. Ce sera soit 192.168.1.1 ou 192.168.0.1 auquel vous ajouterez /24. Pour notre réseau, ce sera donc **192.168.1.1/24**. Nmap va afficher les différents appareils connectés à votre réseau avec le type d'OS. Notez que cela ne fonctionne pas toujours comme il faut: l'imprimante affichée ici est en fait un NAS. Vous pouvez changer les icônes si cela vous embête.



03 LA LISTE DES EXPLOITS

Dans le menu **Attacks**, faites **Find Attack** et laissez la liste se charger. Lorsque ce sera fini, vous pourrez alors faire un clic droit sur chaque appareil du réseau et faire **Attack**. Vous aurez alors l'embarras du choix. Si vous redoutez une attaque particulière, vous pouvez la choisir dans la liste, mais pour tester toutes les attaques d'une catégorie, faites **Check exploits**. Attention, dans **Http** par exemple, il y en a des dizaines (allez sur More plusieurs fois).

04 UN EXEMPLE...

Vous pouvez par exemple commencer par **Attack>smb>ms10_061_spoolss** qui permet pour un attaquant d'exécuter du code en passant par le spooler d'imprimante. Après avoir fait **Launch**, si la réponse (dans la partie en bas) est **Check**, **The target is not exploitable**, c'est que vous êtes à l'abri. Par contre, un plus vert entre crochets **[+]** indique qu'il y a quelque chose à exploiter. Pareil, si vous voyez le mot **successful** quelque part. Pour vous protéger, il faudra alors aller sur Google et chercher la solution avec le nom de l'exploit. Si le problème persiste après une mise à jour, c'est sans doute que votre antivirus ou votre pare-feu est en défaut.

05 HAIL MARY ET L'ATTAQUE À TOUT VA

Vous n'y connaissez rien et vous ne voulez pas y passer des heures? Que diriez-vous d'un petit «*Je vous salue Marie*»? Pas une prière, mais l'option **Hail Mary** dans le menu **Attacks** en haut. Il s'agit en fait d'essayer tous les exploits disponibles sur toutes les machines de votre réseau. Pas de détail donc, mais attention, le processus est long et pas vraiment subtil. Qu'à cela ne tienne, nous sommes ici pour découvrir des vulnérabilités, non?

PAS À PAS

Un exemple d'attaque amusante

CE QU'IL VOUS FAUT

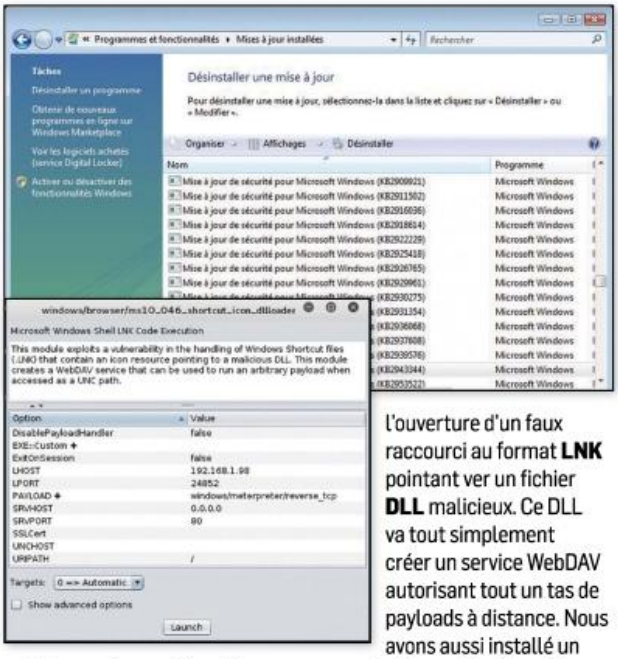
KALI LINUX 2

OÙ LE TROUVER ? :
www.kali.org

DIFFICULTÉ :

01 NOTRE MACHINE DE TEST

Pour notre démonstration, nous avons ajouté à notre réseau un PC sous Vista SP2 64 bits que nous avons délibérément «sabotés»: la mise à jour de sécurité **KB2286198** sensée colmater la faille **ms10_046_shortcut_icon_dllloader** a été désinstallée. Cette dernière autorise



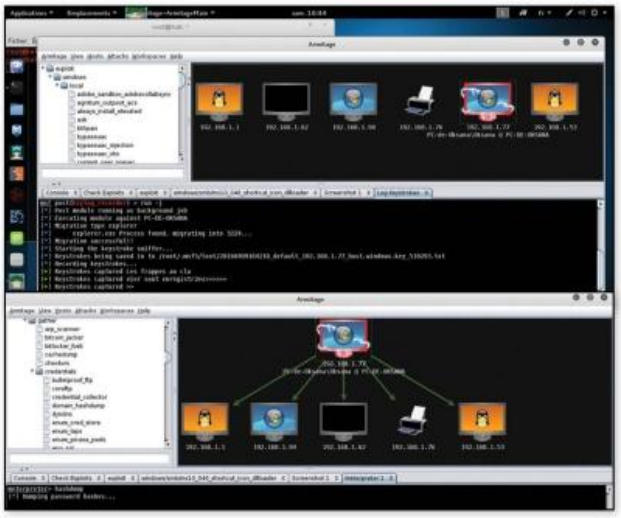
l'ouverture d'un faux raccourci au format **LNK** pointant ver un fichier **DLL** malicieux. Ce DLL va tout simplement créer un service WebDAV autorisant tout un tas de payloads à distance. Nous avons aussi installé un antivirus sur la machine cible sans pour autant le mettre à jour. Par contre, le pare-feu est activé.

02 NOTRE EXPLOIT

Trouvons **ms10_046_shortcut_icon_dllloader** dans la zone de recherche à gauche et lançons l'exploit avec **Launch**. Il s'agit d'un exploit spécial puisqu'un serveur sera créé sur votre machine sous Kali tandis que le client sera contenu dans un fichier **msf.lnk** qui sera créé dans **/root/** (affichez les dossiers cachés dans les modes d'affichage pour le voir). Il faudra transmettre ce fichier à la machine cible. Comme il ne s'agit pas d'un EXE ou d'un BAT, la tâche n'est pas très compliquée. Sachez tout de même qu'un antivirus correctement configuré ne laisserait pas passer ça.

03 LE PC EST INFECTÉ

Dès que la victime aura accepté le fichier **LNK** (via Skype, une clé USB, un e-mail, etc.) et cliqué dessus, les carottes sont cuites! Le PC sous Vista est infecté: vous verrez que son icône changera d'apparence: rouge avec des petits éclairs autour. Faites un clic droit et allez dans **Meterpreter** pour voir vos nouveaux super pouvoirs. Dans **Explore**, vous pourrez enregistrer les frappes au clavier de la victime (**Log Keystroke**), regarder les processus actifs (**Show Process**) ou les fichiers contenus dans le disque dur (**Browse File**). **Pivoting** permet d'attaquer virtuellement depuis une autre machine.



04 PAYLOADS À LA CARTE

Vous pouvez aussi prendre une capture d'écran du bureau (**Screenshot**). Le pare-feu que nous avons laissé sur la machine empêchera cependant la prise de contrôle à distance (**Desktop VNC**) et la prise de contrôle de la webcam (voir notre article sur WSMC à la page 15), mais avec un firewall bancal ou un utilisateur habitué à cliquer **Oui** dès que le pare-feu se manifeste, cela est fort envisageable. Dans **Access**, on peut aussi imaginer charger les hash (**Dump Hash**) du fichier SAM contenant le mot de passe Windows. Avec **Persist**, on peut aussi faire en sorte de garder l'accès à ce PC, même si ce dernier n'est plus sur votre réseau...

N°1 en kiosques
NOUVEAU !

Le GUIDE non officiel de l'utilisateur WINDOWS 10

PC – Tablettes – Smartphones

CHIFFREZ VOTRE TÉLÉPHONE !

Comptes, paramètres, fichiers et applications : il est possible de chiffrer tout ce que contient votre téléphone. Pratique en cas de vol ou si vous avez des données sensibles, le chiffrement est accessible à tous, mais n'est peut-être pas une solution miracle pour tout le monde. Voyons de plus près les mécanismes d'Android, les précautions à prendre et même comment chiffrer vos conversations et SMS.

Avant de se mettre à l'ouvrage, prenons quelques instants pour réfléchir. Avez-vous vraiment besoin de chiffrer le contenu de votre téléphone ? Si votre appareil est protégé avec un code ou un schéma de verrouillage, c'est peut-être suffisant pour mettre à l'abri vos photos ou autres documents stockés en local, votre compte Gmail ou Paypal. En cas de vol, le premier réflexe du malandrin sera d'effacer le contenu, de changer l'IMEI pour revendre votre Xpersung le plus vite possible sans aller chercher des photos de vos fesses dans les entrailles de la bête (ce qui est possible sans chiffrement, mais pas à la portée de tous).

LE CHIFFREMENT, INDISPENSABLE ?

Par contre, le chiffrement peut-être utile si vous êtes une cible potentielle pour l'espionnage ou que d'autres personnes que vous sont concernées par les données contenues sur votre téléphone : ingénieur, haut fonctionnaire, élu, journaliste, etc. Il faut aussi savoir qu'une fois que le chiffrement est activé, vous ne pouvez plus faire machine arrière à moins de réinitialiser votre appareil avec ses valeurs d'usine. Il faudra donc absolument faire une sauvegarde avant le chiffrement (car des accidents peuvent arriver) et avant un éventuel retour à la normale (vous avez changé d'avis, vous voulez vendre votre téléphone, etc.) Notez aussi que

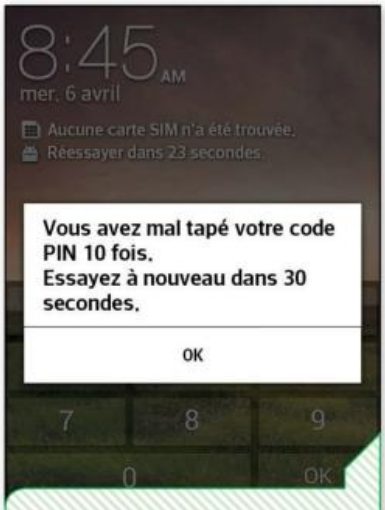
LEXIQUE

BRUTE FORCE :
Méthode de récupération de mot de passe qui consiste à essayer toutes les combinaisons de caractères pour tomber sur la bonne entrée. Le logiciel va essayer toutes les combinaisons de lettres, de chiffres et autres caractères pour arriver à ses fins.

dans certains cas vous ne pourrez plus mettre à jour le système ou certaines applis de sécurité et que le chiffrement est parfois lourd pour les appareils les plus anciens ou d'entrée de gamme.

UN CHIFFREMENT QUI S'AMÉLIORE

Nous ne parlerons ici que du système Android puisque sur l'iPhone (depuis la sortie du 3GS et du système iOS 4), Apple a choisi de fournir une méthode de chiffrement intégré devenu contournable. Sur Android, le chiffrement s'appelle Full Disk Encryption (FDE). Disponible dès les versions 3 (Honeycomb pour tablettes) et 4 (Ice Cream Sandwich), le FDE était malheureusement vulnérable aux attaques «off-device». Il est donc possible de brancher un téléphone sur un PC et de bidouiller le contenu avec ADB (Android Debug Bridge) pour retrouver le contenu chiffré. Il faudra bien sûr lancer une attaque brute force peu évidente, mais le risque est bien là. L'arrivée de la version Lollipop 5.0 a changé la donne. Non seulement le chiffrement est proposé lors du premier lancement, mais les mécanismes de chiffrements ont évolué. Dorénavant, une clé 128 bits est générée au premier lancement, elle est ensuite hashée (SHA256) et signée dans une partie hardware du téléphone et pas simplement dans la mémoire flash. Les risques de fuite sont donc à ce jour nuls. Google a même senti le vent du changement puisque sur ses Nexus, le chiffrement est obligatoire sur le système 5.0 tandis qu'il le sera pour tous les appareils suffisamment puissants avec la version 6. La bonne nouvelle, c'est qu'il s'agisse des versions 3, 4, ou 5, le processus de chiffrement est le même pour l'utilisateur. Et comme nous sommes gentils, nous vous rappelons ensuite comment chiffrer vos conversations et vos SMS.
Suivez le guide...



Pour un voleur, l'attaque «brute force» est presque impossible puisque le système vous fera patienter durant de longues secondes toutes les 10 tentatives infructueuses. Avec des techniques poussées, cela est pourtant possible d'où l'intérêt de bien choisir son mot de passe.

PAS À PAS

Chiffrer le contenu de votre téléphone

01 LES OPTIONS DE SÉCURITÉ

Rappelons avant de commencer qu'il faudra faire une sauvegarde de vos données avant de chiffrer votre téléphone. Allez dans **Paramètres** puis sélectionnez **Sécurité**. Suivant la marque de votre appareil et votre version d'Android, vous trouverez l'option **Chiffrer l'appareil** ou **Crypter le téléphone**.

02 PRENEZ VOS PRÉCAUTIONS

Il faudra ensuite suivre les instructions. La plupart du temps, on vous demandera de brancher le téléphone sur secteur ou de démarrer le processus avec 80% de batterie disponible. Car en interrompant le processus, vous perdrez vos données.

03 LE MODE DE VERROUILLAGE

Sélectionnez ensuite un mode de déverrouillage. Encore une fois, selon la marque et la version du système, les options peuvent varier. Si vous utilisez une version antérieure à Lollipop (5.0), utilisez un mot de passe solide à la place d'un PIN standard pour rendre difficile l'attaque «brute force».

04 LAISSEZ LE CHARME AGIR !

Après avoir saisi votre sésame, vous devrez une nouvelle fois valider pour commencer le processus de chiffrement. Le délai est variable suivant la quantité de données que vous avez stockées, mais il ne devrait pas dépasser une heure. Votre téléphone devrait redémarrer plusieurs fois, alors surtout ne faites pas de manipulation hasardeuse!

PAS À PAS

Chiffrer vos appels et vos SMS

01 TÉLÉPHONEZ CHIFFRÉ AVEC DISCRETIO

Dans *Pirate Informatique* n°17, nous vous avions présenté Discretio, une appli révolutionnaire qui permet à deux correspondants de communiquer en WiFi ou 3G. L'authentification comme le contenu de la conversation seront chiffrés et même une analyse poussée des paquets ne révélera rien. Si vous souhaitez vous la jouer Jack Bauer ou tout simplement éviter les IMSI Catcher (voir les Dossiers du Pirate n°4)...
Lien: **http://goo.gl/HNacD1**

02 VOS SMS CHIFFRÉS AVEC SMSSECURE

SMSSecure est un «fork» de TextSecure. Comme son prédécesseur, SMSSecure va s'ajouter à votre appli standard d'envoi de SMS pour vous proposer de chiffrer en 256 bits vos textos ou MMS avant de les envoyer à vos destinataires. Même si un gouvernement ou un pirate arrive à intercepter vos correspondances, les petits curieux n'auront dans les mains qu'une suite de caractères incompréhensible. Pour que cela fonctionne, il faut que SMSSecure soit installé sur les appareils de vos amis.
Lien: **https://goo.gl/tEKD3v**

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

100% Windows

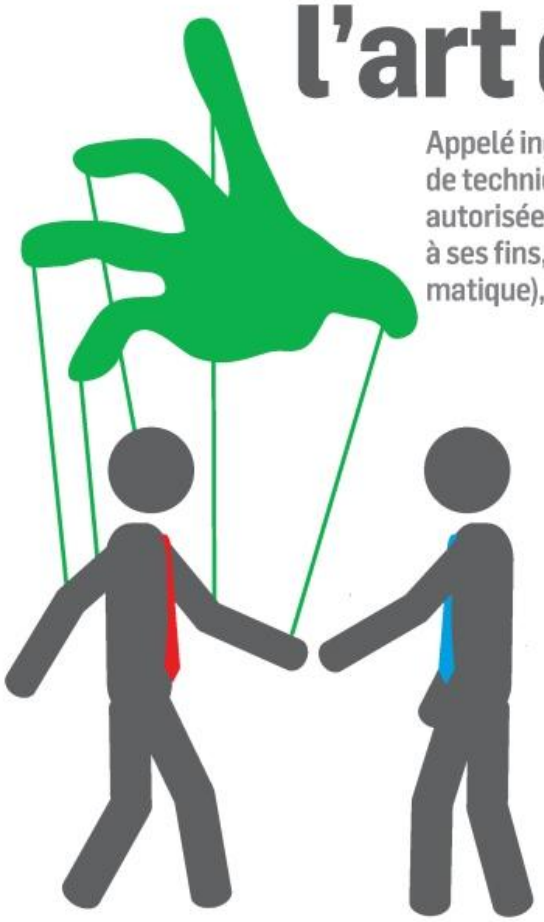
Actuellement #Guide pratique

100 PAGES DE TUTOS POUR DÉPANNER SON PC

SOCIAL ENGINEERING :

l'art de la tromperie

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



Einstein disait «*Deux choses sont infinies : l'Univers et la bêtise humaine. Mais, en ce qui concerne l'Univers, je n'en ai pas encore acquis la certitude absolue*». En utilisant la bêtise, l'ignorance, la peur, l'avarice, la fierté, la paresse ou la crédulité de certaines personnes, il est possible d'obtenir ce qu'on veut. Pourquoi essayer de hacker un mot de passe, s'il suffit de le demander «gentiment». Ce n'est pas aussi simple que cela, mais en utilisant un peu sa tête, il est possible de manipuler les gens pour leur faire croire à certaines situations et leur «monter un bateau». Il faut pour cela se mettre dans la tête de la cible. Il existe pour cela plusieurs techniques. Par téléphone par exemple, le but du pirate est d'avoir un renseignement le plus rapidement possible. Pour cela, il aura préparé son personnage, son discours et son «histoire». Il sera très persuasif dans le timbre de sa voix. Certains hackers ont quelques techniques pour parfaire leur crédibilité, comme posséder un logiciel qui va générer des bruits de bureau ou qui va changer le timbre de la voix pour imiter celle d'une secrétaire ou d'un vieux monsieur (comme MorphVOX Pro par exemple).

La fraude au président, comment ça marche ?

C'est l'été et à la société X, les dirigeants sont en vacances, en RTT ou en pause-déjeuner... Le téléphone sonne et c'est une secrétaire qui décroche.

La secrétaire : -Société X, bonjour !
Le pirate : -Bonjour mon petit, c'est Mr Untel. J'appelle car je m'inquiète pour le virement que nous devions envoyer en Moldavie. Personne ne m'a confirmé quoi que ce soit.
La secrétaire : - Pardon, vous êtes Monsieur comment ?
Le pirate : -Enfin mademoiselle, vous n'êtes pas familière avec l'organigramme de X ? C'est Monsieur Untel, le président de la zone Europe de la compagnie pour laquelle vous travaillez !
La secrétaire : -Heu...
Le pirate : -Bon, passez-moi Louisa s'il vous plaît. [*il utilise délibérément un prénom, trouvé sur Internet par exemple, pour montrer qu'il connaît la personne et qu'il est le chef*]
La secrétaire : -Heu, Madame Machin est en vacances et... [*pour la secrétaire, Louisa c'est Madame Machin, cela renforce la conviction que son interlocuteur est bien un patron*]
Le pirate : -Et Thierry, il est là ?
La secrétaire : -Heu, Monsieur Michu est en congé paternité et...
Le pirate : -Ha oui effectivement, il me l'avait dit.

0110101010001001101010001000101010110010010010101000100101001010010101010010000

LES PRÉCAUTIONS À PRENDRE

1▸ VERROUILLER LES ACCÈS

Attention aux accès : physiques ou numériques. Une porte ouverte, un PC allumé ou une clé USB oubliée sont des points faibles qu'un pirate peut exploiter. De même, il faut sensibiliser les employés au risque des réseaux sociaux. Divulguer des informations sur sa société peut se faire sur Facebook mais aussi au bar du coin.

2▸ SENSIBILISER LES EMPLOYÉS

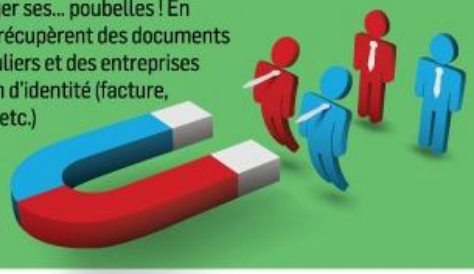
Dans notre exemple de l'arnaque au président, le pirate a utilisé la peur pour arriver à ses fins, mais on peut aussi imaginer utiliser la flatterie (« *Thierry m'a dit le plus grand bien de vous* ») ou l'empathie (« *Ho ma pauvre, vous êtes seule au bureau alors qu'il fait si beau...* ») Il faut aussi sensibiliser les employés à cela. Si quelqu'un veut faire votre travail à votre place, c'est louche.

3▸ ÉTABLIR UNE CHAÎNE DE COMMANDEMENT

Toujours au niveau de la sensibilisation des employés, vérifiez que ces derniers connaissent les personnes avec qui elles auront l'habitude de travailler et sur leurs compétences en matière de sécurité informatique : la solidité des mots de passe et la non-divulgation de ces derniers. Attention aussi aux copieurs : site Internet (phishing), lettre à en-tête, nom de domaine d'un e-mail, etc.

4▸ DÉTRUISER LES DOCUMENTS IMPORTANTS

Il faut aussi protéger ses... poubelles ! En effet, de nombreux hackers récupèrent des documents dans les déchets des particuliers et des entreprises pour parfaire une usurpation d'identité (facture, numéro de sécurité sociale, etc.) ou mieux connaître la cible (noms, fonctions, horaires ou montants du salaire des employés).



UNE SEULE PARADE : LA PARANOÏA

Il existe aussi d'autres cas de figure. Par exemple, le pirate peut prendre contact avec la société par lettre : en-tête, logo et filigrane à l'appui. On peut aussi imaginer une boîte postale avec un nom d'emprunt pour une société fictive ou avec un nom semant la confusion. Via Internet, le pirate peut se faire passer pour un responsable informatique ou un ingénieur réseau dans l'espoir d'obtenir des informations sensibles : mots de passe, personne présente ou pas dans les locaux, etc. On peut aussi imaginer un contact direct. Ici, les accessoires seront un costard-cravate ou un bleu de travail en fonction de son «histoire». Le pirate peut aussi cumuler ces différentes techniques : téléphoner pour obtenir un rendez-vous puis confirmer par e-mail pour mieux vous gruger lors de l'entretien où vous vous rendrez compte qu'il partage la même passion que vous pour la pêche à la mouche ou le yoyo ! Pour une entreprise, il est absolument vital de former le personnel à ce genre de problème. Un pirate prendra soin de s'attaquer aux personnes les plus «faibles» techniquement : secrétaires, comptables, stagiaires et les petits nouveaux. Mais sans parler de récupération de mots de passe, il existe d'autres manœuvres pour se jouer de personnes faibles, car nouvelles, jeunes ou impressionnables.

Vous avez déjà entendu parler de la «fraude au président» (voir notre exemple) ?

KEVIN MITNICK ET SON «ART OF DECEPTION»

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

[ça, c'est de l'impro mais ça fonctionne]
Et bien, il va falloir que vous fassiez vous-même ce virement. Je vous envoie les détails sur l'e-mail de Thierry. Vous y avez accès ?

La secrétaire : -Oui oui, bien sûr ! [*trop contente d'enfin pouvoir se «rattraper» auprès du grand patron*]

Et voilà comment se faire virer 10, 20, 50 000 € ou même plus sur un compte à l'étranger. Il suffit de cibler le montant en fonction du volume d'affaire de la société. Bien sûr, cela peut bloquer avec la banque (qui ne connaît pas ce compte suspect), mais là encore il existe des moyens de faire passer la pilule.
Le pirate peut aussi utiliser un clone de l'e-mail de Monsieur Michu pour joindre la secrétaire et dire quelque chose du genre : «*Monsieur Untel va appeler, j'ai oublié de faire un virement, sauvez-moi la mise* !». On peut aussi imaginer un pirate qui se ferait passer pour un fournisseur et qui notifierait la société X d'un changement de RIB. Tous les virements vers ce fournisseur iront dans les poches des pirates...

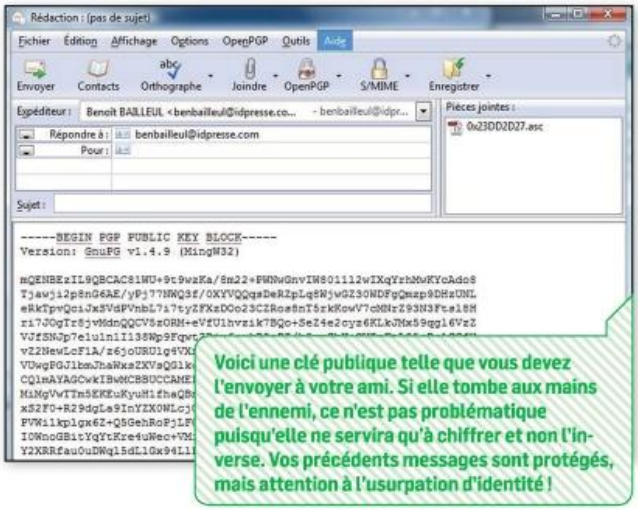
CHIFFREMENT SYMÉTRIQUE ET ASYMÉTRIQUE

Dans nos pages, nous parlons souvent de chiffrement asymétrique ou de clé publique. Même si nous expliquons les termes dans les lexiques, certains lecteurs nous ont demandé de faire le point sur ces différentes notions... Car, même si les logiciels modernes s'occupent de tout, il est intéressant de savoir comment tout cela fonctionne.

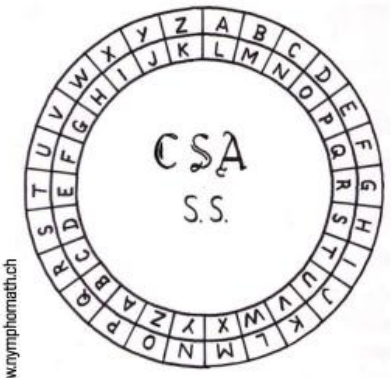
Pour échanger des messages avec un interlocuteur sans que ces derniers soient interceptés, on peut le masquer (c'est le principe de la stéganographie, voir *Pirate Informatique n°10*), mais on peut aussi le «chiffrer». Il s'agit d'une méthode mathématique qui va modifier le fichier en utilisant une constante : la clé de chiffrement. Jules César par exemple utilisait une méthode de chiffrement par décalage de X caractères dans l'alphabet latin. Avec un décalage de 4, il fallait lire E à la place d'un A. Bien sûr, ce type de chiffrement très rudimentaire (il n'y a que 26 lettres dans l'alphabet ce qui ne laisse que 26 possibilités) a laissé place à des algorithmes plus complexes et aux masques jetables. Avec l'informatique, ce ne sont plus uniquement les écrits qui peuvent être chiffrés, mais n'importe quel type de fichier numérique. Une photo ou un enregistrement multimédia étant constitué de 0 et de 1, il est donc possible de les chiffrer pour rendre le fichier inaccessible à celui qui n'a pas la bonne clé. Lorsqu'on parle de chiffrement symétrique, la clé est la même pour les deux interlocuteurs. On encode et on décode le message avec la même clé. Cette clé est une suite binaire plus ou moins longue. Le problème avec ce type de chiffrement est la transmission de la clé. Si le canal n'est pas lui-même sécurisé, la clé peut se retrouver dans la nature et compromettre le secret. Et plus on a d'interlocuteurs, plus on a un risque de fuite.

CLÉ PUBLIQUE POUR LE CHIFFREMENT, CLÉ PRIVÉE POUR LE DÉCHIFFREMENT

C'est ainsi que dans les années 70 des chercheurs ont planché sur cette problématique. Comment échanger des clés via un canal non sécurisé tout en permettant le chiffrement ? En utilisant 2 clés pour chaque intervenant : une clé privée, jamais dévoilée et une clé publique qu'il est possible d'envoyer par e-mail, SMS ou même en la chantant à tue-tête. Votre ami



Voici une clé publique telle que vous devez l'envoyer à votre ami. Si elle tombe aux mains de l'ennemi, ce n'est pas problématique puisqu'elle ne servira qu'à chiffrer et non l'inverse. Vos précédents messages sont protégés, mais attention à l'usurpation d'identité !



Cadran sudiste

© www.nymphomath.ch

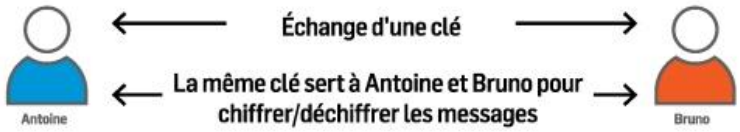
Un type de cadran de chiffrement utilisé pendant la guerre de Sécession. Il s'agit seulement d'un type de chiffrement par décalage de 11 caractères. Pas étonnant qu'ils aient perdu la guerre...

n'aura qu'à chiffrer son message ou fichier avec votre clé publique. De votre côté, vous le déchiffrerez avec votre clé privée que vous êtes le seul à posséder. La paire de clés d'une personne a été générée parallèlement et il est bien sûr impossible de déduire la clé privée d'une personne en connaissant sa clé publique même si les deux sont étroitement liées.

ÊTRE SÛR DE SON INTERLOCUTEUR

Le principe de la «signature» est légèrement différent, mais il fonctionne aussi avec un système de paires de clés. Comment être sûr que ce message vient bien de votre ami et pas d'un usurpateur ? Si vous communiquez par un nouveau canal, cette opération est primordiale. Il suffit en fait d'envoyer un message chiffré avec votre clé privée. Pour savoir si c'est de vous dont il s'agit, votre ami devra décoder le message avec votre clé publique. Faites l'inverse pour savoir si votre ami est bien celui qu'il prétend ! Une fois mutuellement authentifié, vous pourrez converser par la méthode énoncée plus haut : déchiffrement avec votre clé privée d'un message envoyé par votre ami chiffré avec votre clé publique. Vous êtes perdus ? Regardez nos infographies...

1▸ CHIFFREMENT SYMÉTRIQUE



Problème : si la clé est interceptée, toutes les communications passées, présentes et futures sont compromises.

2▸ CHIFFREMENT ASYMÉTRIQUE : LES DEUX PRINCIPES

Antoine et Bruno génèrent chacun de leur côté une paire de clés avec un logiciel. Les deux amis s'échangent alors leurs clés publiques.

3▸ CHIFFREMENT ASYMÉTRIQUE : LA PRATIQUE

En pratique, les logiciels prennent en charge automatiquement toute cette suite d'événements pour à la fois signer et garantir la confidentialité. Voyons comment cela fonctionne...

cRARk : CRACKEZ AVEC VOTRE CARTE GRAPHIQUE !

Dans notre précédent numéro, nous avons vu comment cracker le chiffrement du format ZIP avec plusieurs méthodes. Dans ces pages, nous allons étudier le fonctionnement de cRARk, un logiciel qui s'attaque au RAR et au 7z. Celui-ci a la particularité d'utiliser la puissance du GPU de votre carte graphique pour arriver à ses fins...

LEXIQUE

***CPU :**
Accronyme de Central Processing Unit. C'est votre processeur : Intel i3, i5, i7, Celeron ou leurs alter ego chez AMD.

***GPU :**
C'est le processeur de votre carte graphique. Ils sont souvent plus doués pour le calcul parallèle que les CPU...

***BRUTE FORCE :**
Méthode de récupération de mot de passe qui consiste à essayer toutes les combinaisons de caractères pour tomber sur la bonne entrée. Le logiciel va essayer toutes les combinaisons de lettres, de chiffres et autres caractères pour arriver à ses fins.

CRARk utilise la puissance de votre GPU pour attaquer en brute force le chiffrement AES256 des fichiers RAR et 7z. Pourquoi utiliser le GPU ? Parce que l'architecture de ce dernier s'y prête plus que le CPU : plus de cœurs permettant des calculs en parallèle. Il faut juste que votre carte graphique soit compatible avec les technologies CUDA de nVidia ou OpenCL de AMD/ATI (à ne pas confondre avec OpenGL).

JUSQU'À 30 FOIS PLUS RAPIDE

Attention, car les cartes graphiques intégrées ou bas de gamme se montreront parfois moins puissantes que le CPU. Et comme cRARk ne supporte pas le multicœur, il faudra d'abord savoir quel processeur utiliser. De même, le logiciel est spécialisé dans le brute force. L'attaque par dictionnaire est possible, mais cela ne se fera qu'avec le CPU. Et il serait bien dommage de s'en passer puisqu'avec des cartes graphiques très puissantes, la rapidité d'exécution peut être multipliée par 30. Comme le chiffrement AES des formats RAR et 7z est réputé plus solide que le ZipCrypto que nous avons utilisé dans le numéro 28 de Pirate Informatique, ce gain de puissance ne sera pas de trop...

La version pour les fichiers RAR de cRARk dispose d'une interface graphique appelée cRARk GUI. Mettez l'EXE dans le dossier contenant cRARk et lancez-le. Notez que ce logiciel n'a pas été créé par le développeur de cRARk et qu'il ne fonctionne pas avec les fichiers 7Zip.

Lien : http://goo.gl/06fPqU

PARALLEL PASSWORD RECOVERY

Si vous cherchez un outil similaire avec une interface graphique et utilisant la pleine puissance de votre CPU et de votre GPU, Parallel Password Recovery est un logiciel qui utilise le code de cRARk. Le problème, c'est que ce dernier est payant (à partir de 27 €). Pour vous faire une idée, vous pouvez néanmoins utiliser la version démo, limitée à la recherche de mots de passe de moins de 5 caractères...

Lien : **www.parallelrecovery.com**

Nos expériences avec cRARk

CE QU'IL VOUS FAUT

CRARK
OÙ LE TROUVER ? : **www.crark.net**

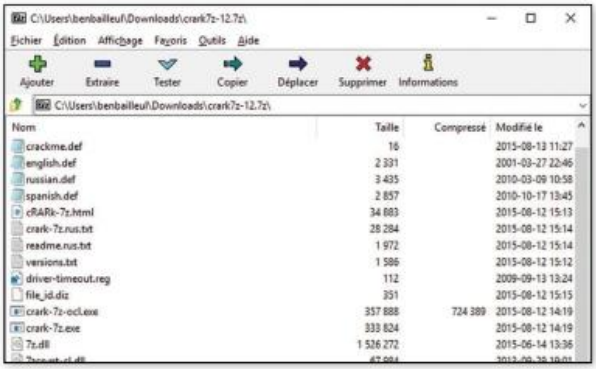
GPU CAPS VIEWER
OÙ LE TROUVER ? : **http://goo.gl/zKdUT9**
DIFFICULTÉ : ☠☠☠

01 LES PILOTES

Avant d'utiliser cRARk, il faudra d'abord s'assurer que votre carte graphique est compatible avec les technologies OpenCL ou CUDA. Pour notre vieille Radeon Mobility HD 5000 de 2010, ce sera la première option. Téléchargez GPU Caps Viewer et regardez le champ **OpenCL** du premier onglet. Si vous voyez **GPU** et si la case idoine est cochée dans **GPU Computing** c'est bon! En cas de problème, désinstallez tous les pilotes de votre carte graphique et téléchargez les derniers en date. Évitez les pilotes génériques de Microsoft.

02 PLUSIEURS VERSIONS

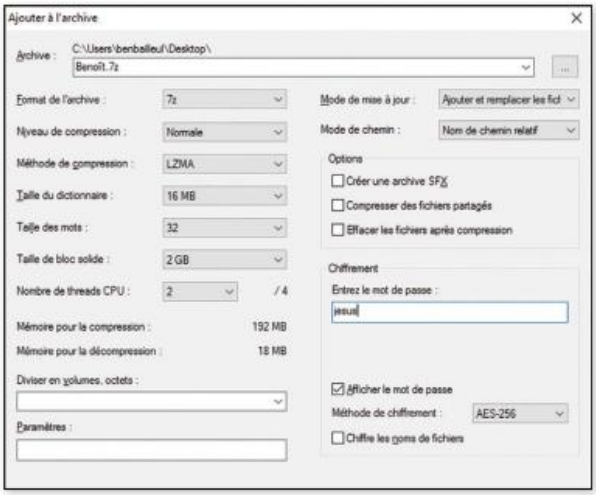
Il faudra ensuite choisir votre version en fonction de votre fichier cible (RAR ou 7z) et de votre système 32 ou 64 bits. Notez que la version pour les RAR contient le logiciel écrit pour l'OpenCL (**ocl**) et pour CUDA tandis que les versions pour 7-zip sont séparées. Si



vous avez Linux ou MacOS, vous trouverez aussi votre bonheur. Décompactez l'archive dans un dossier, mais faites attention de ne pas inclure le fichier **crackme** qui est lui-même chiffré et fourni à titre de test.

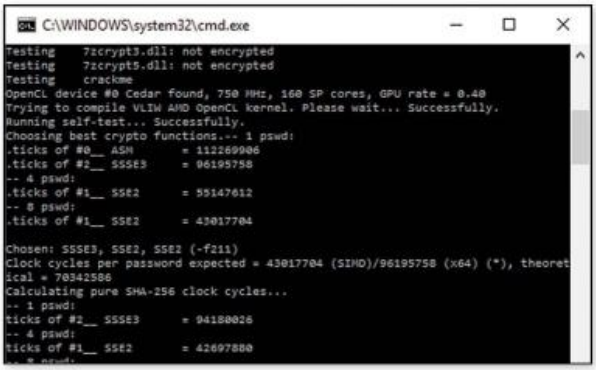
03 NOS FICHIERS DE TEST

Pour nos tests, nous avons créé 3 fichiers de test avec trois mots de passe différents: **jesus**, **&1e** et **AzErTy**. Ils sont très simples, car avec moins de 200 mots par seconde un mot de passe de 8 caractères en minuscules mettrait des mois pour être retrouvé. Le dernier nous aidera à utiliser une option de la dernière chance un peu plus loin. Lançons un benchmark avant d'attaquer. Maintenez la pression sur la touche **Maj** du clavier et faites un clic droit dans le dossier contenant vos fichiers et sélectionnez **Ouvrir une fenêtre de commandes ici**. Tapez ensuite **crark-7zip-ocl.exe -b test.7z** (puisque nous utilisons la version 7-zip avec une carte compatible OpenCL).



04 LA COMPARAISON DES PUISSANCES

Si vous voyez **OpenCL capable device not found** (ou CUDA), c'est que vous avez un problème avec la reconnaissance de votre carte graphique. Si tout se passe bien, vous devriez voir des lignes de textes défiler et à la fin, le nombre de mots de passe testé à la seconde. Sur notre vieille machine de test, le GPU peut tester 127 mots à la seconde (cela peut monter jusqu'à 15000 avec une GeForce GTX). Pour voir la différence avec votre CPU, désactivez l'OpenCL ou le CUDA avec GPU Caps Viewer. Pour nous, le GPU est avantageux, puisque le résultat est de 52 sésames à la seconde avec le processeur.



05 PROGRAMMONS L'ATTAQUE

Avant d'attaquer, il nous reste encore à paramétrer le fichier de configuration. Renommez le fichier **english.def** en **password.def** et ouvrez-le avec un éditeur de texte (le **Bloc-note** par exemple). Ce fichier est programmable: tout ce qui commence par **#** est considéré comme un commentaire et ne sera pas appliqué. Trouvez les lignes suivantes:

 # Most common definition - brute-force search using
 # only lower-case Latin letters.

Normalement, vous trouverez **[$a]*** en dessous ce qui correspond à la recherche des minuscules. À vous de voir le type de caractère que vous recherchez. Si vous vous souvenez que votre sésame ne comprend que des chiffres, il faudra mettre **[$1]***. Et si vous n'avez aucune idée, mettez **[$a $A $1 $!]*** pour tous les types de caractères. N'oubliez pas de sauvegarder. Attention, cette méthode est très longue voir sans issue.

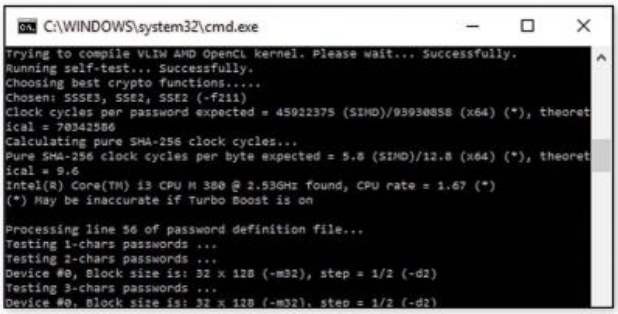
```
# End of charset definition
#
##
# Here password definitions begins.
#
# Password definition
#
# Most common definition - brute-force search using
# only lower-case Latin letters.
[$a $A $1 $!]*

# The same as the above, but using both cases Latin letter
# [$a $A] *

# Search for password consisting of digits only
# $1 *
```

06 AJOUTER LES CARACTÈRES FRANÇAIS

Tapez enfin **crark-7zip-ocl.exe test.7z** et laissez cRARk faire son travail. Dans notre tentative de trouver **jesus** (il est parmi nous, vous le saviez ?) en utilisant cette technique, le logiciel mettra plusieurs jours tandis qu'il mettra moins de deux heures en ne cherchant que des minuscules. D'où l'intérêt d'avoir des souvenirs ou des indices sur le mot de passe recherché! Avec seulement 3 caractères de toutes origines, **&1e** n'a tenu que quelques minutes, mais si nous nous étions cantonnés aux seules minuscules, nous n'aurions jamais cracké ce mot de passe. Le problème de notre fichier **password.def** est qu'il est basé sur les caractères anglais (vous vous souvenez l'avoir renommé non?). Pour les caractères espagnol ou russe, il y a des fichiers préconfigurés, mais pas pour le français. Pas de problème, il suffit d'ajouter les caractères accentués et la cédille dans le champ **# $a = [abcdefghijklmnopqrstuvwxyz]** sans oublier de retirer le **#**.

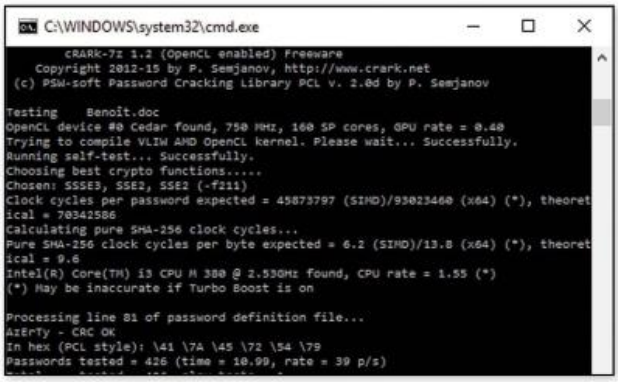


07 JE L'AI PRESQUE !

Nous passerons le reste des réglages dédiés à l'attaque par dictionnaire pour nous concentrer sur une option très intéressante: la ligne 81 et la fameuse option «*purée, je l'ai presque*». Imaginons que vous vous souveniez presque de votre mot de passe. En lieu et place d'**AzErTy,** vous vous souvenez d'**AzErTY**. Allez dans **password.def**, remettez le **#** devant les autres champs pour les rendre inactifs et regardez en bas du document aux lignes:

 # If you almost remember the whole password, but you
 # probably has mistyped it (let the password was
«MyPass1234»)

Tapez **{AzErTY}** (sans **#**) en dessous. Le logiciel cherchera alors à trouver le bon mot de passe à partir de celui que vous croyez être le bon. Dans cet exemple très simple, le bon mot de passe a été retrouvé en moins d'une minute.



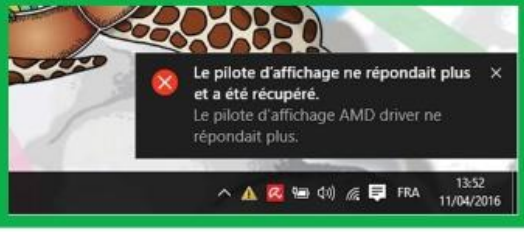
UN PROBLÈME ? QUE DES SOLUTIONS...

Si vous avez un message d'erreur concernant le **delay** du GPU (**exeed timeout**) ou si Windows vous annonce une perte du pilote d'affichage, cela peut avoir différentes cause:

1 • Si vous avez le choix, évitez de cracker en utilisant votre circuit vidéo primaire.

2 • Utilisez la commande **-d**. Par exemple, **crark-7zip-ocl.exe -d5 test.7z** autorisera un processus plus lent, mais plus sécurisé.

3 • Lancez le fichier **driver-timeout.reg** et validez plusieurs fois. Attention, nous vous conseillons de faire une sauvegarde de votre registre avant de faire cette manipulation (qui a pourtant fonctionné sur notre machine de test).



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.

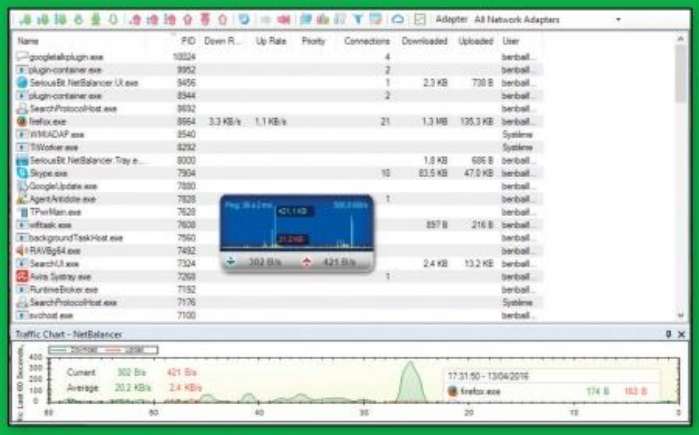
Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

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*.

#1 Limiter la bande passante de vos applications

AVEC NETBALANCER

NetBalancer est un petit logiciel qui va devenir indispensable à tous les «control freak» de la bande passante. Une fois installé, il va non seulement vous afficher toute votre activité réseau (comme GlassWire, voir *Pirate Informatique* n°24), mais il permet aussi de mettre des garde-fous. En cliquant sur l'icône en haut à droite à côté du petit nuage, vous pourrez contrôler la priorité de download/upload de chaque processus. Pratique, pour éviter d'engorger sa bande passante lorsque vous travaillez. Il est possible d'éditer des règles précises, de couper complètement le trafic vers certaines applications: le contrôle total quoi...

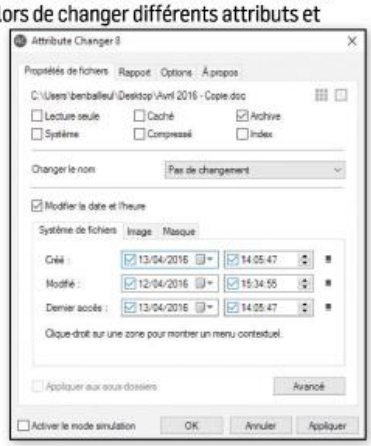


Lien : **https://netbalancer.com**

#2 Trafiquer les métadonnées de vos fichiers

AVEC ATTRIBUTE CHANGER

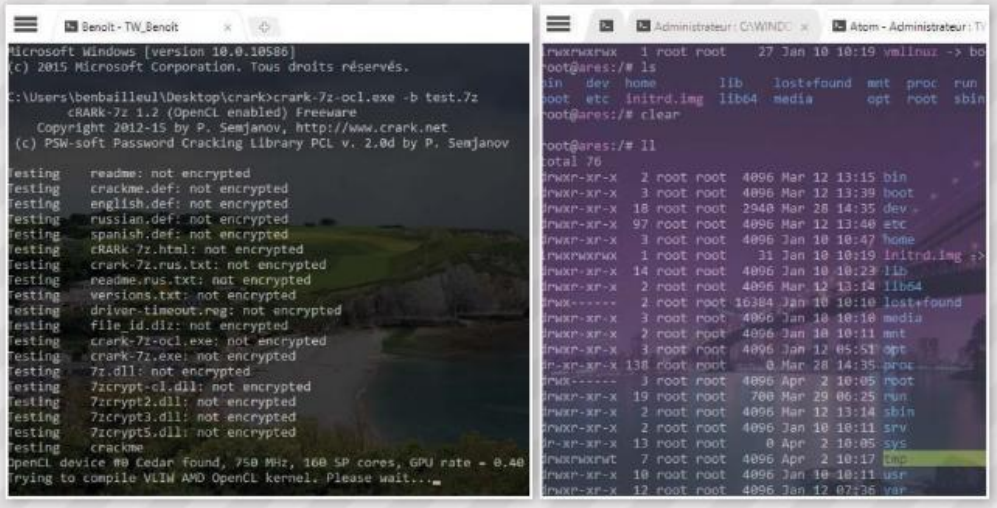
Attribute Changer est un logiciel qui va changer le menu contextuel, lorsque vous faites un clic droit sur un fichier. Vous serez libre alors de changer différents attributs et métadonnées comme l'heure de création ou de modification du fichier (pratique pour rendre un devoir en retard ou changer la date de prise de vue d'une photo). Vous pourrez aussi changer les privilèges comme choisir de mettre un fichier en lecture seule pour éviter que votre famille ne puisse modifier le contenu ou le camoufler comme un fichier caché ou un élément du système. Vous pourrez même garder une trace des modifications pour revenir en arrière en cas de besoin...



Lien : **www.petges.lu**

#3 Remplacer le terminal de Windows

AVEC TERMINAL WINGS



Encore un super logiciel de notre ami J-P Lesueur (voir notre interview page 16)! Terminal Wings va avantageusement remplacer l'invite de commande MS-Dos. Comme précisé dans la description, il ne s'agit pas d'un émulateur, mais d'une sorte de skin de luxe. Au programme : navigation par onglets, code couelri, possibilité d'ajouter un papier peint, d'utiliser un effet de transparence, de créer des profils distincts (apparence, emplacement du shell, commande à exécuter), etc. Attention, pour l'instant le logiciel n'est disponible que pour Windows 10.

Lien : **www.phrozensoft.com**

#4 Identifier et contrer les ransomwares

AVEC ID RANSOMWARE

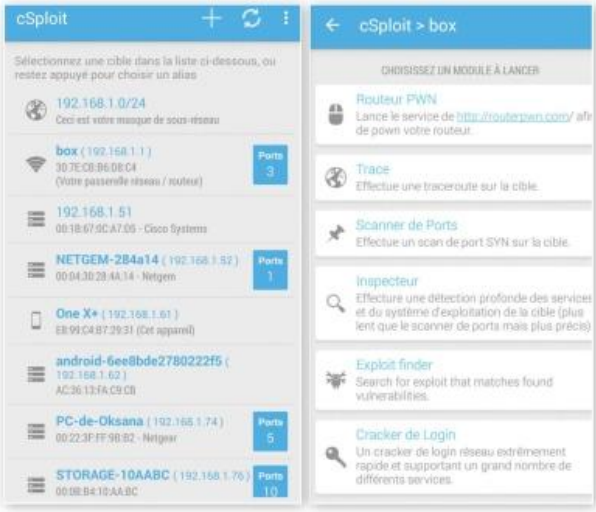
Nous vous avions déjà parlé des ransomwares dans notre numéro 26. Ces malware vont chiffrer vos précieux documents pour ne vous donner la clé qu'une fois que vous aurez payé une somme d'argent. Bien sûr, cela ne fonctionne pas toujours et nous vous déconseillons de payer quoi que ce soit. Si vous n'avez rien trouvé sur Internet, faites un tour sur le site ID Ransomware. Car, en plus de retrouver précisément le nom de votre ransomware à partir des fichiers chiffrés ou de la note vous réclamant le paiement, il vous donnera la solution pour récupérer vos fichiers si cette solution existe. Il arrive en effet que les pirates se prennent les pieds dans le tapis ou se fassent tout simplement arrêter. Dans tous les cas, sauvegarder vos fichiers, vous pourriez trouver une solution plus tard !

Lien : **https://id-ransomware.malwarehunterteam.com**

#5 Du pentesting sur mobile

AVEC CSPLOIT ANDROID

Vous voulez vérifier la sécurité du réseau Wi-Fi d'un ami ? Pas besoin de vous déplacer avec un PC sous Kali Linux puisqu'avec un mobile sous Android et cSploit, vous pourrez lancer toute une batterie de tests : sniffing, sidejacking, crack de mots de passe, scan de ports, manipuler le trafic (ARP poisoning) et réaliser des attaques de type « man-in-the-middle ». Si vous connaissiez dSploit, vous ne serez pas dépaysé avec son successeur. L'interface est légèrement plus agréable et certains menus sont en français. Pour le reste, c'est la même chose avec des mises à jour au niveau des exploits disponibles et des failles connues.



Lien : **http://www.csploit.org**

#6 Tester votre lecteur PDF

AVEC ADOBE PDF EXPLOIT GENERATOR

Si vous avez un parc de vieilles machines disposant de versions d'Adobe Reader et d'Adobe Acrobat jamais mis à jour, ce script Python auto-exécutable va vous permettre de générer vous-même un PDF malicieux exploitant des failles connues de ces logiciels. Bien sûr, vous pouvez aussi les tester sur des alternatives non propriétaires comme Foxit Reader. À n'essayez que sur vos machines hein ?

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

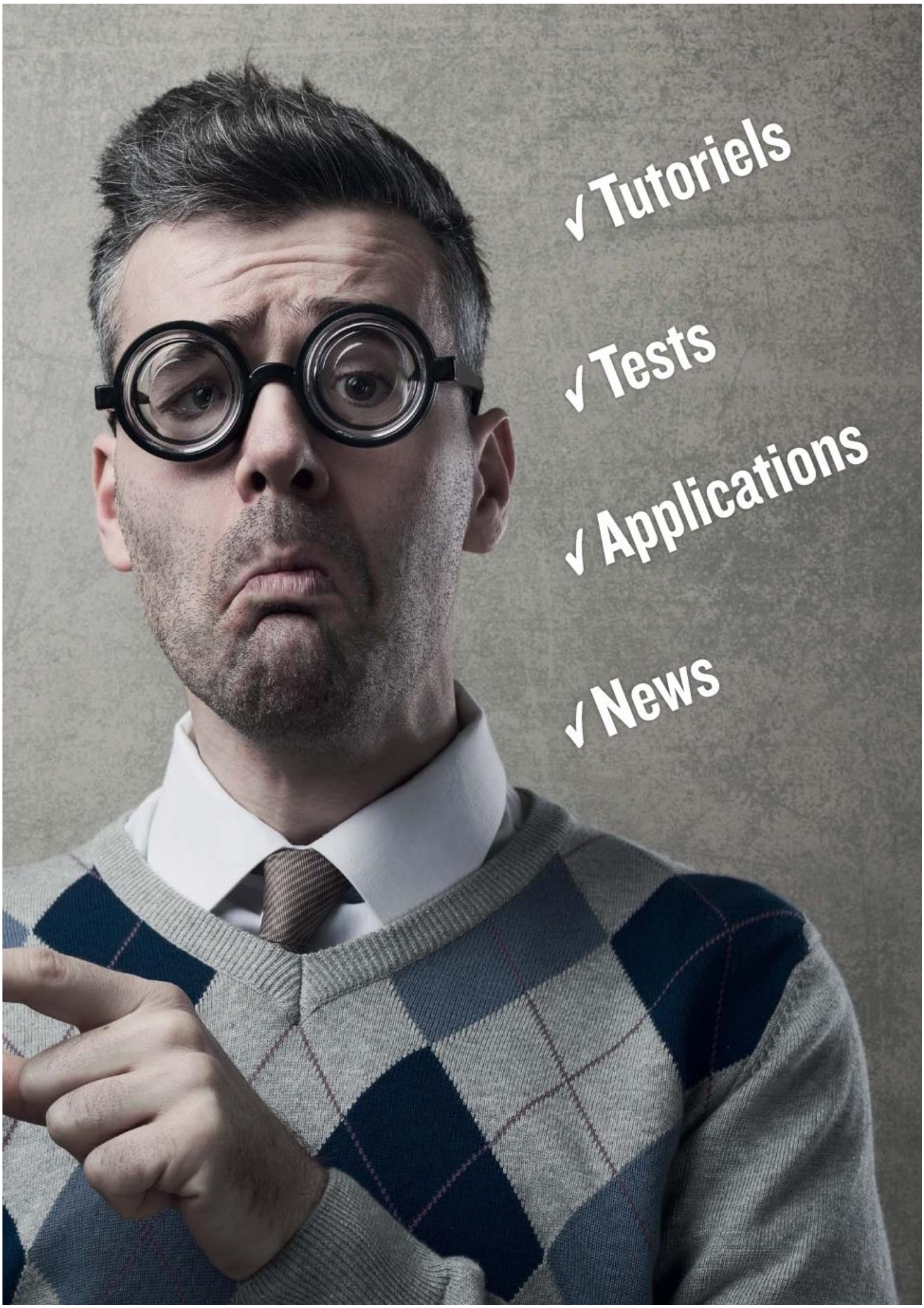
#7 Récupérer des mots de passe

AVEC RAINBOWCRACK

Disponible pour Windows et GNU/Linux, RainbowCrack est un logiciel qui permet de récupérer des mots de passe. Il ne s'agit pas d'attaque brute force ou par dictionnaire, mais d'utiliser des rainbow tables. Pour faire simple, il s'agit de fichiers qui contiennent des précalculs intermédiaires permettant de retrouver rapidement des mots de passe à partir de leurs hash. Comme cRARk (voir page 36), le logiciel utilise les technologies CUDA et OpenCL de nVidia et de AMD/ATI pour tirer profit de la puissance du GPU de votre carte graphique. Si ce sujet vous intéresse, nous pourrons en faire un sujet dans le prochain numéro. Pour trouver des rainbow tables, c'est par ici que ça se passe : **http://project-rainbowcrack.com/table.htm**

Lien : **http://project-rainbowcrack.com**


« Comment je protège mes photos persos ? »
Android-MT.com
SOLUTIONS & ASTUCES


✓Tutoriels
✓Tests
✓Applications
✓News

L'ALLIANCE DU STREAM ET DU P2P

Difficile d'expliquer le concept d'Ace Stream en quelques mots. Il s'agit d'un logiciel permettant de streamer à la fois des films et des séries en utilisant de banals fichiers Torrents mais il concurrence aussi le stream traditionnel et SopCast en ce qui concerne les retransmissions sportives en direct.

LEXIQUE

***STREAMING :**
Technologie qui permet d'écouter de la musique ou de voir une vidéo sans avoir à télécharger de fichier en amont. Lorsque vous regardez YouTube ou écoutez Spotify, vous «streamez».

***BITTORRENT :**
Ensemble de protocoles P2P («peer to peer», de personne à personne) qui permet de télécharger et de partager entre tous les intervenants en utilisant des fichiers .torrent. Ici, il s'agit d'utiliser cette technologie pour imiter la spontanéité du stream.

AceStream a deux visages. Il y a d'abord le plugin Ace Stream P2P qui permet d'afficher du contenu multimédia directement sur son navigateur en utilisant la technologie BitTorrent mais il y a aussi le lecteur multimédia Ace Player, basé sur VLC Media Player, qui autorise la lecture de fichiers multimédias depuis un .torrent ou depuis un lien interactif genre «magnet». Nous laisserons de côté l'aspect navigateur, car non seulement il ne nous a pas convaincus au niveau technique (plantage, arrêt intempestif) mais les services compatibles ne sont pas très intéressants.

ACE PLAYER, LE « SOPCAST-KILLER »

De l'autre côté, le Ace Player nous a agréablement surpris. Ce logiciel concurrence en fait le téléchargement Torrent traditionnel, les nouvelles solutions hybrides comme Popcorn Time (voir *Pirate Informatique n°21*) ou Torrents Time (voir les micro-fiches de cette rubrique) mais aussi le logiciel SopCast ! En effet le logiciel chinois est en nette perte de vitesse par rapport au nouveau venu russe. Il suffit de regarder le nombre de liens distillés sur les sites spécialisés pour se rendre compte que Ace Stream est devenu la référence pour le sport en direct. Son seul inconvénient ? Le fait de «s'inviter» comme logiciel par défaut pour tous vos fichiers.

NOS SITES DE LIENS « SPORTS

LiveTV

Trouvez votre match et cliquez sur les liens Ace Stream les mieux notés. Faites **Montrer tout** en bas pour afficher l'intégralité des liens.

Lien: **http://livetv102.net/fr**

RojaDirecta

Trouvez votre match et cliquez sur les liens Ace Stream. Si vous voyez **(web)** à côté c'est qu'il s'agit sans doute d'un lien ArenaVision. En bas à droite, cliquez sur **Clickaqui** pour ouvrir le player.

Lien: **www.rojadirecta.me**

PAS À PAS

Les deux facettes d'Ace Player

CE QU'IL VOUS FAUT

ACE STREAM MEDIA

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

DIFFICULTÉ :

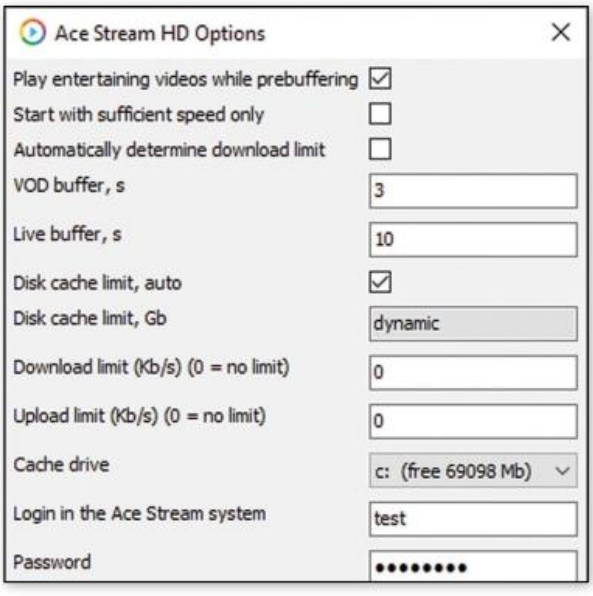
01 L'INSTALLATION

Commençons par télécharger Ace Stream Media (sur la gauche) en choisissant la version de VLC qui vous convient. Ce «pack» installera le player ainsi que les plugins pour vos navigateurs (n'oubliez pas de les fermer). Vous serez d'ailleurs dirigé vers une

page permettant de tester la bonne intégration. Ici c'est un peu la loterie: ça fonctionne ou pas. Si regarder des vidéos en Torrent depuis votre navigateur vous intéresse, essayez avec un autre butineur...

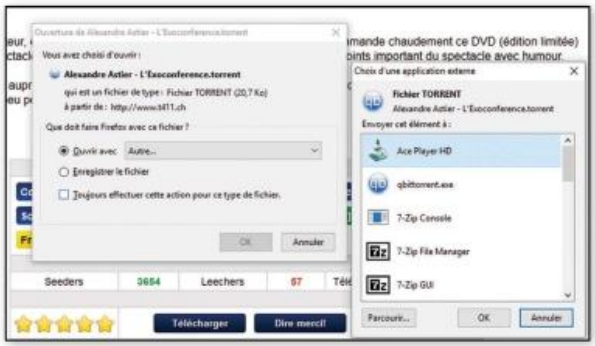
02 LES OPTIONS

Le player est similaire à VLC Media Player et il va se configurer comme l'application par défaut pour tous vos fichiers multimédias. Pour remédier à ce problème, dans Windows 10 allez dans **Paramètres**>**Système**>**Application par défaut**. Vous trouverez aussi des options dans la zone de notification (en bas à droite près de l'horloge): contrôle de la bande passante, mémoire cache, etc. Si vous vous êtes enregistré, c'est ici qu'il faudra mettre vos identifiants. Ne touchez à rien si vous n'êtes pas à l'aise.



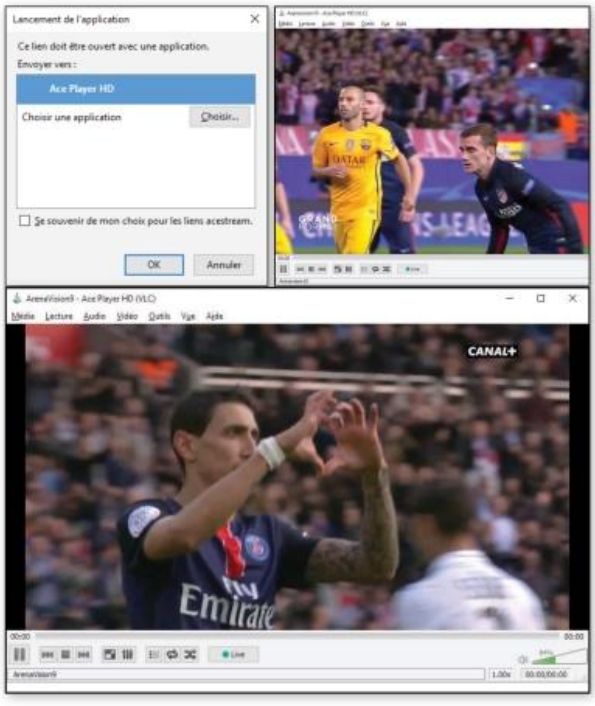
03 CINÉMA...

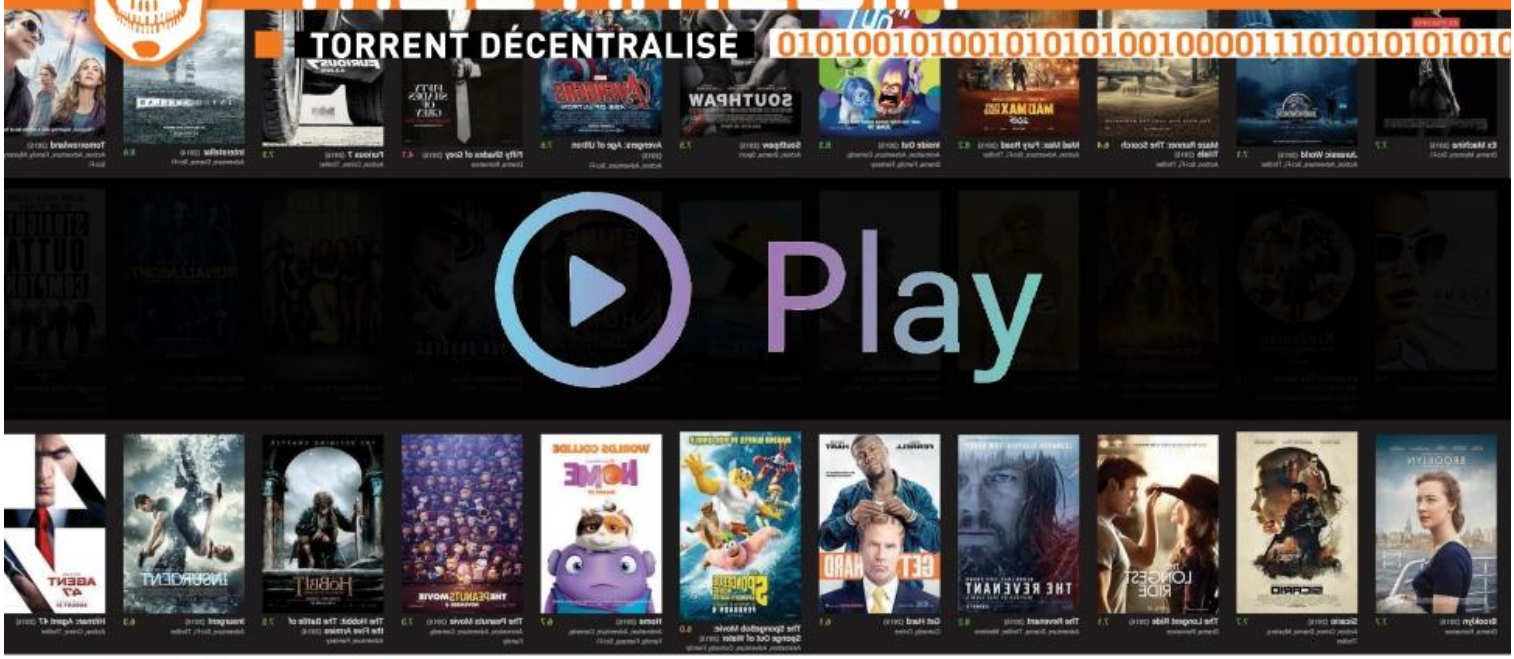
Dorénavant, lorsque vous lancerez un magnet ou un .torrent, Ace Player prendra le relais. Il faudra parfois choisir le programme de lancement via une fenêtre Windows. En fonction de la santé du Torrent, votre film/série/album se lancera après quelques secondes.



04 ...OU SPORTS EN DIRECT

Pour le sport c'est encore plus simple! Il suffit de choisir son match (voir notre encadré) et de lancer le lien. La qualité fera tomber de l'armoire ceux qui sont habitués au «stream traditionnel». Notez que, comme SopCast, Ace Stream est aussi disponible pour mobile Android. Si vous avez un media center équipé de ce système, vous pourrez donc voir vos matchs sur la télé.

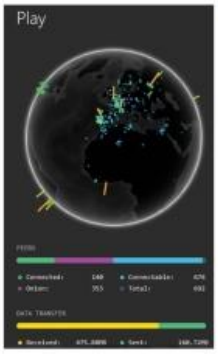




PLAY : LE TORRENT INVINCIBLE

Cela fait des années que les ayants droit font la guerre aux sites Torrent. Entre les menaces d'HADOPI, les blocages de sites ou les procès, le jeu du chat et de la souris ne fait que commencer. Adossé au réseau ZeroNet, Play propose un tracker Torrent indestructible. Explications...

À la page 12 de ce magazine, nous vous avons parlé de ZeroNet, un darknet décentralisé et anonyme permettant d'envoyer des messages ou de créer des sites sans utiliser de serveur. L'avantage de ZeroNet, c'est qu'un site accessible par ce biais n'est pas censurable et que personne ne peut savoir qui fait quoi. En utilisant les propriétés spéciales de ce réseau, des petits malins ont crée Play. Il s'agit d'un site utilisant ZeroNet (il faudra absolument être connecté à ZeroNet pour y accéder) qui fait office de tracker Torrent. Sur la page principale, on trouve les derniers films du moment. Le site est inattaquable et inblocable.



En tirant vers la gauche l'icône 0 en haut à droite, vous aurez accès aux statistiques de Play: nombres de peer, ratio, type de fichiers échangés, etc.

CHAQUE PARTICIPANT HÉBERGE LE SITE...

Ce que nous avons dernièrement connu avec les déménagements de T411 ou la guerre contre The Pirate Bay ne risque pas d'arriver à Play puisque chaque participant «seede» lui-même le site. Impossible de truquer les DNS, de menacer l'hébergeur ou de demander aux FAI de bloquer l'accès. Attention, comme les téléchargements se font via votre client Torrent, vous êtes anonyme quand vous êtes sur le site, mais pas lorsque vous téléchargez, même avec Tor d'activé par défaut. Certes, sur ZeroNet les sites sont limités à quelques Mo, mais quand ce que Play propose relève du tour de force : des centaines de liens magnet vers des fichiers en bonne santé ! Bien sûr, Play propose du contenu illégal, mais il s'agit avant tout d'une expérience pour démontrer que le modèle centralisé est peut-être dépassé...

LEXIQUE

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

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

***SEED :**
«Graine» dans la langue d'Axl Rose. Dans un réseau BitTorrent, un seed est un intervenant qui dispose de l'intégralité d'un fichier et qui le partage. On dit qu'il «seede». Dans Zeronet, on seede les sites, les forums, etc.

PAS À PAS

Play avec ZeroNet

CE QU'IL VOUS FAUT

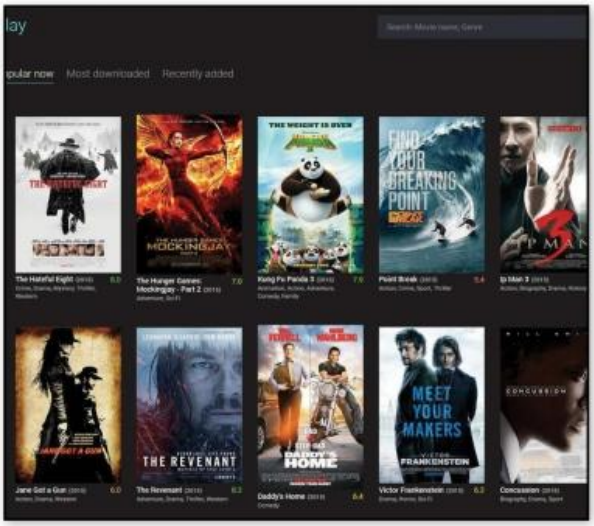
ZERONET
OÙ LE TROUVER ? : **https://zeronet.io**

PLAY
OÙ LE TROUVER ? : **http://tinyurl.com/ztb3v2f** (ZeroNet requis)
DIFFICULTÉ :

01 PLAY AVEC ZERONET

Même si vous n'avez pas lu notre article page 12, vous allez pouvoir utiliser Play. À l'inverse des autres services de ZeroNet, vous n'êtes pas obligé de vous créer un identifiant Zeroid. bit. Téléchargez ZeroNet, démarrez le service (double cliquez dans le fichier **.cmd**) et dirigez-vous vers le lien que nous vous fournissons. Si ce dernier est mort, faites une recherche sur Google ou demandez-le-nous !

02 L'INTERFACE DE PLAY



Vous serez dirigé vers un site très joli (certains trackers pourraient en prendre de la graine) avec plein d'affiches de films. Vous pourrez naviguer entre les films les plus populaires (**Popular now**), ceux qui ont été les plus téléchargés (**Most downloaded**) et ceux qui ont été ajoutés récemment (**Recently added**). Vous pouvez aussi chercher avec un mot clé.

03 LE TÉLÉCHARGEMENT

En cliquant sur une affiche, vous aurez parfois le choix entre plusieurs versions ou qualités. Cliquez sur ce qui vous convient et vous déclencherez l'ouverture de votre client Torrent. Attention, à moins de faire transiter l'intégralité de votre trafic via un VPN, vous ne serez plus anonyme à partir de ce moment. La rapidité de téléchargement est plus lente que d'habitude, mais très correcte (avec notre connexion des pointes à 400ko/s au lieu de 1,2Mo/s).

04 DES SOUS-TITRES POUR VOS FICHIERS

Bien sûr, même si on compte quelques films français, l'anglais est à l'honneur. Parfois des sous-titres (en anglais aussi) seront inclus avec le fichier vidéo, mais si vous désirez des sous-titres français au format **.sub**, **.srt** ou autres, il faudra allez sur **www.opensubtitles.org**. Vous trouverez forcément votre bonheur. Pour la lecture, choisissez VLC Media Player et allez dans le menu **Sous-titres** après avoir lancé votre vidéo.

#1 Streamez des Torrents

avec Torrents Time

Si vous nous lisez depuis un certain temps, vous connaissez sans doute PopCorn Time et ses clones. Ces logiciels ou applis pour mobile permettent de regarder les derniers films et séries sur son appareil préféré en utilisant le meilleur du stream et du P2P. Ce système fait des émules avec l'arrivée de Torrents Time, un programme qui va utiliser les Torrents sains de certains sites pour afficher la vidéo dans le navigateur. Ce qui aurait pu passer pour une initiative confidentielle est sur le point de connaître un essor sans précédent puisque le célèbre annuaire The Pirate Bay (TPB) a lui-même décidé de rendre compatible son service avec Torrents Time! Une fois installé sur votre PC, votre navigateur affichera un bouton **Stream It** à côté du choix entre télécharger le Torrent et le magnet. La plupart des navigateurs sont compatibles bien sûr. Si TPB est inaccessible sur votre navigateur c'est que le site est banni par la plupart des FAI français. Pour en profiter il faudra passer par un proxy ou, plus simple, changer de DNS (voir notre article sur OpenNIC dans le n° 27 de *Pirate Informatique*)

Lien: **https://torrents-time.com ; : https://thepiratebay.se**

#2 Convertir des images depuis le menu contextuel

avec SendTo-Convert

Vous manipulez des photos, des GIF animés, des logos ou des images pour votre site? Au lieu de lancer votre logiciel de retouches/conversions à chaque fois que vous voulez faire une manipulation, pourquoi ne pas faire confiance à SendTo-Convert? Ce logiciel va ajouter une entrée au menu contextuel **clic droit>Envoyez vers** pour pouvoir convertir, mais aussi redimensionner, garder la transparence, ajuster en fonction d'un ratio, etc. Seuls les formats vectoriels ne sont pas pris en compte. Suivez notre lien, regardez tout en bas de la page et choisissez la version en fonction de votre système (32 ou 64 bits).

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

#3 Enregistrez vos morceaux favoris

avec YouTube-mp3.org

Si vous n'êtes pas trop «stream», YouTube-mp3.org permet de télécharger le son d'une vidéo YouTube. Idéal pour enregistrer des morceaux introuvables, des concerts entiers, des spectacles comiques ou garder la piste sonore d'un documentaire pour s'en faire un podcast. Pas besoin de créer un compte, la seule chose qu'il vous faut est l'adresse URL d'une vidéo YouTube. La conversion est lancée dès que vous nous soumettez l'adresse de la vidéo, ensuite il vous suffira de télécharger le MP3. Les services de ce type sont légion, mais ce dernier ne comprend pas de pubs et reste très rapide...

Lien: **http://www.youtube-mp3.org**

#4 Des jeux sur navigateur

avec WebGL Games & Unity Web player

Il est bien loin le temps des jeux Flash ridicules en mode fenêtré, pixélisés et injouables. Maintenant les jeux sur navigateurs sont en 3D et proposent autant de productions originales que de clones de succès d'antan. Pour en profiter il suffit de télécharger le plugin Unity Web Player et de faire son choix sur un site comme WebGLgames.com. Ce site propose en effet une sélection de jeux fort sympathiques qui utilisent la techno WebGL issue du HTML5. Au programme: FPS, jeux d'arcade, de courses, de stratégie. Nos préférés: *Dead Trigger 2*, *HexGL* et *Circle Game*.

Lien: **www.webglgames.com ;**
Lien: **https://unity3d.com/webplayer**

#5 De la VoIP sans prises de tête

AVEC GRUVEO

Compatible avec la plupart des navigateurs du marché et fonctionnant sur n'importe quel système capable d'afficher une page Web, Gruveo est une solution de VoIP simple et efficace. Grâce au protocole WebRTC vous aller pouvoir converser avec la personne de votre choix en lui communiquant juste un code que vous aurez défini sur la page du service. La qualité est au rendez-vous et comme il n'y a rien à installer, c'est le bonheur. Côté chiffrement c'est très léger (SSL) mais suffisant pour éviter de se faire espionner par kévindu75 en mode script kiddie...

Lien: **www.gruveo.com**

Merci à LOrdKiki2Nazareth!

#6 Le Spotify du pauvre

AVEC TUBEATS

Depuis la déliquescence de GrooveShark nous n'avions pas encore eu l'occasion de trouver une plate-forme de stream gratuite, légale et sans pub. C'est chose faite avec Tubeats qui va piocher les morceaux dans le répertoire de YouTube ou d'autres plates-formes vidéos. Si vous vous inscrivez, vous pouvez vous confectionner des

playlists. Si vous ne savez pas quoi écouter, le site propose les tubes du moment ou des morceaux en accord avec vos goûts. Il est même possible d'avoir le clip en miniature lorsqu'il est disponible. À essayer!

Lien: **http://tubeats.com**

#7 Des filtres et retouches photo

AVEC GOOGLE NIK COLLECTION

En 2012, Google a acheté la société Nik Software, éditrice de logiciels de retouche photo. Alors qu'avant, le pack complet des programmes de cette compagnie coûtait la modique somme de 500 dollars, en 2016 Google l'a rendu gratuit! Bien sûr si c'est Google et que c'est gratuit on peut s'attendre à des petites surprises au niveau de la licence d'utilisation, mais rien de plus grave que d'habitude (Conditions d'utilisation de Google du 14 avril 2014). Attention, ces programmes ne sont pas autonomes et doivent fonctionner avec Photoshop, Photoshop Elements ou Photoshop Lightroom. Parmi ces 7 programmes, on compte Color Efex Pro (filtres en tous genres), HDR Efex Pro (pour réaliser des photos en grande plage dynamique), Dfine pour la réduction du brut et divers autres softs pour la correction des couleurs, les photos en noir & blanc, etc. L'accélération GPU est de la partie avec les cartes graphiques récentes.

Lien: **www.google.com/nikcollection**

X-MATÉRIELS

> Raspberry Pi 3, LE RETOUR DE LA REVANCHE

Si vous lisez fréquemment *Pirate Informatique*, vous savez que nous parlons souvent du Rapsberry Pi dans nos colonnes. Ce micro-ordinateur, créé par la fondation de David Braben dans le but d'encourager l'apprentissage de l'informatique aux personnes avec peu de moyens ou dans les pays en voie de développement, est devenu objet tendance et même culte chez certains bidouilleurs. PC d'appoint pour certains, carte programmable pour d'autres, le Raspberry Pi est plein de surprises et cette version 3 ajoute encore

COMPARATIF DES DEUX DERNIERS MODÈLES DE RASPBERRY PI

	Raspberry Pi 2	Raspberry Pi 3
Date de sortie	Février 2015	Février 2016
Chipset	ARMv7 (4 cœurs)	ARM v8 Cortex-A53 (4 cœurs 64 bits)
Horloge	900 MHz	1200 MHz
RAM	1 Go	1 Go
Type de mémoire	DDR2 400 MHz	LPDDR2 400 MHz
Stockage	Carte MicroSD	Carte MicroSD
Ports USB	4	4 avec la possibilité d'alimenter des périphériques plus puissants
Wi-Fi	Non	Oui
Bluetooth	Non	Oui (v4.1 + Low Energy)

des améliorations. Mais, la grosse nouveauté de cette nouvelle mouture est l'ajout de modules Bluetooth et Wi-Fi. Soulignons que de nombreuses distributions Linux permettent de faire ce qu'on veut avec la machine : un PC tout terrain (Raspbian voir page suivante), un media center (OpenELEC), du retogaming (PiPlay et Retropie) ou un NAS (ownCloud). Bien sûr, les anciens périphériques sont compatibles avec cette version 3, y compris les HAT, ces fameux add-on permettant d'ajouter des fonctions pour la domotique ou la robotique (GPS, capteur de mouvement, servi moteur, etc.) Retrouvez sur notre CD nos précédents articles et démonstrations sur cette bécane magique !

Prix : **46 €** **www.raspberrypi.org**

Lindy 40454, POUR SÉCURISER VOS PORTS USB

Voici un petit appareil astucieux permettant à un utilisateur d'être absolument sûr que ses ports USB ne soient pas utilisés dans son dos. Il s'agit d'un simple dongle qui insérera une sorte de bouchon de plastique à l'intérieur des ports USB. Bien sûr, cela empêchera un tiers de connecter quoi que ce soit. Quatre bouchons de plastique sont livrés avec le dongle et il vous faudra bien sûr ce dernier pour les retirer et rendre vos ports-USB à nouveau opérationnels.

Prix : **30 €** **http://goo.gl/29CJXt**

Archos PC Stick, UN PC À BRANCHER !

Avec ses dimensions réduites (113 x 37,6 x 14 mm) et son poids de 60 grammes, il est difficile de croire que nous avons affaire à un PC ! Équipé d'un processeur Intel Atom Z3735F cadencé à 1,3 Ghz, de 2 Go de RAM, d'un slot Micro SD pour le stockage et d'un port USB, l'Archos PC Stick est un ordinateur sous Windows 10 à brancher sur un téléviseur ou n'importe quel écran disposant d'un port HDMI. Pilotable en Bluetooth depuis une tablette, l'appareil est aussi silencieux puisque ne comptant pas de ventilateur. Le bémol se situe autour de la réactivité de l'appareil. Pour surfer ou afficher une présentation PowerPoint, ça va, mais n'espérez pas lancer Photoshop ! Pourquoi avoir choisi d'intégrer Windows 10 et pas un OS moins gourmand ? Il est néanmoins possible de régler le système pour éviter les effets de manches superflus. Une sacrée prouesse technique tout de même...

Prix : **100 €**

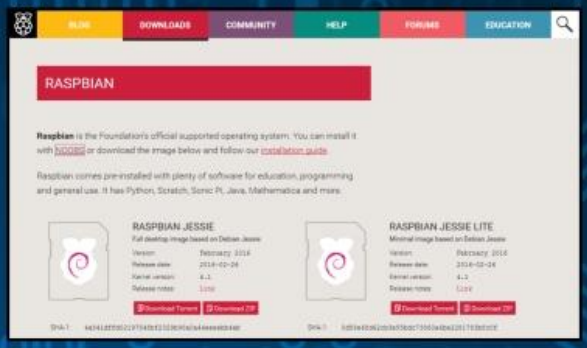
www.archos.com

NOTRE TEST EXCLUSIF

Raspberry Pi 3, les premiers pas avec Raspbian

Avec notre partenaire KUBII www.kubii.fr

Il est assez difficile de choisir par quoi commencer lorsqu'on présente un appareil comme le Raspberry Pi. Nous avons donc décidé de vous montrer le système officiel de la machine : Raspbian. Cette version spéciale de la distribution GNU/Linux Debian est idéale pour ce nano-PC, car elle intègre tout ce qu'il faut pour en faire un PC complet...



#1 TÉLÉCHARGEMENT DE L'IMAGE

Commençons par télécharger l'image de Raspbian «Jessie» et par dézipper l'archive avec l'explorateur ou 7-Zip. Vous devriez vous retrouver avec un fichier au format **.img**. Pour mettre le contenu de cette dernière dans la carte, il faudra utiliser le logiciel Win32 Disk Imager. Lancez-le, sélectionnez **2016-xx-xx-rasbian-jessie.img** avec l'icône en forme de dossier puis spécifiez l'emplacement de la carte SD (au moins 8Go) dans la colonne **Device**. Faites **Write** et attendez la fin du processus.

#2 BRANCHEMENT ET LANCEMENT

Il est temps de brancher le Raspberry Pi sur l'écran via les ports HDMI ou RCA. Branchez aussi le clavier et la souris sur les ports USB. Une fois que l'alimentation est branchée (celle d'un téléphone portable fera l'affaire), Raspbian va démarrer. L'interface graphique devrait se lancer automatiquement. On vous demandera peut-être aussi de vous identifier. L'identifiant (login) est **pi** et le mot de passe est **raspberry**. Attention, car le sésame ne sera pas affiché lors de la frappe et n'oubliez pas que le clavier est réglé en QWERTY par défaut.

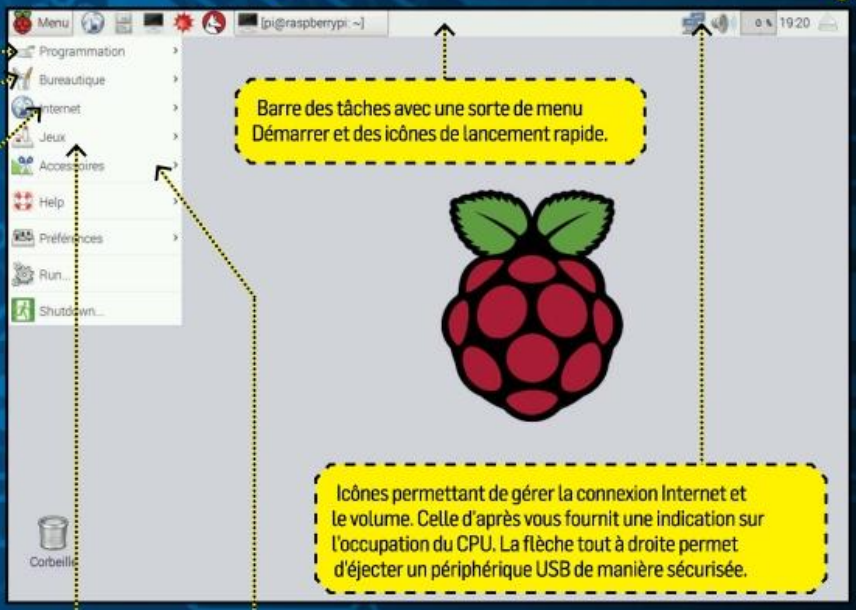
#3 PREMIER CONTACT

Dans **Programmation**, on trouve Java, Python, mais aussi le logiciel de calculs algébriques Mathematica. Scratch est destiné à apprendre la programmation aux enfants tandis que Sonic Pi permet de coder...de la musique ! Ce logiciel permet de coder en live pour des événements musicaux. Une autre manière de faire de la musique...

Bureautique propose tout simplement la suite LibreOffice avec un tableur, un éditeur de texte type Word, un logiciel de dessin, de formules mathématiques, etc.

Pas de surprise dans **Internet** : le navigateur Epiphany et le client de messagerie Claws Mail...

Dans **Jeux**, vous trouverez la version Raspberry Pi de Minecraft complètement gratuite et des petites réalisations sous Python.



Barre des tâches avec une sorte de menu Démarrer et des icônes de lancement rapide.

Icônes permettant de gérer la connexion Internet et le volume. Celle d'après vous fournit une indication sur l'occupation du CPU. La flèche tout à droite permet d'éjecter un périphérique USB de manière sécurisée.

Accessoires rassemble les programmes basiques intégrés à l'environnement de bureau LXDE : calculatrice, terminal pour les lignes de commandes, gestionnaire des tâches, lecteur PDF, gestion d'archives, etc.

LE GUIDE PRATIQUE

100%

MICRO-FICHES, TRUCS & ASTUCES

SUR NOTRE CD :

Les meilleurs logiciels et services de pros OFFERTS

Armitage

Torrent

BIG BROTHER

CRACK

DARKNET

Windows

ATTAQUE

IDPRESSE

L 12730 - 29 - 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