100% PRATIQUE

La trousse à outils du hacker

LE GUIDE ULTIME 2019

LES DOSSIERS DU Pirate

3,50€ seulement

SOLUTIONS 100 % GRATUITES… ET PROS!

0% PUBLICITÉ

BEST-OF

80 LOGICIELS & SERVICES HACKING

+ ANONYMAT & PROTECTION

GRATUITS!

+ TUTOS & ASTUCES

EN - DE 5 MN CHRONO !

SOMMAIRE

EN PARTENARIAT AVEC LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

PROTECTION

p8
Antivirus et **ANTIMALWARE**

p12
Nos **OUTILS** complémentaires

p16
ANALYSER votre **SYSTÈME** en profondeur

p18
Protégez-vous des **RANSOMWARES**

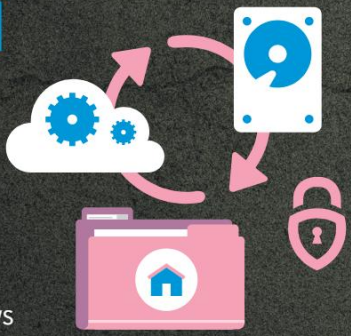
p22
De **NOUVELLES SOLUTIONS** pour de nouveaux problèmes

SAUVEGARDE

p30
Avira **PASSWORD** Manager

p32
7 LIVE CD au secours de votre PC

p38
Comment **SAUVEGARDER** Windows



BONUS p88

Émulation console ou PC, le jeu dans tous ses états

HACKING

p44
Récupérez tous vos **SÉSAMES**

p50
Sécurisez votre **WIFI**

p54
Prenez le **CONTRÔLE** !

p60
Tout sur les « **HASH** »

p63
BIDOUILLEZ votre Windows

ANONYMAT & VIE PRIVÉE

p68
Chiffrez vos **DONNÉES**

p72
PROTÉGEZ vos **DONNÉES** locales

p78
PROTÉGEZ votre vie privée avec un **VPN**

LES DOSSIERS DU **Pirate**

N°21 - Octobre – Décembre 2019

Une publication du groupe ID Presse.
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme

Kenshiro : Benoît Bailleul

Rei & Lui : Kevin Dachez, Aude Boireau

Lynn & Bart : Stéphanie Compain & Sergueï Afanasiuk

Correctrice :
Marie-Line Bailleul

Imprimé en France par / Printed in France by :

Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 2267-6295

«Pirate» est édité par SARL ID Presse, RCS : Aix-en-Provence 491 497 665
Parution : 4 numéros par an.

THE JOKER, LE MALWARE QUI RIT À LA FACE DES UTILISATEURS ANDROID

L'expert en sécurité Aleksejs Kuprins a découvert un nouveau malware dévastateur : THE JOKER. Ce virus, qui sévit sur les smartphones Android, extorque de l'argent aux utilisateurs en souscrivant à des abonnements premiums à leur insu. Le logiciel malveillant a été détecté dans une vingtaine d'applications disponibles sur le Play Store, parmi Great VPN ou Rapid Face Scanner. À elles seules, ces apps comptabilisaient plus de 500 000 téléchargements. Entre temps, Google a fait le ménage en retirant toutes les applis vérolées. Mais entre nous, THE JOKER ne meurt jamais n'est-ce pas Batou ?

UN FRANÇAIS INTERPELLÉ POUR UNE CYBERARNAQUE DE GRANDE AMPLEUR

28 000 victimes et 2000 plaintes déposées. Voilà le bilan de ce jeune escroc français, arrêté début septembre. L'homme est suspecté d'avoir élaboré une vaste opération de "sextorsion" sur internet. Comme l'explique Jérome Notin, directeur général de la plateforme Cybermalveillance.gouv.fr, *"il leur faisait croire qu'il les avait filmés en train de visionner des vidéos pornographiques. C'était évidemment faux, mais si les victimes avaient fréquenté un site pornographique dans les jours qui précédaient, elles s'inquiétaient forcément"*. À force de chantage, le délinquant aurait réussi à amasser près de 20 000 euros. Somme dont il ne pourra pas profiter tout de suite.

LES ATTAQUES VIA ANSOMWARES :

les mots de passes faibles, le principal danger

Les chercheurs en cybersécurité de F-Secure viennent de délivrer un rapport détaillé sur l'activité cybercriminelle durant le premier semestre 2019. Selon ce document, l'attaque par force brute est la méthode préférée des pirates, représentant ainsi 31% des agressions par ransomware. Cette technique consiste à bombarder un serveur ou un point d'accès avec une infinité de mots de passe jusqu'à tomber sur le bon. Évidemment, des bots se chargent de créer et proposer toutes les combinaisons possibles. *"Tout simplement, les attaques par force brute sont le premier choix des hackers parce qu'elles fonctionnent, nous constatons qu'il y a une abondance de comptes qui ont beaucoup trop de mots de passe peu sécurisés et faibles - ce qui rend leur contournement trop facile pour les pirates"*, explique Jardon Niemela, chercheur principal chez F-Secure.

Edward Snowden demande (encore) l'asile à la France

L'ex-ennemi public numéro 1 des USA et lanceur d'alerte a réitéré sa demande d'asile auprès de l'État français. Sa première tentative avait été refusée par l'administration Hollande. L'ancien agent de la NSA s'est exprimé au cours d'une interview pour France Inter, où il a essayé de plaider sa cause. *"On ne veut pas que la France devienne comme ces pays que vous n'aimez pas. Le plus triste dans toute cette histoire, c'est que le seul endroit où un lanceur d'alerte américain a la possibilité de parler, ce n'est pas en Europe, mais c'est ici (*en Russie, NDLR). *Ce n'est pas seulement la France qui est en question, c'est le monde occidental, c'est le système dans lequel on vit. Protéger les lanceurs d'alerte, ça n'a rien d'hostile"*, assure-t-il.

Le nouveau site des utilisateurs ANDROID

- Des dizaines de tutoriels et dossiers pratiques
- Mobiles & Tablettes : des tests complets !
- Sélection des meilleures applis + des vidéos et du fun !

Android MT

Solutions & Astuces

www.android-mt.com

NOUVEAU SITE !

PROTECTION

p8
Antivirus et **ANTIMALWARE**

p12
Nos **OUTILS** complémentaires

p16
ANALYSER votre **SYSTÈME** en profondeur

p18
Protégez-vous des **RANSOMWARES**

p22
De **NOUVELLES SOLUTIONS** pour de nouveaux problèmes

ANTIVIRUS ET ANTIMALWARES

Unshorten.me → Vérifier une URL raccourcie

Très pratiques sur les réseaux sociaux, comme Twitter avec sa limite de caractères, ou simplement pour éviter d'envoyer des liens à rallonge, les raccourcisseurs d'URL (goo.gl, tinyurl.com, bit.ly...) sont malheureusement quelquefois utilisés pour nuire. Si la source est suspecte ou simplement inconnue, mieux vaut se méfier: utilisez Unshorten.me pour découvrir ce qui se cache derrière une URL raccourcie.

Lien : **https://unshorten.me**

No More Ransom !
→ Contre les ransomwares

Le site à consulter si vous êtes victime d'un rançongiciel, un de ces logiciels malfaisants qui chiffrent vos données et exigent une rançon pour vous donner la clé. On y trouve tout ce qu'il faut savoir sur ces malwares au niveau de la prévention, un service de détection en ligne (pour savoir de quel mal vous avez hérité) et plusieurs outils de déchiffrement, accompagnés de guides d'utilisation.

Lien : **www.nomoreransom.org**

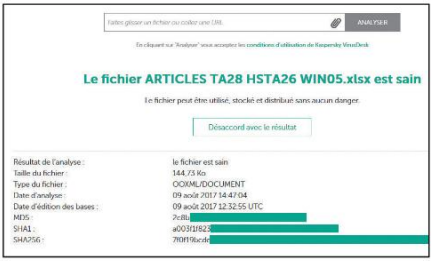
Kaspersky VirusDesk
→ En cas de doute

Kaspersky, célèbre éditeur d'antivirus, propose un service Web qui vous permet de vérifier qu'un fichier ou un lien Internet est sans risque pour votre PC. Pour les fichiers, le logiciel antivirus maison est exploité. Pour les sites Internet, VirusDesk utilise la base de données de réputation Kaspersky Security Network.

Lien : **https://virusdesk.kaspersky.fr**

VÉRIFIEZ FICHIERS ET SITES DOUTEUX AVEC KASPERSKY VIRUSDESK

TUTO



01› ANALYSER UN FICHIER

Faites glisser le fichier suspect dans le champ prévu à cet effet (vous pouvez aussi cliquer sur le trombone pour parcourir la machine). Cliquez sur **Analyser** et attendez le résultat. Attention, certains bloqueurs de publicités peuvent empêcher le fonctionnement de l'analyse.

02› ANALYSER UN LIEN

Collez le lien Web dans le champ et validez avec **Analyser**. Kaspersky compare l'adresse avec sa base de données pour définir si le lien est sans danger ou non. En cas d'erreur, cliquez sur **Désaccord avec le résultat** et suivez la procédure de signalement.

CONTRÔLEZ LES URL RACCOURCIES AVEC UNSHORTEN.ME

TUTO

01› TAPER L'URL

Tapez ou copiez l'adresse raccourci dans le champ prévu à cet effet, sur la page d'accueil d'unshorten.me (une copie est préférable, elle évite les erreurs ou les confusions). Puis cliquez sur le bouton **Un-Shorten**.

02› VÉRIFIER LE LIEN

Le site déchiffre l'URL et affiche une miniature de la page correspondante. Vous pouvez vous rendre directement dessus (bouton **Visit Website**), ou consulter d'abord son score de fiabilité (**Internet Safety User Score**) s'il ne vous inspire pas confiance.

VirusTotal → Plusieurs antivirus en un

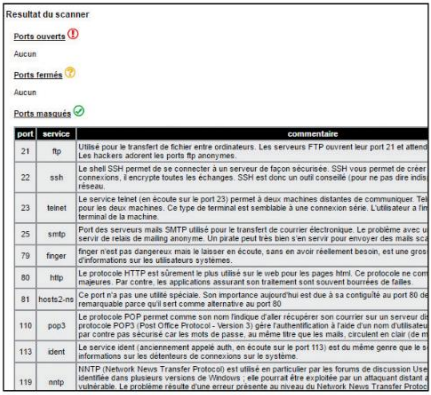
Vous recevez un fichier suspect, ou un lien vers un site que vous ne connaissez pas? Sans être paranoïaque, peut-être qu'il s'agit d'un fichier ou d'une URL infecté(e). Pour en avoir le cœur net, passez-le au crible avec VirusTotal. Ce service met à contribution plusieursantivirus différents pour vérifier que les fichiers que vous lui soumettez ne sont pas infectés.

Lien : **www.virustotal.com**

ID Ransomware → En désespoir de cause

Vous êtes victime d'un ransomware et le service No More Ransom (page précédente) ne vous a pas tiré d'affaire? Avant de payer pour obtenir la clé de déverrouillage de vos données (et encore, ce n'est pas garanti!), essayez ID Ransomware. Via ce site, vous identifiez le coupable en téléversant un des fichiers cryptés. Le site vous souffle une solution pour récupérer vos données. Si elle existe...

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


Resultat du scanner

Ports ouverts

Aucun

Ports fermés

Aucun

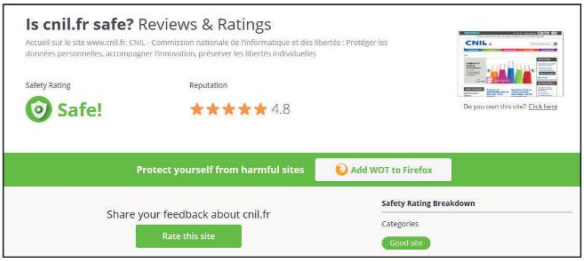
Ports masqués

port	service	commentaire
21	ftp	Utilisé pour le transfert de fichier entre ordinateurs. Les serveurs FTP ouvrent leur port 21 et attend Les hackers adorent les ports ftp anonymes.
22	ssh	Le shell SSH permet de se connecter à un serveur de façon sécurisée. SSH vous permet de créer connexions, il encrypte toutes les échanges. SSH est donc un outil conseillé (pour ne pas dire indis réseau.
23	telnet	Le service telnet (en écoute sur le port 23) permet à deux machines distantes de communiquer. Tel pour les deux machines. Ce type de terminal est semblable à une connexion série. L'utilisateur a l'in terminal de la machine.
25	smtp	Port des serveurs mails SMTP utilisé pour le transfert de courrier électronique. Le problème avec u servi de relais de mailing anonyme. Un pirate peut très bien s'en servir pour envoyer des mails sca
79	finger	finger n'est pas dangereux mais le laisser en écoute, sans en avoir réellement besoin, est une gros d'informations sur les utilisateurs systèmes.
80	http	Le protocole HTTP est sûrement le plus utilisé sur le web pour les pages html. Ce protocole ne com majeures. Par contre, les applications assurant son traitement sont souvent bourrées de failles.
81	hosts2-ns	Ce port n'a pas une utilité spéciale. Son importance aujourd'hui est due à sa contiguïté au port 80 de remarquable parce qu'il sert comme alternative au port 80.
110	pop3	Le protocole POP permet comme son nom l'indique d'aller récupérer son courrier sur un serveur di protocole POP3 (Post Office Protocol - Version 3) gère l'authentification à l'aide d'un nom d'utilisateu par contre pas sécurisé car les mots de passe, au même titre que les mails, circulent en clair (de m
113	ident	Le service ident (anciennement appelé auth, en écoute sur le port 113) est du même genre que le s informations sur les détenteurs de connexions sur le système.
119	nntp	NNTP (Network News Transfer Protocol) est utilisé en particulier par les forums de discussion Use identifiée dans plusieurs versions de Windows , elle pourrait être exploitée par un attaquant distant vulnérable. Le problème résulte d'une erreur présente au niveau du Network News Transfer Protoc

Inoculer → Scanner les ports du PC

Vous pensiez être totalement protégé, mais vous avez quand même réussi à attraper un virus sur votre PC? La faille est probablement liée à un port laissé ouvert. Depuis le site, cliquez sur **Scanner les ports de mon ordinateur maintenant**. Les ports laissés ouverts sont notés en rouge, à vous de les fermer via votre pare-feu. Notez que le rôle de ce scanner étant de tester la sécurité de votre machine, votre pare-feu peut croire à une attaque. Fausse alerte, vous ne risquez rien.

Lien : **www.inoculer.com/scannerdeports.php**



WOT → Vérifier la fiabilité d'un site

Pour éviter d'attraper des cochonneries, mieux vaut éviter les sites douteux. Mais comment savoir si tel ou tel site ou service est sain ou s'il vaut mieux s'en détourner? En demandant à WOT. Connectez-vous sur le service, et tapez l'adresse du site à évaluer dans le champ situé en haut à droite. Notez que le service peut être installé comme extension dans votre navigateur.

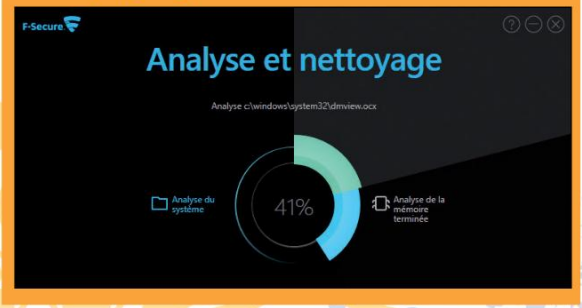
Lien : **www.mywot.com**

F-Secure Online Scanner

→ Antivirus en ligne

Même si nous vous conseillons d'installer un antivirus sur votre PC, cela n'est pas obligatoire pour effectuer une analyse ponctuelle de la machine. L'éditeur d'antivirus F-Secure propose un outil en ligne gratuit pour chercher et éliminer d'éventuels programmes malveillants sur votre ordinateur. Pratique, quand on a un doute.

Lien : **https://goo.gl/5KPNic**



ON AIME AUSSI !

Jotti
> Avis d'experts

Un autre scanner de fichiers en ligne, fonctionnant sur le même principe que VirusTotal: il met à contribution plusieurs services antivirus.

Lien : **https://virusscan.jotti.org/fr**

Secuser
> Vérification complémentaire

Si vous avez besoin d'un scan rapide sur une machine qui ne possède pas d'antivirus, ou d'une analyse complémentaire à celle de votre antivirus.

Lien : **www.secuser.com/antivirus**

ESET Online Scanner
> Analyse par dossier

ESET Online Scanner permet de vérifier si votre ordinateur est infecté par un virus ou un malware. L'avantage est ici de pouvoir cibler un ou plusieurs dossiers.

Lien : **http://goo.gl/oO2bVG**

HouseCall
> En 32 et 64 bits

L'antivirus en ligne de Trend Micro. Attention, on vous demande au préalable d'indiquer votre version de Windows : 32 ou 64-bit.

Lien : **http://housecall.trendmicro.com**

DÉTECTEZ ET ÉLIMINEZ LES VIRUS !

Ralentissements suspects, publicités ou faux messages d'alerte, crash à répétition... Votre PC est peut-être infecté par un virus !

Les symptômes d'une infection sont aussi variés que la nature des malwares (« logiciels malfaisants ») susceptibles de s'introduire sur votre PC, via votre connexion Internet, ou une clé USB elle-même infectée. Cela va de la simple gêne à la destruction de données, en passant par le blocage du PC. La première ligne de défense contre les virus informatiques, c'est vous. Evitez les sites louches, n'ouvrez pas les pièces jointes à des mails d'origine suspecte. La seconde barrière, c'est la protection en temps réel exercée par votre antivirus. Une protection indispensable, mais pas infaillible : un virus peut à l'occasion se glisser entre les mailles du filet. Les pages qui suivent vous expliquent comment analyser votre système en profondeur pour détecter une attaque et la neutraliser, avec votre antivirus d'abord, des utilitaires spécialisés ensuite, voire un CD de secours si Windows ne démarre même plus.

UN ANTIVIRUS C'EST BIEN, MAIS POURQUOI NE PAS PRENDRE DES MESURES SUPPLÉMENTAIRES ?

4 OUTILS COMPLÉMENTAIRES

Même si vous avez un antivirus performant, vous pouvez aussi faire appel à des antimalwares spécialisés dans certains types d'attaque...

Malwarebytes

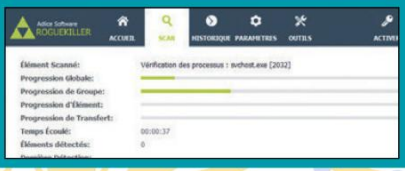
Face à certains virus particulièrement retors, votre antivirus généraliste risque d'être mis en échec. En cas d'infection, et régulièrement à titre préventif, Malwarebytes est une très bonne solution. Le logiciel dispose d'une période d'essai mais la version gratuite est très bonne. Si vous avez un doute sur la bonne tenue d'une désinfection, c'est le programme à utiliser.

Lien : **https://fr.malwarebytes.com**

Roguekiller

Autre grand spécialiste de la chasse aux malwares, RogueKiller complétera utilement votre antivirus. À l'issue de l'examen (assez long), RogueKiller affiche la liste des logiciels indésirables et des anomalies qu'il a détectés, avec un code couleur indiquant leur niveau de dangerosité : rouge, orange, ou gris. Cochez celle en rouge ou orange et cliquez sur **Supprimer sélection**.

Lien : **https://goo.gl/wkTy6a**



Adwcleaner

Les adwares encombrent votre navigateur, détournent vos recherches sur Internet, et affichent des encarts publicitaires dans Windows. Relativement inoffensifs, ils sont souvent ignorés par les antivirus. AdwCleaner les élimine. Faire le ménage. L'analyse effectuée, cliquez sur Nettoyer pour éliminer les adwares détectés. Pensez à enregistrer vos éventuels travaux en cours avant de valider par **OK**.

Lien : **https://goo.gl/Qr2YZ7**

ZHP Cleaner

Vous rencontrez de plus en plus de problèmes avec votre navigateur : affichage de publicité, pop-up, barre de navigation non désirée ? Il s'agit peut-être de redirections d'URL (votre flux Internet passe par un proxy alors que vous n'avez rien demandé) et cela peut ouvrir la porte au phishing, à différents spywares ou pire...un botnet. ZHPCleaner va rétablir les paramètres proxy et supprimer les redirections d'URL sur tous vos navigateurs.

Lien : **www.nicolascoolman.com**

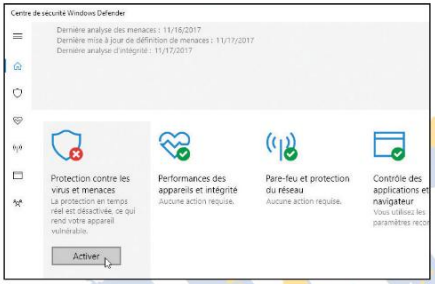
VÉRIFIEZ VOTRE ORDINATEUR

L'antivirus Windows Defender, intégré au système, fait normalement barrage aux virus sans que vous ayez à intervenir. En cas de doute, vous pouvez cependant lancer manuellement une analyse.

INFOS [WINDOWS DEFENDER] Difficulté : ☠☠☠ TUTO

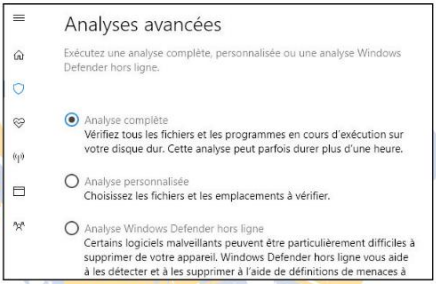
01› OUVRIR WINDOWS DEFENDER

Pour accéder à l'interface de Windows Defender, faites un double-clic sur son icône, à l'extrémité de la barre des tâches (au besoin, cliquez sur la petite flèche verticale pour révéler les icônes). Il est normalement activé. Sinon, cliquez sur le bouton **Activer**.



02› LANCER UNE ANALYSE

Cliquez sur le bloc **Protection contre les virus et menaces**. C'est là qu'en cas de doute, vous pouvez lancer une analyse de l'ordinateur. Choisissez **Analyse avancée**, puis effectuez une **Analyse complète**, éventuellement suivie d'une **Analyse hors ligne** en cas de problème.



ESSAYEZ UN ANTIVIRUS EN LIGNE

En plus de l'antivirus installé sur votre PC, soumettez votre ordinateur à une analyse complémentaire, avec un antivirus en ligne comme F-Secure.

INFOS **[F-SECURE]**
Où le trouver ? [**www.f-secure.com**] Difficulté : ☠☠☠

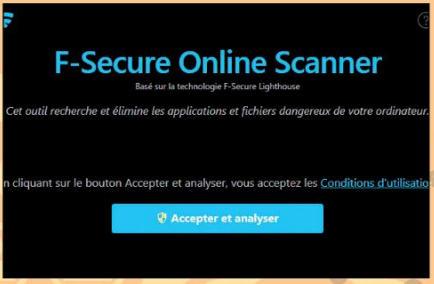
TUTO

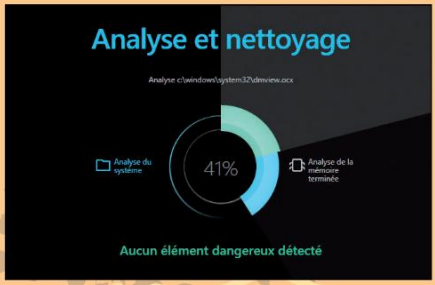
01 › ANALYSER

Sur la page d'accueil du service, cliquez sur **Online Scanner** – **Analysez et nettoyez gratuitement votre PC** puis **Lancer dès maintenant**. Acceptez le téléchargement du fichier proposé. C'est un exécutable, il n'y a rien à installer. Lancez-le et cliquez sur **Accepter et analyser**.

02 › NETTOYER

F-Secure analyse la mémoire de l'ordinateur puis le système entier. Patientez jusqu'à la fin de l'opération. Si le service détecte un fichier malveillant, il vous en informera et tentera automatiquement de le supprimer.





ANALYSEZ VOTRE SYSTÈME EN PROFONDEUR

Avast, l'un des meilleurs antivirus gratuits, permet une analyse très poussée de votre système, avec un scan au démarrage effectué avant même que Windows ne prenne la main.

INFOS [AVAST]
Où le trouver ? [www.avast.com] Difficulté : ☠☠☠

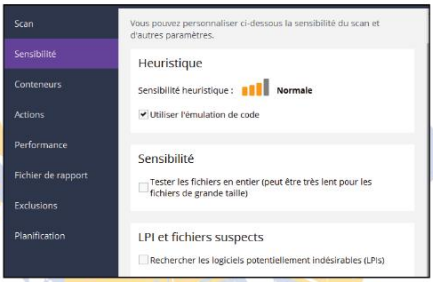
TUTO

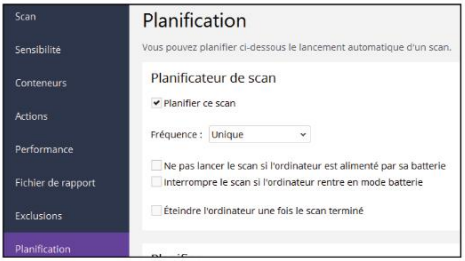
01 › LANCER UNE ANALYSE

Ouvrez Avast, cliquez sur **Protection** puis **Antivirus** et **Exécuter une analyse complète**. Vous pouvez continuer à utiliser le PC pendant ce temps, sachant que des ralentissements peuvent éventuellement survenir. Le scan d'Avant est aussi complet qu'il est long. Même pour un ordinateur peu chargé en logiciels et fichiers, cela peut prendre une heure au minimum.

02 › RÉGLER LES PARAMÈTRES

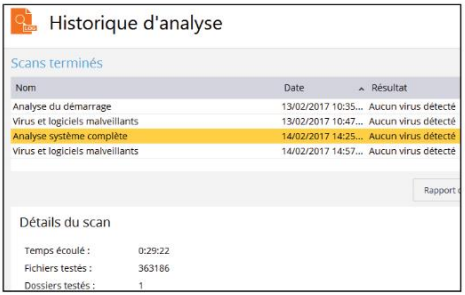
Si vous voulez choisir précisément les paramètres de l'analyse, des zones à scanner aux actions à effectuer en cas de menace, en passant par le niveau de sensibilité, c'est dans **Protection > Antivirus > Autres analyses > Créer une analyse personnalisée** que ça se passe. À réserver aux connaisseurs.





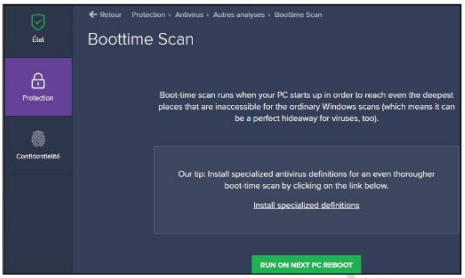
03 › PROGRAMMER L'OPÉRATION

L'analyse complète de base vous suffit, mais vous aimeriez la lancer plus tard? Cliquez sur l'engrenage en haut à droite du bloc **Exécuter une analyse complète** puis sur **Planification**. Cochez **Planifier ce scan**, choisissez sa fréquence, d'éventuelles options pour finir par l'heure et le jour de lancement. Validez avec **OK**.



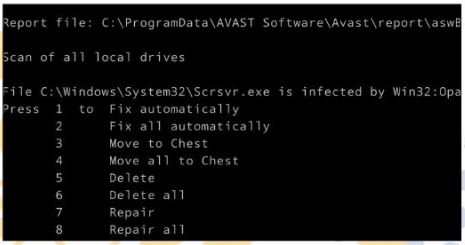
04 › VOIR LES RÉSULTATS

Dans **Protection > Antivirus**, cliquez sur **Historique d'analyse**. Une liste des scans passés s'affiche. Sélectionnez-en un et consultez les **Détails du scan**. Si Avast a trouvé quelque chose, vous avez accès à un **Rapport détaillé**, qui permet d'obtenir un fichier texte. Pratique pour le communiquer à quelqu'un ou le poster sur un forum, par exemple.



05 › SCANNER AU DÉMARRAGE

Ouvrez Avast et allez dans **Protection > Antivirus > Autres analyses > Analyse au démarrage**. Cliquez sur **Install specialized definitions** pour obtenir des définitions spécifiques et permettre à Avast d'analyser plus en profondeur le système. Validez avec **Run on next PC reboot** et redémarrez votre PC pour lancer le scan.



06 › ÉRADIQUER LES MENACES

Si l'antivirus découvre quelque chose, il faudra demander une réparation (**Heal** ou **Repair**) ou une mise en quarantaine (**Move to Chest**) plutôt qu'un effacement (**Delete**) afin d'éviter de supprimer un fichier important, en cas de faux positif par exemple (fichier considéré à tort comme infecté).

PROTÉGEZ-VOUS DES RANSOMWARES !

Destinés à racketter les utilisateurs qui en sont victimes, les ransomwares prolifèrent. Personne n'est à l'abri, et mieux vaut dès aujourd'hui vous protéger avec un logiciel spécialisé.

Les ransomwares ou rançongiciels sont des malwares introduits par un ver informatique. Une fois installés sur votre PC, ils ciblent les types de fichiers correspondant à vos données personnelles (photos, vidéos, documents DOC ou XLS, etc.), et les chiffrent avec une double clé très solide. Au bout de quelques minutes, vos documents deviennent inaccessibles et un message s'affiche sur votre écran, vous invitant à payer une somme d'argent pour récupérer la clé privée qui a servi au chiffrement et ainsi retrouver vos données. S'il est parfois possible d'agir après le chiffrage des données via des programmes spécifiques (voyez l'étape 4 ci-contre), il est important de se protéger. Antivirus spécialisé, le logiciel RansomFree se base sur l'analyse de 40 ransomwares et leurs variantes connues. Dès que le schéma typique d'un tel programme est détecté, RansomFree bloque le processus de chiffrement. Notez qu'il ne vous empêche pas d'utiliser des logiciels de chiffrement comme VeraCypt ou AxCrypt.

INFOS [RANSOMFREE]
Où le trouver ? [https://ransomfree. cybereason.com] Difficulté :

TUTO

01 › INSTALLER RANSOMFREE

Une fois installé, RansomFree va disséminer des fichiers leurres (des sortes d'appâts inoffensifs en somme) aux quatre coins de votre disque dur. Si un ransomware tente de chiffrer vos données, il ira aussi s'attaquer à ces fichiers et déclenchera l'alerte. Vous n'avez rien à faire ni aucun réglage à effectuer.

02 › LAISSER FAIRE LE LOGICIEL

Vous pouvez avoir l'impression que RansomFree n'est pas actif, puisqu'il agit en silence et qu'il n'apparaît pas dans la liste des programmes en cours du Gestionnaire des tâches. Rassurez-vous : RansomFree démarre systématiquement en même temps que Windows. Notez qu'il fonctionne aussi si un disque dur réseau est attaqué.

03 › RÉAGIR AUX ALERTES

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

04 › AGIR EN CAS D'INFECTION

Le site www.nomoreransom.org centralise tout ce qu'il faut savoir sur ces malwares au niveau de la prévention, mais il dispose aussi d'un service de détection en ligne (pour savoir de quel mal vous avez hérité) et de plusieurs outils de déchiffrement. Ce sont plus de 25 ransomwares qui peuvent être éradiqués avec ces outils.

RÉCUPÉREZ VOS DONNÉES

Victime d'un ransomware, vous vous retrouvez avec des fichiers chiffrés auxquels vous ne pouvez plus accéder ? Essayez Ransomware File Decryptor.

INFOS **[RANSOMWARE FILE DECRYPTOR]**
Où le trouver ? [**https://goo.gl/b7UxEw**] Difficulté : ☠☠☠

TUTO

01› DÉSIGNER LE COUPABLE

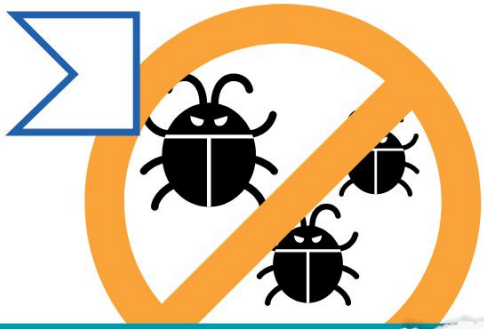
Ne nécessitant pas d'installation, Ransomware File Decryptor est un logiciel très facile à prendre en main. Acceptez le contrat d'utilisation (**Agree**) puis sélectionnez le ransomware dont vous êtes la victime. Si vous ne connaissez pas le nom, cherchez sur Internet l'extension de fichier qui apparaît ou voyez le site **www.nomoreransom.org**.

02› DÉCRYPTER UN FICHIER

Notez qu'on trouve même WannaCry dans la liste ! Faites ensuite **Select & Decrypt** pour sélectionner un fichier chiffré avec ce ransomware. Au bout de quelques secondes, Ransomware File Decryptor va vous rendre votre fichier d'origine.

VÉRIFIEZ FICHIERS ET SITES SUSPECTS

Le service en ligne VirusTotal met à contribution plusieurs antivirus différents pour vérifier que les fichiers que vous lui soumettez ne sont pas infectés.



INFOS **[VIRUSTOTAL]**
Où le trouver ? [**www.virustotal.com**] Difficulté :

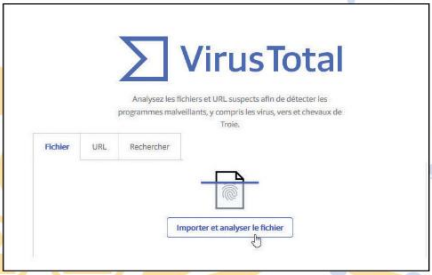
TUTO

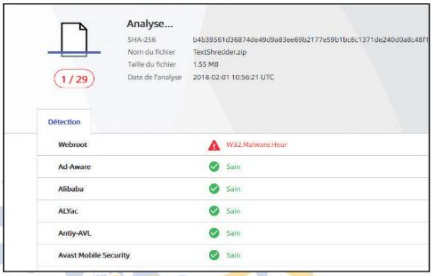
01› SÉLECTIONNER UN FICHIER OU UN SITE

La plupart des services d'antivirus en ligne nécessitent le téléchargement d'un module sur l'ordinateur. VirusTotal ne présente pas cet inconvénient. Il permet de scanner des fichiers (faites **Importer et analyser le fichier**), mais aussi d'analyser un site Web en soumettant son URL (onglet **URL**).

02› LANCER L'ANAYSE

VirusTotal scanne le fichier, et affiche les résultats d'analyse obtenus par différents antivirus. Si tous le considèrent comme sain, il ne devrait pas y avoir de souci. Si certains détectent une menace, soyez prudent ! Le cas échéant, faites une recherche sur Internet avec le nom de l'intrus.





DE NOUVELLES SOLUTIONS POUR DE NOUVEAUX PROBLÈMES

Un antivirus c'est bien, mais il existe des menaces qui peuvent ne pas être détectées par les solutions standards. Dans ces prochaines pages, nous allons parler des différents freewares de la société Phrozen.

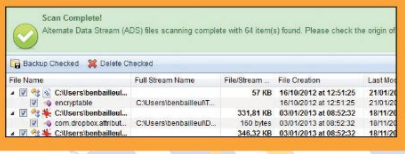
RunPE Detector

→ Contre les RAT

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

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

Lien : **www.phrozen.io/freeware**



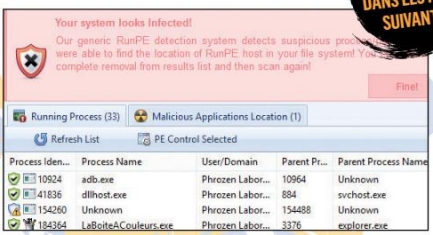
ADS Revealer

→ Sécurisez les volumes NTFS

ADS Revealer détecte sur les volumes NTFS la présence de fichiers cachés pouvant être des malwares : les fichiers ADS. Ces derniers, bien qu'invisibles depuis l'explorateur de fichiers Windows, ont un contenu bien physique et peuvent pulluler sans éveiller les soupçons de l'utilisateur. Il a même été prouvé que malgré les restrictions de Microsoft, il est toujours possible d'exécuter du code directement à partir d'un emplacement ADS....

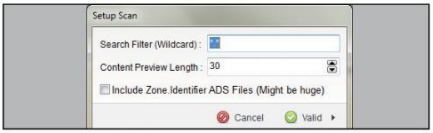
Lien : **www.phrozen.io/freeware**

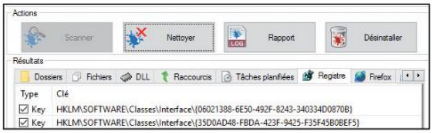
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



LES FICHIERS ADS À LA LOUPE !

TUTO





01 › LES OPTIONS

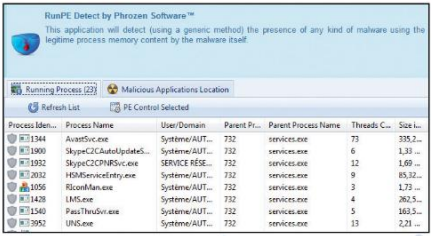
Le logiciel ne s'installe pas, il suffit de décompacter l'archive et de le lancer en tant qu'administrateur. Faites ensuite **Run Scan** puis choisissez la cible : tout le système (**Full System**), Tout le disque (**Target Drive**) ou un dossier particulier (**Target Folder**). Il est possible de filtrer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

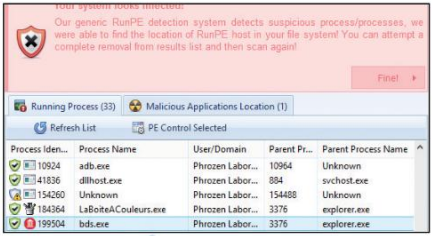
02 › LA MARCHE À SUIVRE

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

STOPPER L'USURPATION D'UN PROCESSUS AVEC RUNPE DETECTOR

TUTO





01 › LA LISTE DES PROCESSUS

Décompactez l'archive et lancez-le en tant qu'administrateur (clic droit dans l'icône). Vous verrez alors l'intégralité des processus qui tournent en tâche de fond sur votre machine. Faites alors **Run Scan**. Le logiciel va comparer les empreintes de ces processus avec des empreintes «connues».

02 › USURPATION DÉTECTÉE !

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

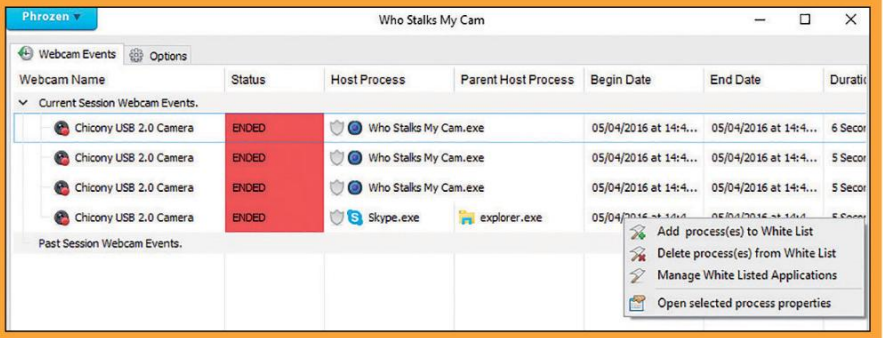
Winja → Le Ninja de Windows

Le nouveau venu Winja (pour Windows Ninja) est un complément idéal pour votre antivirus. Basé sur l'API Google Virus Total et développé conjointement avec la firme américaine, Winja propose de soumettre n'importe quel fichier louche à une cinquantaine d'antivirus en ligne différents. Un doute sur un fichier avant même de le télécharger? Le logiciel va vérifier sa dangerosité avant qu'il ne soit rapatrié sur votre ordinateur. Si «processus inconnu» vient apparaître dans votre gestionnaire des tâches, Winja ira se renseigner dans son immense base de données pour vous rassurer.

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Lien : **www.phrozen.io/freeware**

Who Stalk My Cam → Pour surveiller sa webcam



Who Stalk My Cam 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 et 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. Notez que WSMC n'est plus dans le catalogue de la compagnie, car il doit subir des modifications. Mais si vous êtes curieux, suivez notre lien en gardant en tête que le logiciel n'est peut-être pas mis à jour...

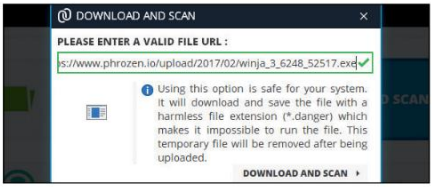
Lien : **http://who-stalks-my-cam.findmysoft.com**

SURVEILLEZ ET CONTREZ LES MENACES AVEC WINJA

TUTO

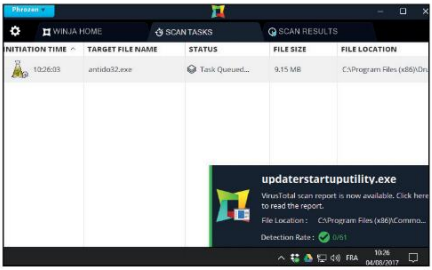
01› EXPLORER L'INTERFACE

Procédez à l'installation du soft en suivant notre lien. Relancez Winja. L'interface s'affiche avec ses outils. En vert vous ouvrez le fichier déjà présent sur votre PC, en jaune vous scannez un fichier en ligne, en bleu vous sondez les processus actifs et le rouge ouvre les outils complémentaires. Ces derniers doivent être lancés en mode administrateur.



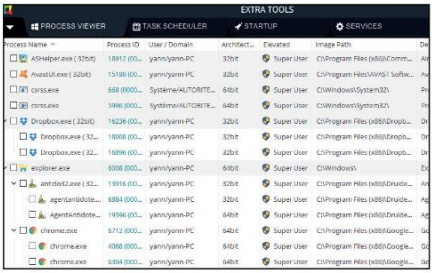
02› SCANNER AVANT DE TÉLÉCHARGER

Vous êtes sur un site de téléchargement légal et on vous propose de récupérer un fichier EXE ? Pourquoi prendre un risque ? Depuis votre navigateur préféré, faites un clic droit dans le bouton de téléchargement et faites **Copier l'adresse du lien** (ou équivalent). Dans Winja, allez dans **Download and Scan** puis copiez ce lien pour cliquer à nouveau sur **Download and Scan**. Patientez jusqu'au verdict.



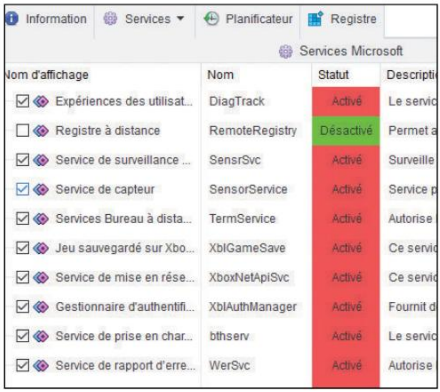
03› SCANNER LES PROCESSUS

Dans **Quick Process Scan**, sélectionnez les programmes qui tournent en arrière-plan. Vous pourriez avoir des surprises : des noms méconnus sont parfois parfaitement légitimes tandis que d'autres aux noms «passe-partout» sont des malwares. Winja est très rapide, car il se base sur les précédentes recherches des internautes en se fiant à l'empreinte unique de votre fichier (hash MD5 et SHA-1).



04› UTILISER LES OUTILS

Explorez les **Outils supplémentaires (Extra Tools)** pour un scan plus précis des processus, des tâches planifiées de Windows (qui peuvent être utilisées par des virus), des programmes qui se lancent au démarrage de Windows, des services de Windows ou encore de votre réseau Internet.

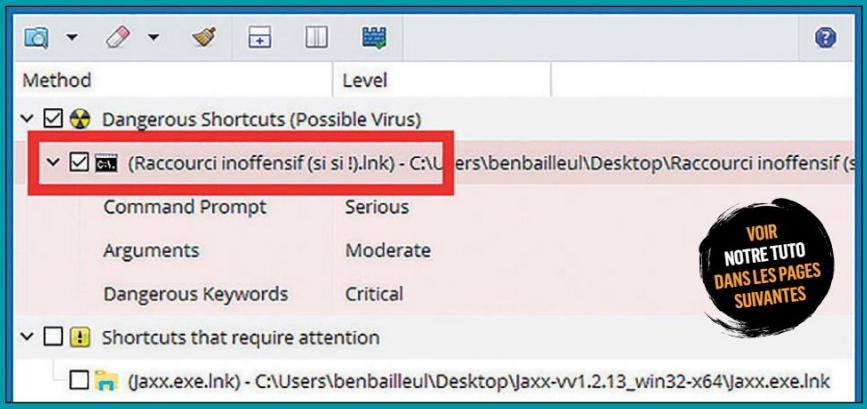


Windows Privacy Tweaker
→ Windows 10 plus discret

Windows 10 collecte quantité de données sur votre PC, qui sont transmises à des serveurs de Microsoft. Les paramètres de confidentialité du système permettent de limiter un peu ces fuites. Windows Privacy Tweaker va plus loin, en désactivant des services cachés, ou en apportant des modifications au registre. La création d'un point de restauration vous est proposée avant toute action, permettant de revenir facilement en arrière.

Lien : **www.phrozen.io/freeware**

Shortcut Scanner → Faites la chasse aux faux raccourcis



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

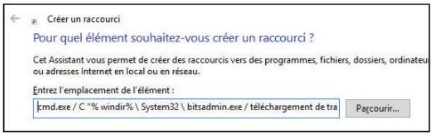
Lien : **www.phrozen.io/freeware**

SCANNEZ LES RACCOURCIS AVEC SHORTCUT SCANNER

TUTO

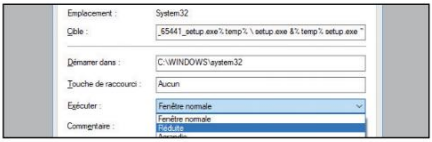
01› LA PORTE D'ENTRÉE

Cette démonstration se base sur un programme Windows natif, appelé BITSAdmin Tool et qui est intégré à Windows depuis Windows XP SP2. C'est la «porte d'entrée». Cet outil de ligne de commande a été conçu pour créer des tâches de téléchargements et pour surveiller leurs progressions. Bitsadmin.exe est bien signé par Microsoft et approuvé par d'autres logiciels antivirus et peut être utilisé en une seule ligne de commande. Par exemple : **bitsadmin / transfer downloader / priorité normale** https://phrozensoft.com/uploads/2016/09/Winja_2_6084_65441_setup.exe% temp% \ setup.exe



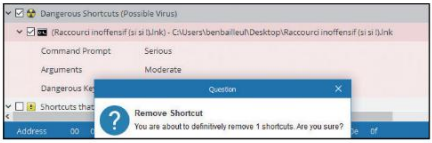
02› CRÉATION DU RACCOURCI

Cette commande va télécharger dans le dossier temporaire de Windows un fichier d'application situé sur les serveurs de PhrozenSoft. Utilisons maintenant cet outil de ligne de commande pour l'exploiter dans un nouveau raccourci Windows. Faites un clic droit quelque part dans votre explorateur, cliquez sur **Créer un nouveau raccourci** et entrez la ligne de commande suivante : **cmd.exe / C "% windir% \ System32 \ bitsadmin.exe / téléchargement de transfert / priorité normale** https://phrozensoft.com/uploads/2016/09/Winja_2_6084_65441_setup.exe% temp% \ setup.exe &% temp% setup.exe"



03› JUSTE UN EXEMPLE

Une fois le raccourci créé avec succès, nous allons modifier ses propriétés (clic droit sur le raccourci puis sélectionnez **Propriétés**). Mettez l'option **Exécuter** sur **Réduite**, cela aidera à rendre le terminal moins visible en le réduisant à la barre des tâches en charge. Bravo, votre premier raccourci malveillant est maintenant prêt ! Attention, bitsadmin.exe est juste un exemple de ce que vous pouvez faire en utilisant un raccourci de Windows, vous pouvez potentiellement faire toutes les choses malveillantes possibles que vous pourriez faire à travers des lignes de commande.



04› FAITES LA CHASSE AUX FAUX RACCOURCIS !

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

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

SAUVEGARDE

p30
Avira **PASSWORD** Manager

p32
7 LIVE CD au secours de votre PC

p38
Comment **SAUVEGARDER** Windows

AVIRA PASSWORD MANAGER

LA GARANTIE DE MOTS DE PASSE SÛRS

Plus connue pour son antivirus, la société de sécurité numérique Avira propose aussi un gestionnaire de mots de passe. Facile d'accès et disponible sur toutes les plates-formes principales (navigateurs, ordinateurs et smartphones), le vrai plus d'Avira réside néanmoins dans sa version pro, qui donne accès à une véritable vigie sur vos mots de passe.

« **81 %** des vols de données sont causés par des mots de passe faibles ou dérobés. » S'appuyant sur une étude du site web allemand Security Insider, Avira affiche ce constat alarmant en page d'accueil de son service de gestionnaire de mots de passe. Avec son extension pour navigateurs, Avira Password Manager est assez complet, même en version gratuite : il permet d'importer ses mots de passe, les stocker et d'en générer de nouveaux pour les modifier. Avec une mention particulière à la fonction remplissage des champs de connexion (identifiant et mot de passe), qui reconnaît le compte automatiquement, là où d'autres services nécessitent un ou deux clics en plus.

DES ALERTES SÉCURITÉS BIEN PRATIQUES, MAIS PAYANTES

Disponible sur Chrome, Firefox, Windows, Mac, Android et iOS, Avira Password Manager est tout terrain, bien qu'un peu envahissant car souvent installé avec d'autres produits Avira. En plus des mots de passe, Avira Password Manager propose de conserver des notes sécurisées, un service devenu assez commun pour les gestionnaires de mots de passe dans le cloud*. Mais son véritable atout est sa version Pro, qui permet de surveiller ses mots de passe, détecter de potentielles failles de sécurité de ses services et aide à les résoudre.

Lien : **https://www.avira.com/fr/avira-password-manager**

GÉRER SES MOTS DE PASSE AVEC AVIRA PASSWORD MANAGER

TUTO

01 › INSTALLER L'APPLICATION ET L'EXTENSION

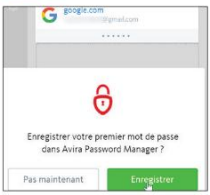
Après vous être inscrit avec un **mot de passe maître**, cliquez sur **Verify account** dans l'e-mail qui vous a été envoyé. Cliquez ensuite sur **Download now**, puis installez l'application et activez l'extension **Avira Password Manager** (et **Protection Web Avira** si vous le souhaitez).

02 › IMPORTER LES MOTS DE PASSE DE VOTRE NAVIGATEUR

Si vous avez enregistré vos mots de passe dans votre navigateur, cliquez sur **Importer maintenant** dans le troisième champ d'astuces au centre de l'écran. Cliquez ensuite sur **Import depuis navigateur** > **Autoriser** > **Importer** > **Terminé**.

03 › AJOUTER UN MOT DE PASSE MANUELLEMENT

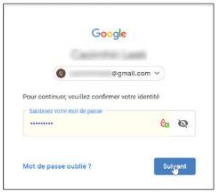
Connectez-vous au service de votre choix (Gmail, par exemple). Une fenêtre apparaît et vous propose d'enregistrer vos identifiant et mot de passe dans Avira Password Manager. Cliquez sur **Enregistrer**.



Il est aussi possible d'ajouter ses identifiants et mots de passe en cliquant sur le **bouton +** dans l'interface d'Avira Password Manager.

04 › SE RECONNECTER AUTOMATIQUEMENT À UN SERVICE

Vous souhaitez vous reconnecter à un service sans avoir à taper vos identifiant et mot de passe ? Avira Password Manager les remplit pour vous. Sur Gmail, par exemple, vous n'avez qu'à cliquer 2 fois sur **Suivant**.



05 › MODIFIER UN MOT DE PASSE

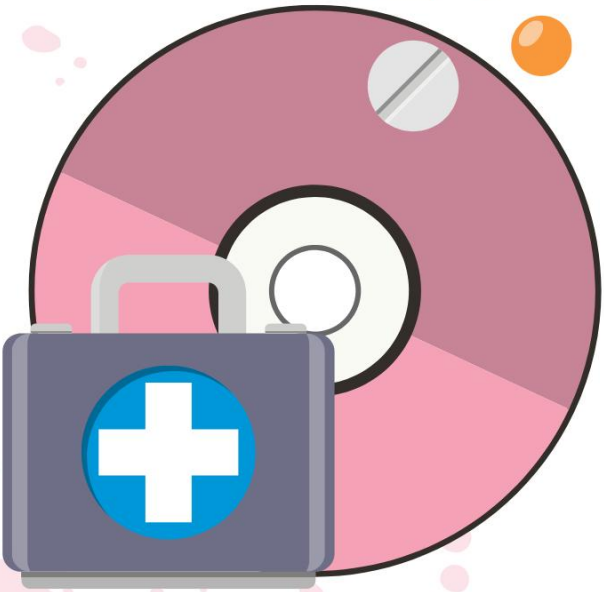
Connectez-vous au service de votre choix (continuons sur Gmail) et rendez-vous sur la page de modification de votre mot de passe. Dans le champ du nouveau mot de passe, cliquez sur l'**icône du Générateur de mot de passe** Avira. Cliquez ensuite sur **Utiliser mot de passe.** Validez la modification (en cliquant sur **Modifier le mot de passe** dans le cas de Gmail). Une fenêtre s'affiche en haut à droite de l'écran. Cliquez sur **Mettre à jour**.

06 › LES AUTRES SERVICES AVIRA

Cliquez sur l'icône Avira dans la barre des tâches en bas de votre écran. Avira vous propose une dizaine d'autres services, comme un antivirus, un VPN ou encore un gestionnaire de mises-à-jour.

7 LIVE CD AU SECOURS DE VOTRE PC...

Il y a des signes qui ne trompent pas : ralentissements, publicités non sollicitées, faux messages d'alerte, crash à répétition ou tout ça à la fois ? Qu'il s'agisse d'une infection, d'un problème de registre ou d'un bug du système, votre valeureux PC a besoin d'être réparé. Que vous ayez la main sur Windows ou non, voici nos solutions «Live CD»... Ha oui la plupart sont compatibles avec Linux.



Les Live CD fonctionnent tous de la même manière. Il faut télécharger une image de disque au format ISO puis la graver sur un CD ou un DVD en fonction de leur taille. Pour certains d'entre eux, il est même possible de les placer sur une clé USB (pratique si votre lecteur est absent ou cassé). Avec le logiciel Xboot, vous pouvez même vous faire une compilation de

différents Live CD sur une seule et même clé USB. Veillez juste à ce que votre BIOS accepte le boot depuis un port USB.

DES DVD BOURRÉS DE SOLUTIONS

En fonction du Live CD que vous aurez choisi, les outils à l'intérieur permettront une désinfection, des diagnostics (RAM, disque dur), une réparation (registre, secteur de disque), une sauvegarde, etc. Lorsque vous aurez terminé, il faudra relancer Windows en croisant les doigts pour qu'il veuille bien se lancer. Si ce n'est pas le cas, les dégâts seront moindres si vous devez formater et réinstaller un système puisque vous aurez sauvegardé vos mots de passe et vos fichiers... Si vous avez un numéro de licence Windows (un autocollant avec une suite de caractères sur votre unité centrale), mais pas le DVD d'installation (versions dites «OEM»), rien ne vous empêche de télécharger un Windows sur Internet. Le téléchargement est légal si vous ne changez pas de PC : profitez-en !

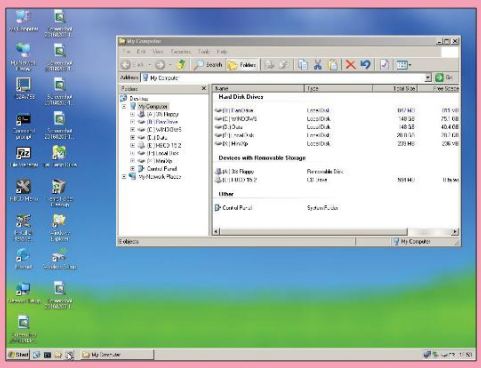
EN CAS DE PANNE, LE PLUS EFFICACE EST SOUVENT DE RÉPARER SANS CHARGER WINDOWS...

CHANGEZ LE BOOT

De base, votre PC va «booter» sur le disque dur pour charger Windows. Pour afficher les menus de votre Live CD, il faudra changer ce réglage dans le BIOS. Il faudra faire **Suppr**, **F1**, **F2** ou **F8** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrer dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier votre lecteur de CD/DVD ou votre port USB si c'est cette solution que vous avez choisie. Attention, certains fabricants de cartes mères intègrent depuis quelques années un BIOS sécurisé et un peu pénible appelé UEFI. Voici un article très intéressant si vous avez ce type de BIOS : **http://goo.gl/KSDTS5**

7 LIVE CD INDISPENSABLES POUR VOTRE PC

Hiren's Boot CD



Hiren's Boot CD fait office de couteau suisse. Il contient énormément de programmes permettant de restaurer un système ou de faire des tests : RAM, processeur, gestionnaire de fichiers, programme DOS, récupération de vos mots de passe, etc. Mais la partie la plus sympa reste son mode MiniXP qui va imiter le fonctionnement d'un système Windows à minima. Vous aurez donc une interface graphique pour lancer tous les programmes contenus dans le CD. Ce mode est aussi idéal pour faire vos sauvegardes de fichiers. Branchez une clé USB ou un disque dur et transférez vos documents ! Attention, il n'est plus mis à jour...

Lien : **www.hirensbootcd.org**

F-Secure Rescue Disk

F-Secure Rescue Disk est un autre Live CD qui propose un antivirus très pratique. Pour mettre à jour la base de données virale, nous vous conseillons de brancher le PC en Ethernet à votre box, car le WiFi fonctionne rarement. Lancez ensuite l'analyse. Lorsque les virus seront découverts, n'oubliez pas de choisir systématiquement l'option la moins radicale : il vaut mieux tenter de guérir un fichier contaminé ou de le mettre en quarantaine que de l'effacer...

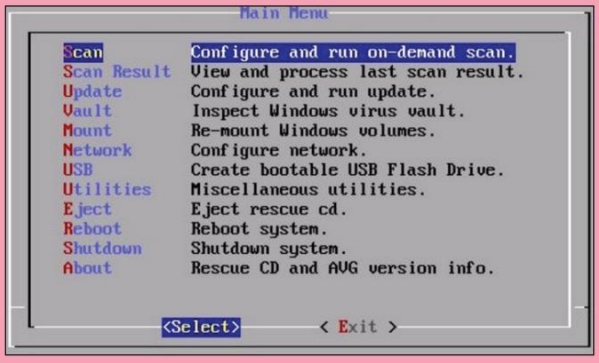
Lien : **https://goo.gl/6D36oI**

MediCat

Cette compilation permet de faire la chasse aux virus, de restaurer un Windows bancal, de sauvegarder des données en cas de problème physique ou de mettre un peu d'ordre dans vos partitions. MediCat comprend aussi des outils de diagnostic en tout genre, plusieurs logiciels pour récupérer vos mots de passe. Idéal pour les altruistes qui n'hésitent pas à se déplacer pour réparer l'ordi d'un ami, MediCat est indispensable. La version la plus «lourde» peut aisément prendre place sur une vieille clé USB de 8 Go, raison de plus pour la garder tout le temps avec soi. Là où Hiren's Boot CD donnait l'accès à un Windows XP «light», MediCat propose un Mini Windows 10 et Lubuntu.

Lien : **https://goo.gl/3imeh8**

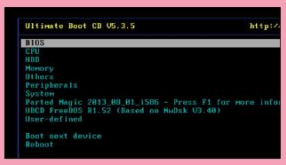
AVG Rescue CD



Et voici l'ultime antivirus ! Au lancement du DVD, choisissez **AVG Rescue CD** et attendez que le contenu se charge dans la RAM. Vous devriez avoir le menu principal avec l'accès à la mise à jour de la base de données virale (**Update**) et aux **Utilities** (gestionnaire de fichiers pour sauver vos données, éditeur de registre, test du disque dur, etc.). Débutez par une mise à jour et pour commencer votre scan, montez les partitions Windows (**Mount**). Choisissez ensuite **Scan**. Il faudra alors sélectionner les éléments à scanner. Si vous ne connaissez pas l'origine du problème, optez pour une recherche en profondeur en sélectionnant toutes les options possibles dans **Scan Options**.

Lien : **http://beta.falconfour.com/category/bootcd**

Ultimate Boot CD



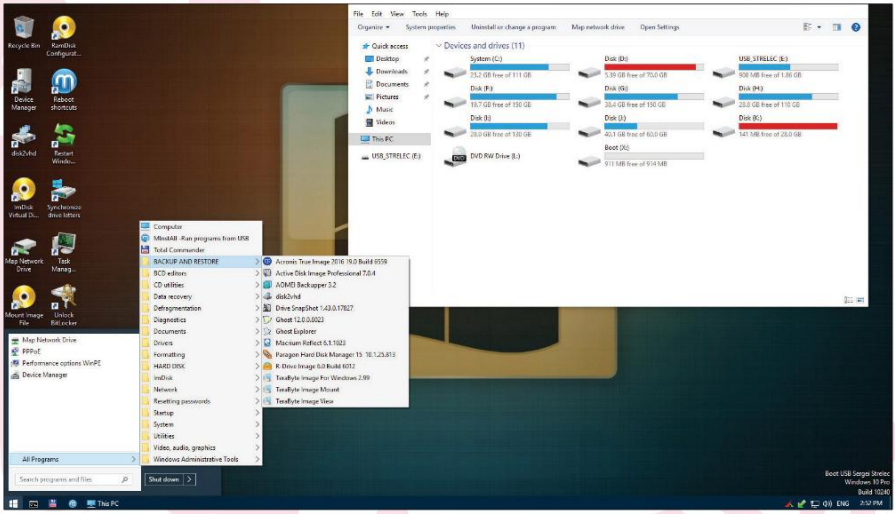
Ultimate Boot CD est une autre compilation d'outils de dépannage informatique pour Linux ou Windows. Il contient des outils pour le diagnostic, le clonage ainsi que le nettoyage du disque dur. L'utilisateur aura entre autres à sa disposition ViVARD, permettant d'effectuer des tâches de maintenance sur le périphérique de stockage en vue d'optimiser ses performances. On compte aussi des utilitaires de modification mot de passe comme Offline NT Password & Registry Editor qui permet de supprimer le mot de passe d'une session Windows. Enfin, le CD comprend des outils de désinfection : Avast, AVG, ou encore McAfee.

Lien : **www.ultimatebootcd.com**

Win PE 10-8 Sergueï Strelec

Et voici le meilleur pour la fin ! Régulièrement mis à jour et extrêmement complet (3,91 Go), ce Live DVD compilé par un informaticien russe est sans doute ce qui se fait de mieux. Ne vous fiez pas à la page avec les menus en cyrillique, tout est bien en anglais. Cliquez sur le bouton vert et sur la page suivante, allez en bas pour accéder au lien de téléchargement. Vous y trouverez des logiciels de sauvegarde, d'entretien de l'ordinateur, des disques durs et des partitions, des diagnostics, des logiciels de récupération de données, des outils de réparation de Windows, audit réseau, récupération de fichiers endommagés, antivirus, drivers, etc.

Lien : **http://sergeistrelec.ru**



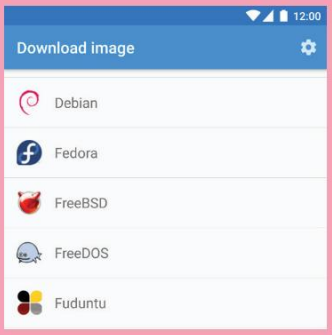
FalconFour's Ultimate Boot CD

Le Live CD de FalconFour's est une amélioration de Hiren Boot avec des options de boot plus complètes, mais toujours avec son mode MiniXP. On y trouve des outils pour réparer des partitions, récupérer des données perdues ou des mots de passe, des logiciels d'audit réseau et quelques antivirus. Comme ses camarades, FalconFour's Ultimate Boot CD est disponible en version DVD ou en forme d'ISO à placer sur une clé USB.

Lien : **http://beta.falconfour.com/category/bootcd**

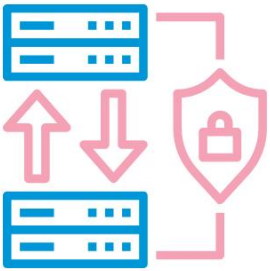
BOOTER SON PC GRÂCE À UN MOBILE AVEC DRIVEDROID

Si vous avez l'utilité de démarrer votre PC ou celui des autres depuis un LiveCD pour réparer, hacker ou changer d'OS, vous allez aimer DriveDroid. Cette appli permet de booter votre PC à partir d'une image (Windows, Linux, etc.) stockée sur votre mobile. Cela peut se révéler pratique dans le cas où vous ne disposez pas de clé USB ou si vous voulez avoir un Kali, un Ubuntu ou un MediCat sous la main, quelle que soit la circonstance. Sélectionnez l'ISO à monter, branchez le câble USB entre votre smartphone et votre PC et c'est parti !



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

SAUVEGARDE DE WINDOWS

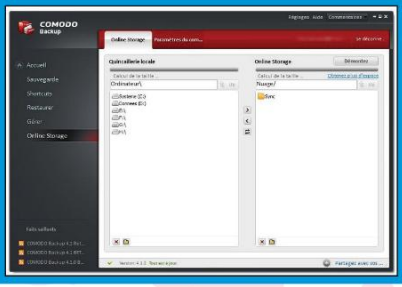


Même si le module de sauvegarde de Windows a fait des progrès, voici une belle sélection de programmes qui proposent des fonctionnalités intéressantes...

Comodo BackUp
→ La solution simple et efficace

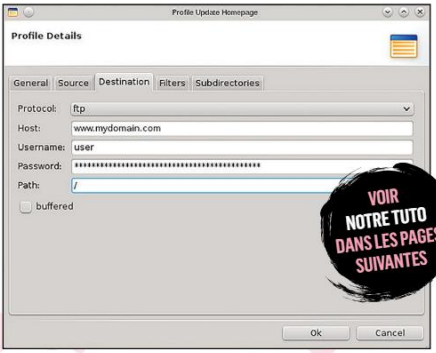
Rien de plus rageant et désespérant que de perdre ses données pendant une réinstallation système. Comodo BackUp est là pour vous éviter cette peine insupportable. Ce logiciel permet de faire des sauvegardes automatiques ou ponctuelles de vos fichiers sur différents supports : clé USB, disque dur externe, cloud, serveur privé, compte-email. Bref, vous avez l'embarras du choix. Les processus sont simples à appréhender, et qui plus est, Comodo BackUp est gratuit et offre 5Go de stockage en ligne. De quoi commencer à mettre au chaud quelques films ou photos compromettantes.

Lien : **www.comodo.com**



FullSync → La sauvegarde contrôlable à distance

L'un des principaux points fort de FullSync est de pouvoir gérer ses différents backups à distance, depuis un autre ordinateur que le vôtre.



VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Pratique pour accéder à des fichiers n'importe où par exemple. Ici également, la sauvegarde planifiée est de la partie, afin de préserver régulièrement ses données. On retrouve ensuite d'autres fonctionnalités plus classiques, comme l'exclusion de dossiers, ou la protection via mot de passe.

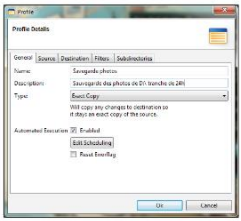
Lien : **https://fullsync.sourceforge.io**

UN EXEMPLE CONCRET AVEC FULLSYNC

TUTO

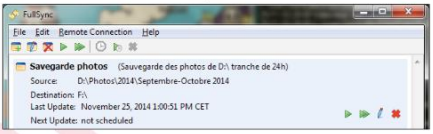
01 › LE «PROFIL»

Avant de commencer, sachez que FullSync est aussi disponible dans une version ne nécessitant pas d'installation. Dès l'ouverture, il faudra vous créer un «profil» (**New Profile**). Il s'agit en fait d'éditer votre sauvegarde. Dans notre exemple, nous allons faire une sauvegarde de nos photos sur un disque dur externe toutes les 24 heures. Après avoir entré un nom et une description, il faudra choisir le **Type**.



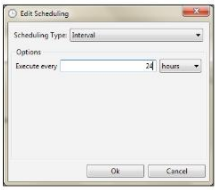
02 › 4 CHOIX DE SAUVEGARDE/ SYNCHRONISATION

Vous aurez 4 choix. **Publish/Update** est utilisé pour mettre à jour un site Web à partir d'une copie locale d'un serveur distant tandis que **Backup Copy** va tout sauvegarder sans effacer quoi que ce soit dans le dossier de destination. **Exact Copy** est la solution idéale pour nos photos puisque tous les changements seront pris en compte, y compris les suppressions (vous n'aurez pas à vous encombrer des versions antérieures de photos). Enfin, **Two Way Sync** va comparer la source et la destination puis ira copier les fichiers plus récents d'un côté comme de l'autre (attention, car les versions antérieures seront écrasées !).



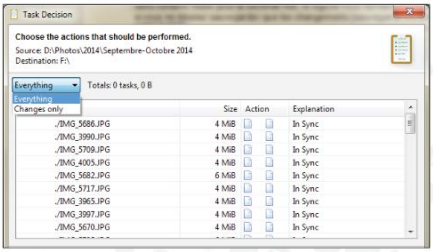
03 › AUTOMATISATION

Plus bas, vous pourrez aussi paramétrer une exécution automatique. Cochez **Enabled** et faites **Edit Scheduling**. Ici, vous pourrez régler un intervalle ou et une date précise (**Crontab**). Validez et dirigez-vous ensuite vers les onglets **Source** et **Destination**. Dans notre cas, nous mettrons file dans protocole puisqu'il s'agit d'une sauvegarde locale, mais vous pouvez aussi sauvegarder vers et depuis un serveur FTP, SFTP et SMB. Dans **Path**, il faudra mettre un chemin (à la fois dans **Source** et **Destination**). Notez que FullSync permet de sauvegarder ou synchroniser des dossiers même si la source et la destination sont toutes deux distantes (de serveur à serveur). Les autres onglets servent à filtrer des dossiers ou fichiers que vous ne voulez pas sauvegarder (filtres par nom, taille, date de modification, etc.).



04 › C'EST TOUT !

Après avoir validé, vous pourrez soit commencer votre première sauvegarde (même si ce n'est pas le moment prévu par vos planifications) en cliquant sur le triangle vert. Vous pouvez aussi vous contenter de suivre votre planification en faisant **Start Scheduler**. Notez que lorsque vous réaliserez votre sauvegarde dans certains modes pour la seconde fois, le logiciel vous demandera si vous voulez tout re-sauvegarder ou si vous ne désirez sauvegarder que les changements (**sauvegarde incrémentielle**).



pCloud → Stocker tranquillement, comme sur un nuage

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

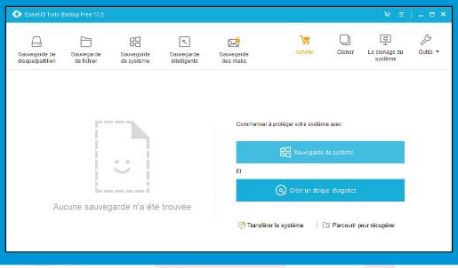
L'autre option quand il s'agit de sauvegarder à tout va sans multiplier le nombre de disques durs externes par 10, c'est le cloud bien entendu ! À ce jeu-là, pCloud reste un challenger de poids. Tout comme Google Drive ou Dropbox, ce service vous permet de stocker l'intégralité de vos fichiers, vidéos, photos de vacances au Cap d'Agde directement sur les serveurs de l'entreprise. Sans abonnement, vous pourrez disposer d'un espace de stockage de 10 Go. Inquiet pour la sécurité de vos données ? Optez pour l'option pCloud Crypto, qui protège vos fichiers avec un puissant système de chiffrement.

Lien : **www.pcloud.com**

EaseUS Todo Backup
→ La référence

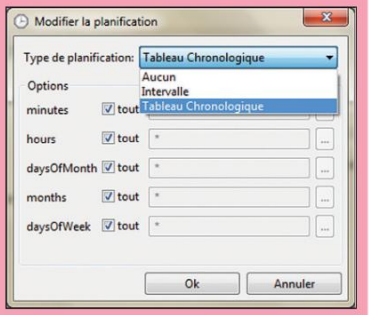
Même dans sa version Free, EaseUS Todo Backup est complet : sauvegarde d'un disque ou d'une partition, d'un groupe de dossiers, du système, planification, sauvegarde sur le réseau, sur un NAS ou un cloud (Google Drive, OneDrive ou Dropbox) et clonage complet de vos disques. Le logiciel permet aussi de créer un disque bootable pour restaurer les données préalablement sauvegardées. Si vous désirez stocker sur des CD ou des DVD, Todo Backup va fractionner votre sauvegarde en paquets de 650 Mo, 700 Mo ou 4,7 Go. Mais ce n'est pas tout. Todo Backup peut aussi effacer de manière sécurisée une partition, créer un disque d'urgence en cas de crash (Linux ou WinPE) et vérifier l'intégrité des différentes images de disque que vous aurez créées.

Lien : **goo.gl/7VvNFt**



SyncThing
→ Le partage en toute sécurité

SyncThing est un outil open source qui vous permet de partager, reproduire et stocker vos fichiers sur l'ensemble de vos appareils à distance. Une sorte de Google Drive local sans le côté invasif



de la firme de Moutain View en somme. Les données sont sécurisées grâce à un chiffrement de bout en bout (AES + TLS), histoire de sauvegarder vos données en toute quiétude.

Lien : **https://syncthing.net**

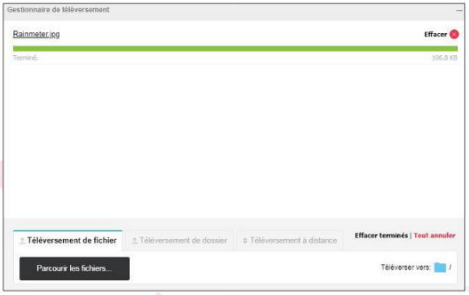
SAUVEGARDER SES DONNÉES SUR LE CLOUD AVEC PCLOUD

TUTO

pCloud est un service en ligne gratuit qui vous permet, à l'instar de Google Drive ou Dropbox, de stocker vos fichiers, vidéos et photos sur le cloud, le "nuage" en bon français. Une fois vos données sur les serveurs de l'entreprise, vous pouvez y accéder où et quand bon vous semble. PCloud a la bonne idée d'être multiplateforme et fonctionne sur PC, Mac, Linux, Android, iOS, Windows Phone, et comme extension sur certains navigateurs internet comme Google Chrome, Mozilla Firefox ou Opera. Voyons ensemble comment sauvegarder votre premier fichier sur pCloud.

01› ACCÉDER À PCLOUD

Une fois votre compte créé, pCloud vous invite à télécharger pCloud Drive. Acceptez ! ce logiciel vous permettra de profiter pleinement de l'expérience pCloud. Laissez l'installation se poursuivre et retournez sur le site. Pour débloquer l'intégralité de votre capacité de stockage (10 Go), les développeurs de pCloud vous demande de suivre quelques étapes. C'est en réalité un tutoriel déguisé, pour vous familiariser avec les diverses fonctionnalités de pCloud. **Suivez scrupuleusement les instructions**.

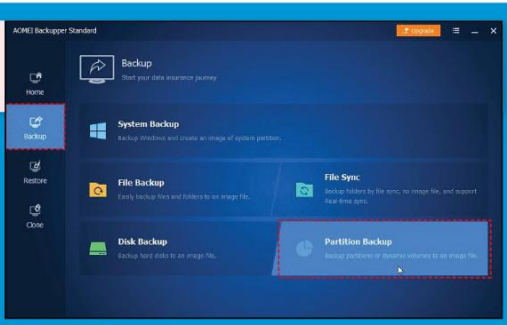


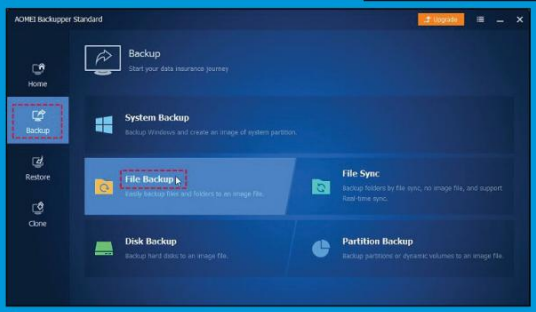
02› TÉLÉVERSER UN FICHIER

Une fois sur la page d'accueil, cliquez sur l'onglet **Téléversement**, en bas à droite de votre écran. Puis une fois dans le gestionnaire, allez sur **Téléversement de fichier**, ou **Téléversement de dossier**, selon ce que vous voulez transférer. Il ne vous reste qu'à laisser le site travailler, et bingo, votre fichier est disponible dans votre espace de stockage personnel sur pCloud.

AOMEI Backupper → Le roi de la sauvegarde

AOMEI Backupper est un logiciel gratuit grâce à qui vous pourrez sauvegarder, cloner ou restaurer des disques durs et des partitions, tout comme l'intégralité de votre système. Un outil pratique notamment lorsque vous changez de



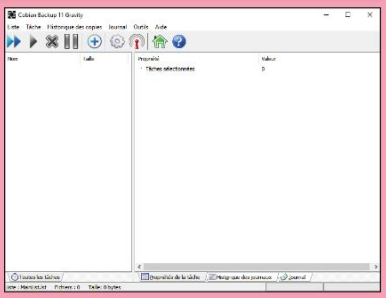


système d'exploitation ou quand vous voulez importer des disques durs entiers sur une nouvelle machine. D'autres outils utiles viennent se greffer à ses fonctions premières, comme un module de cryptage et de compression, ou encore un explorateur de fichiers. Attention, le tout en anglais.

Lien : **www.backup-utility.com**

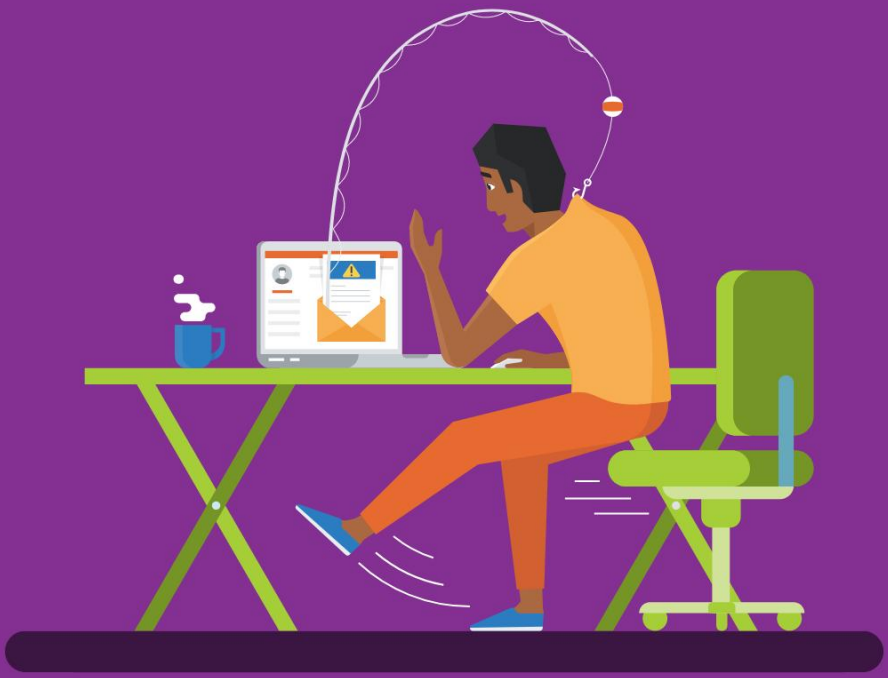
Cobian Backup → Le challenger

Cobian Backup est un autre poids lourd de la sauvegarde. Gratuit et régulièrement mis à jour, il permet presque autant de choses que Todo : sauvegarde standard ou incrémentielle, compression, planification, transfert vers FTP ou un volume disponible sur votre réseau local. Il lui manque cependant le clonage de disque et toutes les petites choses qui font de Todo un cador (disque d'urgence, fractionnement, effacement et sauvegarde du système). Du côté des points forts, on compte un chiffrement AES « complet » et une compatibilité avec la technologie Shadow Copy de Microsoft (création de sauvegarde même si le volume est en activité).



Lien : **cobiansoft.com**

HACKING



p44
Récupérez tous vos **SÉSAMES**

p50
Sécurisez votre **WIFI**

p54
Prenez le **CONTRÔLE** !

p60
Tout sur les « **HASH** »

p63
BIDOUILLEZ
votre Windows

RÉCUPÉREZ TOUS VOS SÉSAMES !

LaZagne

→ IL RÉCUPÈRE TOUT CE QUI PASSE

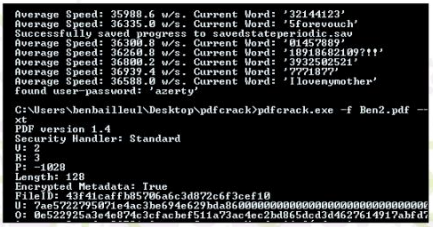
Dans le même genre que RecALL (voir cette sélection), ce programme en ligne de commande va pomper les sésames contenus dans vos navigateurs et plusieurs autres logiciels. Il est légèrement moins complet que RecALL et un peu plus âpre au niveau de son interface, mais est beaucoup plus discret et rapide. Pour accélérer la manœuvre, il est possible de cibler ce que vous voulez récupérer. À essayer d'urgence!

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

PDFCrack → ET CRACK, LE PDF !

PDFCrack est un logiciel destiné à fonctionner sur système Linux, mais il existe une version pour Windows. Il permet de tirer profit des processeurs multicœurs et de la puissance de plusieurs ordinateurs (cluster) pour attaquer les mots de passe d'ouverture et d'autorisation. La progression est automatiquement sauvegardée pour reprendre un projet en cours. Sur notre PC de test, PDFCrack a été capable de passer en revue 37 500 mots de passe à la seconde.

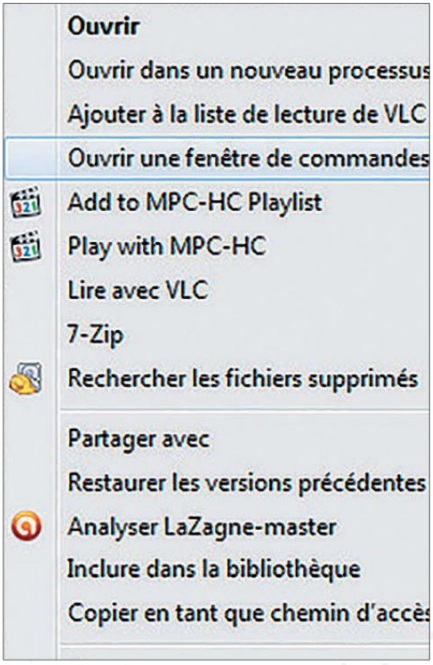
Lien : **http://andi.flowrider.ch/research/pdfcrack.html**



laZagne RÉCUPÉRATION DE MOTS DE PASSE AVEC LAZAGNE

TUTO

Si vous avez physiquement accès à un ordinateur, LaZagne va analyser le contenu de la base de registre et des dossiers pour afficher tous les mots de passe qui traîne en clair : navigateurs, logiciels, bases de données, réseaux WiFi, etc.



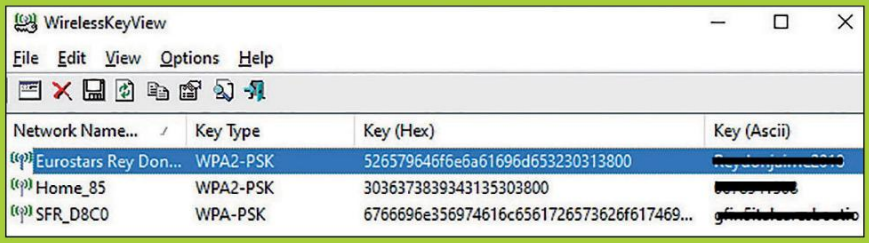
01 › EN LIGNE DE COMMANDE

Décompactez le fichier ZIP et placez le contenu où vous le souhaitez. Rendez-vous dans le dossier **LaZagne-master\Windows**. Maintenez la touche **Maj** du clavier, faites un clic droit dans Standalone puis cliquez sur **Ouvrir une fenêtre de commande ici**. Pour connaître la liste des commandes, faites **lazagne.exe** puis tapez sur **Entrée**.

02 › À L'ACTION !

Vous pouvez constater qu'il suffit de taper **lazagne.exe browsers** pour récupérer les mots de passe contenus dans les navigateurs ou **lazagne.exe mails** pour les clients POP/IMAP/SMTP. Pour obtenir absolument tous les mots de passe contenus dans le PC, il suffit de taper **lazagne.exe all**. Magique !

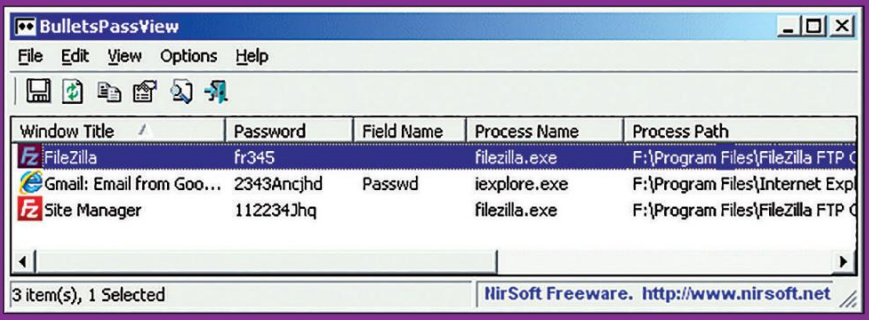
WirelessKeyView → Tous les codes WiFi



WirelessKeyView récupère toutes les clés de sécurité réseau sans fil (WEP / WPA) stockées dans votre ordinateur par le service WLAN AutoConfig de Windows. Il vous permet d'enregistrer facilement toutes les clés dans un fichier texte / html / xml ou de copier une clé unique dans le presse-papiers. Vous pouvez également exporter vos clés sans fil dans un fichier et importer ces clés dans un autre ordinateur.

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

BulletsPassView → Le sésame derrière les puces



Si vous avez des mots de passe sous forme de puces noires et que vous voulez les récupérer, le programme BulletsPassView constitue la solution idéale. Avant de lancer le programme, essayez d'ouvrir les logiciels où il y a des signes de ce genre et faites un scan. Pour FileZilla par exemple, il suffit d'ouvrir le gestionnaire des sites, cliquer sur le site, puis taper **F5** dans le BulletsPassView pour afficher le mot de passe caché.

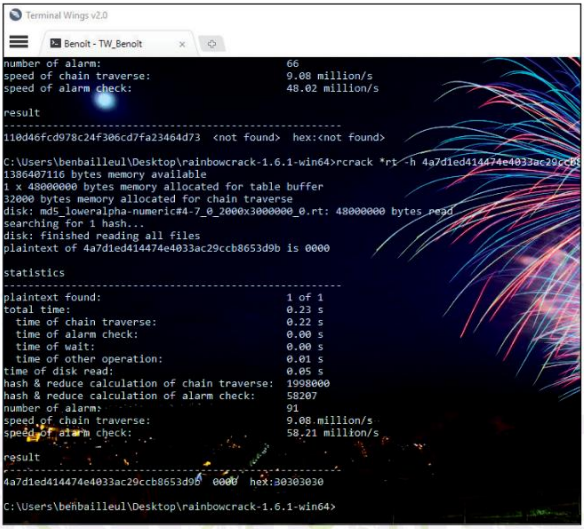
Lien : **www.nirsoft.net/utils/bullets_password_view.html**

RainbowCrack

→ Un compromis «temps-mémoire»

Au lieu de vérifier si tel mot de passe correspond au hash de départ, puis de refaire la même opération jusqu'à trouver le bon sésame, le principe de rainbow table diffère quelque peu. Il s'agit d'une technique de «compromis temps-mémoire» réduisant considérablement le temps nécessaire pour casser un mot de passe. L'inconvénient, c'est qu'il vous faut générer ces fichiers rainbow tables en amont. En fonction de la complexité du mot de passe que vous souhaitez retrouver, ces derniers peuvent peser de 500 Mo à plusieurs To ! Il faut donc de la place sur un disque dur et beaucoup de temps pour les générer (comptez 3 heures pour 1Go avec un PC standard). Heureusement, vous pouvez télécharger ces tables, les acheter et bien sûr les garder pour d'autres tentatives de crack si vous avez eu le courage de les générer vous-même. Nous allons donc voir comment générer ces tables et les utiliser avec RainbowCrack, un logiciel qui en plus d'être compatible avec un grand nombre de hash, supporte le multicoeur et l'accélération graphique (le CUDA de nVidia ou le OpenCL de ATI/AMD). Pas de jaloux pour cette démonstration puisque RainbowCrack est disponible sur Windows et Linux.

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



ON AIME AUSSI !

ProduKey

> Vos clés de logiciels

ProduKey permet de facilement récupérer le numéro de licence de votre Windows, de votre pack Office ou d'autres produits Microsoft. Vous pourrez ainsi réinstaller vos produits sur un autre PC si vous en changez.

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

MessenPass

> Pour les messageries

SI vous avez un vieux PC avec des messageries un peu «old scholl» que vous voudriez récupérer, MessenPass permet de récupérer les mots de passe de MSN, ICQ, GAIM, Miranga, AOL, Piggin, AIM, Trilian, Google Talk, etc.

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

SniffPass

> Léger et tout terrain

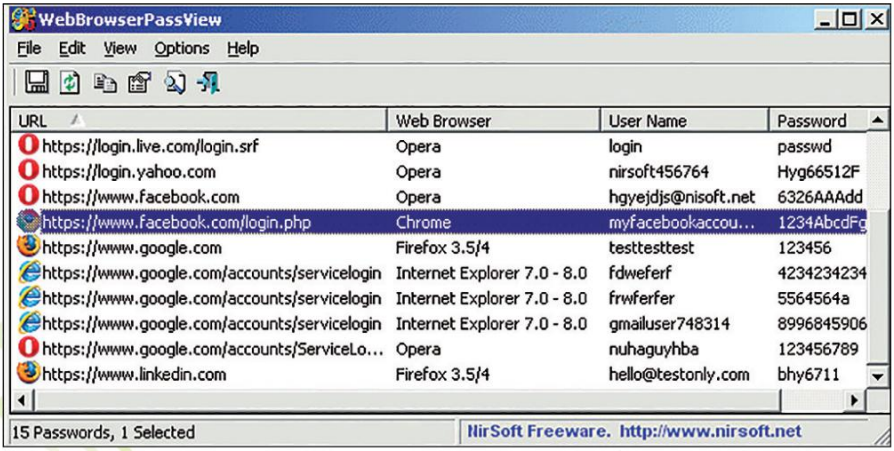
SniffPass va «sniffer» votre réseau à la recherche de mots de passe POP3, IMAP4, SMTP, FTP et HTTP. Si vous avez une connexion, mais que vous avez perdu le mot de passe, lancez le logiciel et SniffPass le retrouvera pour vous..

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

recALL → Récupération de mots de passe en local

Après l'avoir installé, recALL ira chercher des mots de passe, des codes d'accès ou des numéros de licence dans des endroits de votre Windows dont vous ne soupçonniez même pas l'existence (dossier d'installation, base de registre, etc.) Ces emplacements sont préenregistrés et toutes sortes de logiciels sont passés au crible: Windows, Office, antivirus, client mail, tous les mots de passe mémorisés par une vingtaine de navigateurs, client FTP, messagerie instantanée, logiciels commerciaux, jeux vidéo, etc. Bien sûr, les codes d'accès Wi-Fi sont compris dans le lot.

Lien : **http://keit.co/p/recall**



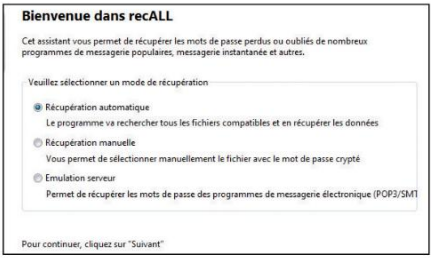
WebBrowserPassView → Pour tous les navigateurs

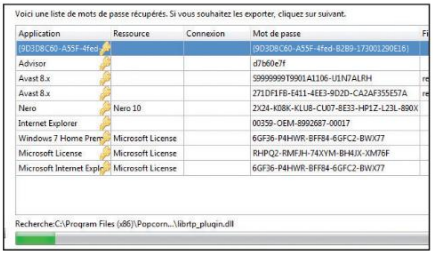
Si vous utilisez plusieurs navigateurs et que vous aimeriez récupérer les mots de passe enregistrés dans votre PC, WebBrowserPassView va faire le sale travail pour vous. Qu'il s'agisse d'Internet Explorer, de Mozilla Firefox, de Google Chrome, de Safari ou d'Opera, il suffit de télécharger le ZIP et de lancer le programme en mode administrateur. Tapez simultanément sur **Ctrl+F** pour faire une recherche, **Ctrl+A** pour tout sélectionner et **Ctrl+S** pour exporter la liste des mots de passe.

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

UN ASPIRATEUR À MOTS DE PASSE AVEC RECALL

TUTO



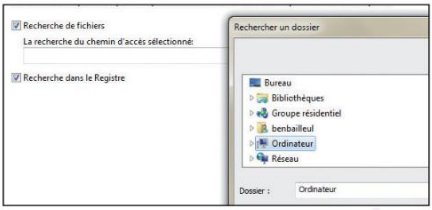


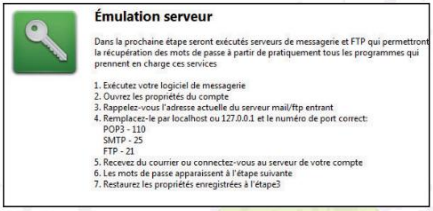
01› LES TROIS OPTIONS

En suivant notre lien, vous verrez que la page principale est en polonais mais l'interface est en français. Au démarrage, le logiciel vous propose trois options : la **Récupération automatique** qui va scanner tout votre disque dur à la recherche du moindre mot de passe, la **Récupération manuelle** qui suppose que vous sachiez dans quel dossier fouiller. La troisième option permet d'émuler un serveur POP ou FTP.

02› LES DONNÉES

Optez pour la première option et laissez le logiciel faire son travail. Cela peut prendre plusieurs minutes, mais au final, vous aurez absolument tous les sésames que contient votre PC ainsi que les codes Wi-Fi et les clés de licence. Pratique, si vous désirez formater ou migrer sur un autre ordinateur. En faisant Suivant, vous pourrez sauvegarder les résultats aux formats CSV, HTML, TXT, ZIP ou KeePass.





03› LA RÉCUPÉRATION MANUELLE

La **Récupération manuelle** est plus précise et moins laborieuse, mais il faudra que vous sachiez où trouver. Cliquer sur l'icône de dossier au bout de la barre de recherche et cochez **Recherche** dans le registre. Enfin si votre application POP, SMTP ou FTP n'est pas dans la liste de compatibilité de recALL, vous pouvez émuler un serveur de ce type pour récupérer les mots de passe.

04› ÉMULATION D'UN SERVEUR

Choisissez la troisième option, faites **Autoriser l'accès** lorsque votre pare-feu se réveillera et suivez les instructions. Il faudra faire pointer votre logiciel POP vers l'IP **127.0.0.1** et envoyer une requête (un message par exemple). RecALL va intercepter le mot de passe à la volée. Ici aussi, vous pourrez sauvegarder les résultats dans un fichier.

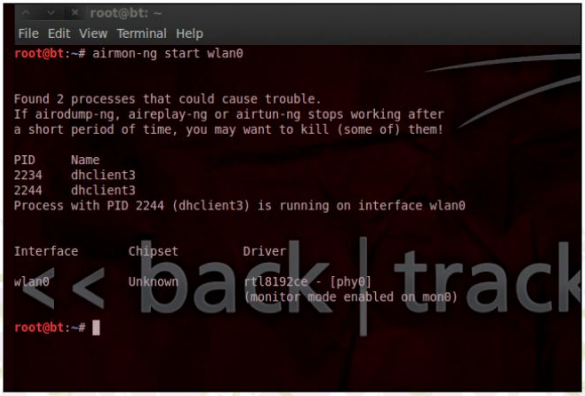
Reaver-wps → Sécurité WiFi

Si vous avez une box récente, vous êtes sans doute équipé d'un dispositif WPS. Il s'agit d'un petit bouton qui permet d'autoriser temporairement l'accès à un appareil sur votre réseau. Le but est de se connecter sans mot de passe et avec un risque très restreint puisque l'accès est refermé au bout de quelques secondes afin d'éviter les intrus. Cependant, certains appareils disposant de cette sécurité WPS connaissent une faille permettant un mode «open bar». Notez que Reaver fonctionne de concert avec Aircrack. Si l'utilisation de ce logiciel vous intéresse, voici un petit tuto en attendant notre article complet dans un prochain numéro : http://goo.gl/VsCOw8.

Lien : **https://goo.gl/QLWXN4**

Aircrack-ng → Un classique intégré à Kali Linux

Aircrack-ng est un ensemble d'outils pour l'audit des réseaux sans fil intégré à la distribution Kali Linux. Sous réserve d'avoir un adaptateur WiFi compatible avec le DPI, le logiciel va analyser les paquets de données transitant entre le point d'accès et un appareil qui tente se s'y connecter. Qu'il s'agisse d'une clé WEP ou WPA, Aircrack-ng va récupérer la clé en utilisant la méthode brute force.



Lien : **www.aircrack-ng.org**

RouterPasswords → Mots de passe de routeurs

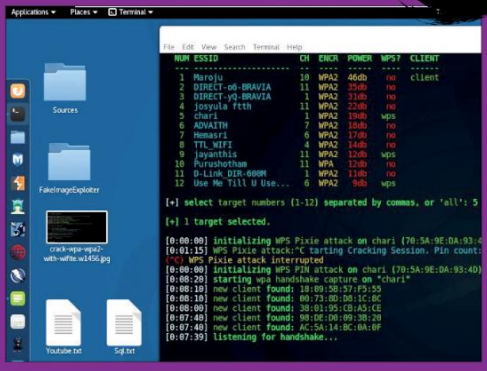
RouterPasswords.com est un site qui répertorie les mots de passe par défauts de centaines de routeurs différents. Il suffit de sélectionner la marque et le modèle pour accéder au couple identifiant/mot de passe ainsi qu'au protocole d'échange de donnée. Si vous êtes un administrateur ou que vous dépannez souvent vos amis étourdis, vous aurez donc accès aux réglages à condition que les utilisateurs n'aient pas changé les identifiants. Si vous ne trouvez pas le modèle exact du routeur que vous recherchez, essayez un mot de passe à partir d'un modèle alternatif du même fabricant !

Lien : **www.routerpasswords.com**

WiFite → Automatiser le pentest WiFi

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

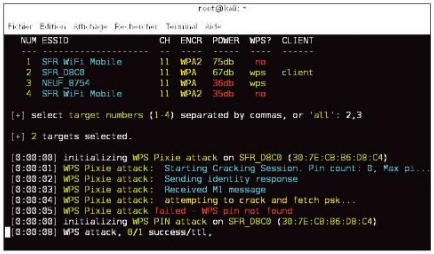
Intégré à la distribution Kali Linux, le moins que l'on puisse dire, c'est que WiFite ne fait pas de détails. Bon point : il automatise les tests de pénétration. Sous réserve d'avoir une carte Wi-Fi compatible avec l'injection de paquet, WiFite va tester les réseaux des environs et tenter de s'y introduire, qu'ils soient protégés en WEP ou WPA. Plus fort, il va même essayer de forcer l'entrée des box ou routeurs protégés par WPS. Les puristes diront que c'est un logiciel de « script kiddies » (des pirates amateurs qui utilisent des outils clés en main, sans comprendre ce qu'ils font), mais il s'agit ici de vérifier la sécurité de son réseau. Si ce dernier est perméable à WiFite, c'est que n'importe qui peut y avoir accès. Il serait donc temps de blinder la sécurité !

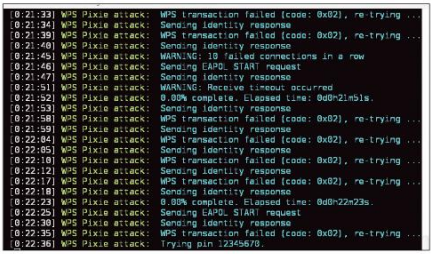


Lien : **https://github.com/derv82/wifite**

WIFITE : TESTEZ VOTRE RÉSEAU SANS FIL

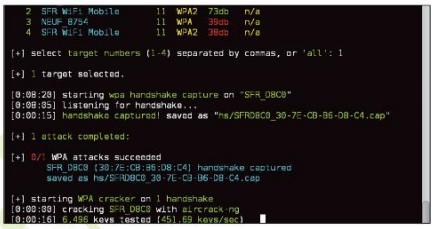
TUTO





01 LES BASES

Dans un terminal, stoppez le service network-manager pour éviter les conflits en tapant **service network-manager stop**. Faites ensuite **wifite** puis **Entrée**. Le logiciel scanne les réseaux alentour. Tapez **Ctrl+C** pour choisir les SSID à attaquer. Attention, si vous faites **all**, il ira frapper à toutes les portes ! Tapez le numéro de votre propre réseau (**Maj +** chiffre du haut du clavier) et validez. WiFite utilise Aircrack et Reaver pour pénétrer votre réseau par tous les moyens. Affinez avec les arguments.



02 WEP ET WPS

Laissons de côté le WPS, dépassé (la commande est **wifite – wep**, si jamais). Côté WPS, les points d'accès disposent de mesures de protection anti « brute force » en autorisant la saisie d'un seul PIN toutes les 60 secondes. Pas de solution miracle : il faut emprunter une adresse Mac « amie ». Cette technique étant plus complexe (Google est votre ami), nous irons au plus simple en tapant **wifite -wps -mac**. Comme plus haut, faites **Ctrl+C** pour choisir les SSID à attaquer.

03 CAPTURER LE HANDSHAKE WPA

L'intrusion d'un réseau protégé par WPA ou WPA2 est plus compliquée. Il faut capturer le « handshake », le moment où un appareil et un point d'accès Wi-Fi vont tenter de s'authentifier mutuellement. Dans le handshake se trouve le mot de passe chiffré. Une fois capturé, il prend place dans **root/hs** (regardez **Dossier Personnel**). Il faut ensuite le cracker, soit par brute force, soit par une attaque dictionnaire. Kali Linux dispose de tous les outils nécessaires.

04 ATTAQUER LE HANDSHAKE

Nous pouvons aussi demander à Aircrack d'essayer de cracker le mot de passe contenu dans le handskake, en tapant simplement **wifite -wpa -aircrack**. Ici, l'attaque a échoué. Même si le handshake a été capturé, Aircrack n'a pas réussi à découvrir le mot de passe « en clair ». Il faut dire que notre point d'accès est bien protégé ! Rien ne vous empêche d'utiliser à nouveau le handshake avec un meilleur dictionnaire ou avec un logiciel de brute force comme **John The Ripper**...

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

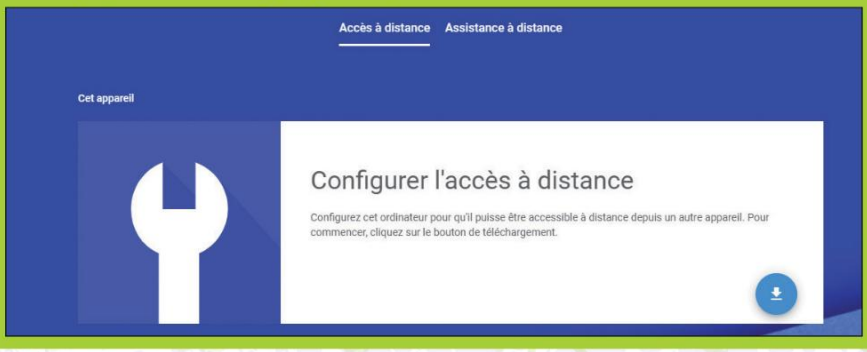
PRENEZ LE CONTRÔLE !

Pas besoin d'être un expert pour prendre le contrôle d'un ordinateur à distance ! Voici notre petite sélection...

Chrome Remote Desktop → La prise de contrôle version Google

Chrome Remote est l'idéal pour les utilisateurs débutants, ou pour ceux qui recherchent avant tout la simplicité. L'extension se télécharge dans Chrome, et il suffit d'entrer le code généré sur l'ordinateur distant pour que les deux machines soient connectées. Petit bonus : Chrome Remote est également disponible sur les appareils Android ou iOS, ce qui permet de dépanner quelqu'un ou d'accéder à votre PC du bureau même en déplacement !

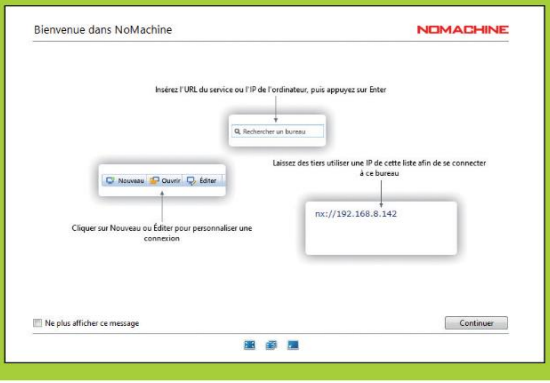
Lien : **https://remotedesktop.google.com/**



NoMachine → Multi-plateforme, maxi efficacité

Pas vraiment connu, NoMachine est pourtant une excellente solution de contrôle à distance. Gratuit et multi-plateforme, il permet de se connecter grâce à un identifiant, et de gérer plusieurs ordinateurs. Le top ? La fluidité garantie par le protocole NX, et la sécurité assurée grâce au SSH. L'utilisateur est guidé étape par étape, et peut configurer NoMachine en finesse. Un logiciel à découvrir !

Lien : **http://keit.co/p/recall**



TeamViewer → L'incontournable

Logiciel le plus connu en ce qui concerne le partage d'écran ou la prise de contrôle à distance, TeamViewer n'a plus besoin de faire ses preuves. À l'inverse d'Ammyy Admin, l'installation de TeamViewer est nécessaire sur tous les appareils que vous souhaitez utiliser. Vous pouvez également profiter des applis mobiles (sur Android et iOS) pour contrôler votre ordinateur à partir de votre smartphone.

Lien : **https://www.teamviewer.com/fr/**

VNC → Fiable et performant

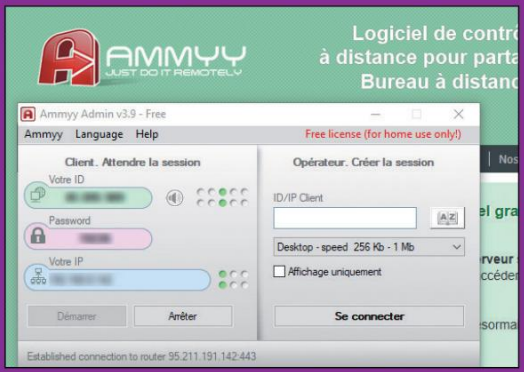
VNC est un peu le dinosaure des logiciels de contrôle à distance. Un peu moins intuitif que TeamViewer, il se rattrape en étant à la fois complet et performant. Deux logiciels doivent être installés : *VNC Server* sur l'ordinateur distant, et *VNC Viewer* sur votre ordinateur. La manipulation peut paraître lourde, mais une fois configuré, VNCse révèle extrêmement fiable et permet une prise de contrôle fluide.

Lien : **https://www.realvnc.com/fr/**

Ammyy Admin → Contrôle sans installation

Ammyy Admin existe depuis de nombreuses années, et sa simplicité en fait un outil idéal pour aider quelqu'un à distance. Aucune installation n'est nécessaire: après le téléchargement, vous lancez l'application, et c'est grâce à un identifiant que vous pourrez lier votre ordinateur à celui auquel vous voulez accéder à distance.

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

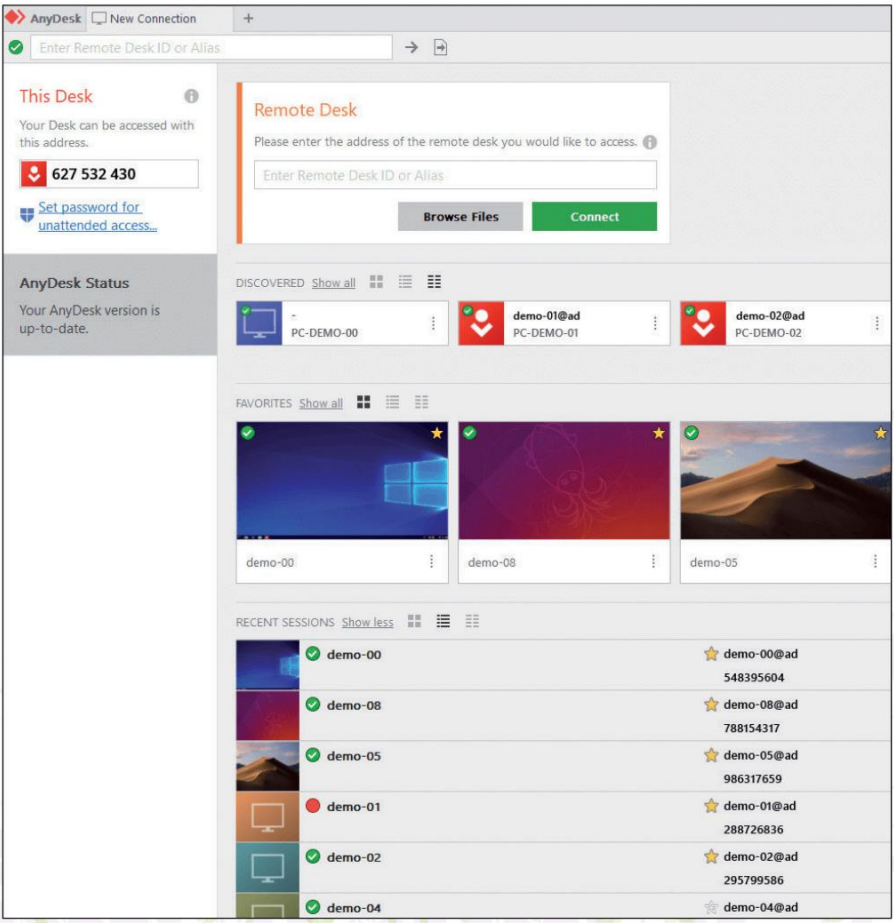


AnyDesk → Portable et réactif

Comme avec Ammyy Admin, c'est grâce à un identifiant que vous pourrez lier les deux ordinateurs. La prise en main est simple et rapide, et AnyDesk présente l'avantage d'être un outil portable : vous pouvez l'utiliser à partir d'une clé USB, et ainsi l'avoir toujours avec vous prêt à fonctionner. Il propose également des fonctionnalités intéressantes, comme l'ajustement automatique de la résolution d'écran.

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Lien : **https://anydesk.com/fr**

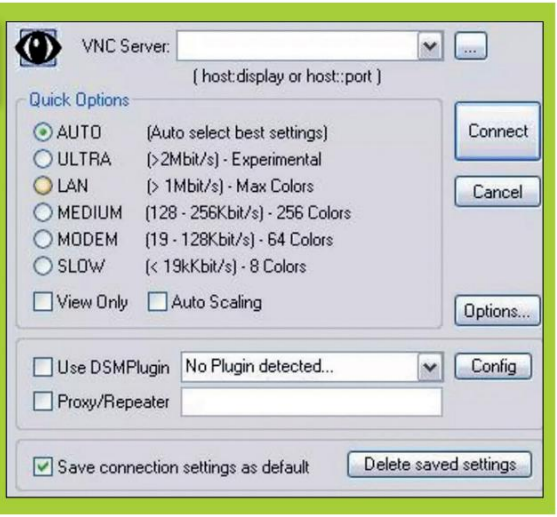


UltraVNC

→ UN LOGICIEL EN FRANÇAIS !

UltraVNC propose un module particulièrement intéressant si vous cherchez une solution ponctuelle : le Simple Clic. Il suffit de télécharger UltraVNC SC, et d'autoriser le contrôle à distance. Dès que la connexion est rompue, UltraVNCSC se désinstalle lui-même. Pas de traces, pas de risques d'une prise de contrôle non souhaitée:c'est une utilisation simple et propre d'un logiciel qui mériterait d'être plus connu.

Lien : **http://www.ultravnc.fr/**

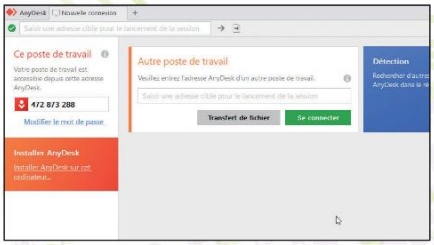


CONTRÔLEZ VOTRE ORDINATEUR À DISTANCE AVEC ANYDESK

TUTO

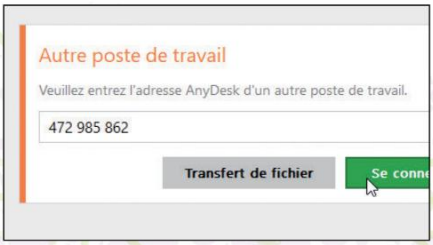
01 › LANCER ANYDESK

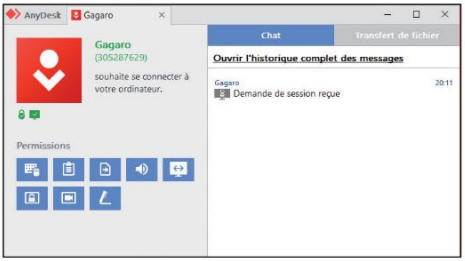
Après avoir téléchargé AnyDesk, double cliquez sur le fichier pour le lancer. AnyDesk ne nécessite pas d'installation, et est portable : vous pouvez également copier le fichier exécutable sur une clé USB, pour pouvoir le lancer sur n'importe quel ordinateur sans avoir besoin de le télécharger à chaque fois.



02 › ACCÉDER À UN ORDINATEUR À DISTANCE

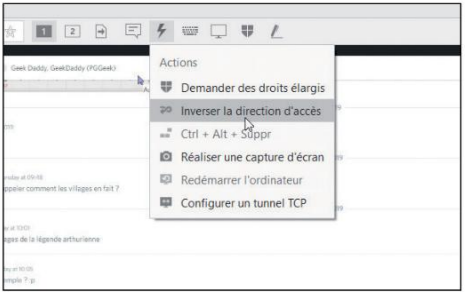
Après avoir lancé AnyDesk sur votre ordinateur, vous pourrez y accéder grâce à l'identifiant affiché en haut à gauche. Lancez AnyDesk sur n'importe quel autre PC, entrez l'identifiant dans le champ sous **Autre poste de travail**, et cliquez sur **Se connecter**.





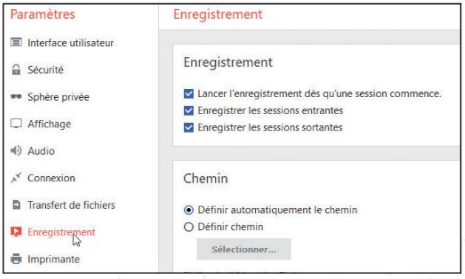
03 › AUTORISER LA CONNEXION

Lorsque vous souhaitez accéder à un ordinateur distant, ce dernier reçoit un message permettant d'autoriser ou de refuser la connexion. Il est également possible de choisir les permissions accordées pour la durée de la session. Sur l'ordinateur distant, la personne le contrôlant devra cliquer sur **Accepter**.



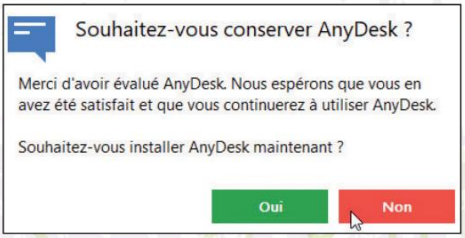
04 › INVERSER LES ACCÈS

Au cours d'une session, vous avez la possibilité d'inverser les accès : l'ordinateur contrôlé devient l'ordinateur en charge. Pour cela, cliquez sur le petit éclair dans la barre d'icônes en haut, puis sur Inverser la direction d'accès. Attendez quelques secondes l'établissement de la connexion.



05 › ENREGISTRER UNE SESSION

Pour garder une trace des actions effectuées, il est possible d'enregistrer tout ce qui se passe pendant la prise de contrôle. Pour cela cliquez sur l'icône du menu, en haut à droite, puis sur **Paramètres > Enregistrement**. Cochez **Lancez l'enregistrement dès qu'une session commence**.



06 › SUPPRIMER ANYDESK

Si votre besoin était ponctuel, et que vous ne souhaitez pas conserver AnyDesk sur votre ordinateur, le logiciel propose de lui-même de se supprimer et d'effacer ses traces. Cliquez sur la croix en haut à droite pour fermer AnyDesk, puis sur **Non** dans la fenêtre qui apparaît.

FindMyHash → Tout sur les "hash"

Le script Python FindMyHash permet de savoir à quel type de hash vous avez affaire. Pour les pirates, il suffit d'intercepter un hash dans un site Web ou une base de données pour obtenir un mot de passe valide presque à chaque coup ! Pour vous, il s'agit, bien sûr, de vérifier que votre mot de passe ne figure pas dans ces bases pour éviter les surprises... En dehors du MD5, très répandu, FindMyHash permet de trouver des hash CISCO7, LM, MYSQL, NTLM, RMD160, SHA1, SHA224, SHA256, SHA384, SHA512, etc.

Difficulté : ☠☠☠ Lien : **http://code.google.com/p/findmyhash**

CrackStation → Une base de données gigantesque

Avant de vous lancer dans des recherches compliquées lorsque vous voulez trouver un mot de passe à partir d'un hash, pourquoi

ne pas essayer CrackStation ? Ce site permet de retrouver le mot de passe correspondant à un hash en consultant des bases de données gigantesques où sont stockés des hash de tous types avec leur équivalent «en clair». Un mot de passe simple comme azerty été trouvé en quelques secondes. Lorsque vous avez un hash entre les mains, la consultation de ce genre de site doit être l'étape numéro 1.

Lien : **https://crackstation.net**

Hash_ID → Une bonne alternative

Si Hashtag ou FindMyHash ne vous ont pas séduit et que vous cherchez un autre logiciel de ce type pour comparer, voici Hash-identifier, ou Hash_ID pour les intimes. Comme les concurrents, il va analyser les suites alphanumériques pour identifier à quel type de hash vous avez affaire. Compatible avec plus de 50 sortes de hash (et leurs variantes), Hash_ID vous fera gagner un temps précieux lorsqu'il faudra lancer une attaque brute force ou dictionnaire avec John The Ripper ou Hashcat (voir les pages précédentes)...

Lien : **https://code.google.com/p/hash-identifier**

Hashtag → Le plus efficace

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

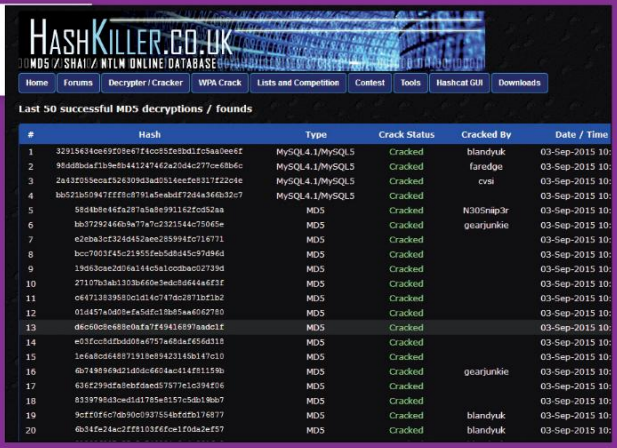
Pour cibler directement la recherche du mot de passe sur un type de hash précis, nous utilisons le script Python HashTag. Ce dernier va reconnaître l'empreinte d'un hash pour vous désigner son type : MD5, SHA, MySQL, etc. Parfois HashTag ne trouvera pas précisément le type utilisé, mais vous donnera un panel de possibilité (car certains hash sont très proches au niveau de leurs structures). C'est largement suffisant pour gagner du temps et éliminer une bonne centaine de fonctions...

```
C:\Python27>python hashtag.py -sh df6b9fb15cfdbb7527be5a8a6e39f39e572c8ddb943fbc79a943438e9d3d85ebfc2ccf9e0eccd9346026c0b6876e0e01556fe56f135582c05fbdbb505d46755a

Hash: df6b9fb15cfdbb7527be5a8a6e39f39e572c8ddb943fbc79a943
ccd9346026c0b6876e0e01556fe56f135582c05fbdbb505d46755a

[*] Keccak-512
[*] Skein-1024(512)
[*] Skein-512
[*] SHA512 - Hashcat Mode 1700
[*] sha512($pass.$salt) - Hashcat Mode 1710
[*] sha512($salt.$pass) - Hashcat Mode 1720
[*] SHA-512(HMAC)
[*] Whirlpool - Hashcat Mode 6100
[*] Whirlpool(HMAC)
[*] sha512(unicode($pass).$salt) - Hashcat Mode 1730
[*] sha512($salt.unicode($pass)) - Hashcat Mode 1740
[*] HMAC-SHA512 (key = $pass) - Hashcat Mode 1750

C:\Python27>_
```

Lien : **http://goo.gl/vQx8E9**

HashKiller → En savoir plus...

Vous voulez en savoir plus sur les hash ? HashKiller est un site qui contient une mine d'informations et d'outils sur ce sujet : des logiciels, des décrypteurs, des dictionnaires de mots et des tutos. Le site propose aussi parfois des concours et si vous ne savez pas par où commencer, vous pouvez aller sur le forum pour poser vos questions.

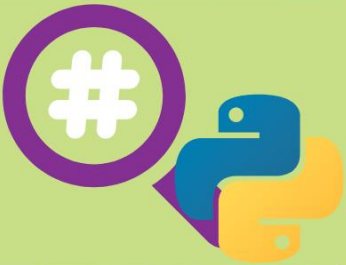


Lien : **www.hashkiller.co.uk**

TROUVEZ LE BON HASH AVEC HASHTAG.PY

TUTO

Notre but est de connaître le type d'un hash pour qu'il soit plus rapide avec Hashcat ou John The Ripper de trouver le mot de passe correspondant. En effet ce genre de logiciels ne peut cracker différents types de hash en même temps. En sachant «où regarder», vous gagnerez un temps fou !



```
#!/usr/bin/python
"""
Name:           HashTag: Parse and Identify Password Hashes
Version:        0.41
Date:           11/05/2013
Author:         Smeege
Contact:        SmeegeSec@gmail.com

Description:    HashTag.py is a python script written to parse and iden
                which consist of identifying a single hash type (-sh),
                file (-f), and traversing subdirectories to locate file
                Many common hash types are supported by the CPU and GPU
                argument (-hc) hashcat modes will be included in the ou

Copyright (c) 2013, Smeege Sec (http://www.smeegesec.com)
All rights reserved.
Please see the attached LICENSE file for additional licensing informati
"""
import argparse
import mimetypes
import os
import shutil
import string

parser = argparse.ArgumentParser(prog='HashTag.py', usage='%(prog)s (-s
argGroup = parser.add_mutually_exclusive_group(required=True)
argGroup.add_argument("-sh", "--singleHash", type=str, help="Identify s
argGroup.add_argument("-f", "--file", type=str, help="Parse a single fi
argGroup.add_argument("-d", "--directory", type=str, help="Parse, ident
parser.add_argument("-o", "--output", type=str, help="Filename to outpu
parser.add_argument("-hc", "--hashcatOutput", action='store_true', defa
parser.add_argument("-n", "--notFound", action='store_true', default=Fa
args = parser.parse_args()

hashDict = dict()

hashcatDict = { \
'MD5': '0', 'md5($pass.$salt)': '10', 'Joomla': '11', 'md5($salt.$pass)
```

```
C:\Windows\system32\cmd.exe

C:\Python27>python hashtag.py -sh 721a9b

Hash: 721a9b52bfceacc503c056e3b9b93cfa

[*] MD5 - Hashcat Mode 0
[*] NTLM - Hashcat Mode 1000
[*] MD4 - Hashcat Mode 900
[*] LM - Hashcat Mode 3000
[*] RAdmin v2.x
[*] Haval-128
[*] MD2
[*] RipeMD-128
[*] Tiger-128
[*] Snefru-128
[*] MD5(HMAC)
[*] MD4(HMAC)
[*] Haval-128(HMAC)
[*] RipeMD-128(HMAC)
[*] Tiger-128(HMAC)
[*] Snefru-128(HMAC)
[*] MD2(HMAC)
[*] MD5(ZipMonster)
[*] MD5(HMAC(Wordpress))
[*] Skein-256(128)
```

01 › INSTALLATION

Avant de commencer, il va falloir installer le langage Python sur votre machine. Préférez la version 2.7 et ne changez pas le répertoire d'installation par défaut. Téléchargez ensuite HashTag.py en suivant notre lien. En bas de la page, faites un clic droit dans le lien et faites **Enregistrer la cible du lien sous**. Placez-le ensuite dans le répertoire **C:\Python27**. Avec tout ça, vous êtes prêt ! Faites **Maj + clic droit** dans le répertoire **C:\Python27** et choisissez **Ouvrir une fenêtre de commandes ici**. Il faudra alors taper **python hashtag.py -sh [votre hash]**.

02 › LA RECHERCHE

Lors de notre premier essai, nous n'avons pas eu de chance, car le hash choisi pouvait potentiellement être d'une vingtaine de types différents. Dans ce cas, il vaudra mieux commencer la recherche par les plus fréquents. Notre deuxième essai a été plus concluant puisqu'en excluant les variantes, HashTag nous a permis de réduire le champ de recherche à 4 types de hash différents ! Nous savons ici que cette suite alphanumérique a de grandes chances d'être un SHA-512.

BIDOUILLEZ WINDOWS

Il vous manque un petit quelque chose dans Windows ? Personne n'est parfait et surtout pas l'OS de Microsoft mais on peut toujours utiliser des «tweak» pour customiser son expérience...

CustomizerGod

→ LE DIEU DES ICÔNES

Les icônes de Windows vous ennuient ? CustomizerGod est là pour laisser libre cours à vos envies. Compatible Windows 10, 8 et 7, ce logiciel vous permet de modifier l'apparence de toutes les icônes de votre système d'exploitation. Du menu Démarrer, en passant par la souris, la date et l'heure, le volume, la batterie, les possibilités de personnalisation sont légion. Pas besoin d'être un pro de l'informatique, tout se fait le plus simplement du monde.

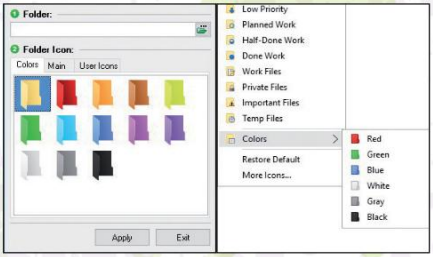
Lien : **www.door2windows.com/customizergod/**

Folder Market

→ POUR DES DOSSIERS HAUT EN COULEUR

À l'heure du travail collaboratif, les dossiers peuvent se multiplier à vitesse grand V et il peut vite devenir compliqué de s'y retrouver. Folder Market vous permet tout simplement de "coloriser" vos dossiers pour les différencier plus facilement. Une trouvaille absolument fantastique pour votre productivité. Il est par ailleurs possible de fixer un niveau de priorité à chaque dossier, comme haute-priorité, basse-priorité, privé ou encore important. La version payante vous autorise même à changer les icônes des dossiers, pour un classement encore plus efficace.

Lien : **http://foldermarker.com/en/folder-marker-free/**



Rainmeter → LA JOIE DE LA CUSTOMISATION

La fonction première de Rainmeter est on ne peut plus simple : afficher des modules divers d'informations sur votre bureau, pour suivre par exemple la place disponible sur votre disque dur, ou encore votre vitesse de connexion Internet. Ce qui rend Rainmeter unique, c'est sa façon de le faire. Ces petits modules sont modélisés sous forme d'objets, et autant dire que les skins utilisés sont très, très classes ! Les montres notamment, utilisées pour remplacer l'horloge classique, sont à tomber par terre. De quoi transformer un bureau tristounet en joyaux de la couronne.

Lien : **www.rainmeter.net**

Tweak Now Power Pack → UNE ROLLS AUX ALLURES DE 2CV

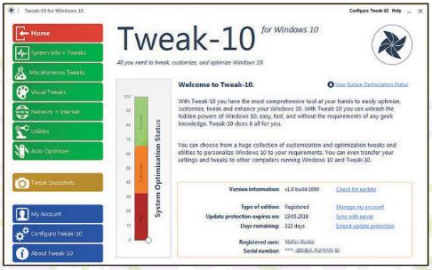
Au premier abord, Tweak Now Power Pack ne donne pas vraiment envie, avec son austérité rappelant les pires logiciels des années 2000. Et puis en cherchant un peu, on se rend vite à l'évidence : ce logiciel gratuit est un petit bijou de personnalisation, avec un nombre ahurissant de fonctionnalités : fixer un redémarrage automatique quotidien, optimiser l'utilisation de la RAM, créer entre un et quatre bureaux virtuels pour switcher selon vos envies et l'activité du moment (gaming ou working par exemple), sans oublier un accès à plus d'une centaine de paramètres cachés Windows. Un must-have.

Lien : **www.tweaknow.com/PowerPack.php#close**

Tweak-10 → POUR UN WINDOWS 10 AU TOP DE SA FORME

Tweak-10 est comme son nom l'indique réservé uniquement au dernier système d'exploitation en date de Microsoft. Son action est principalement portée sur l'optimisation de votre PC. Pour le garder en forme, le soft embarque un nettoyeur de système et de registre, un optimiseur de mémoire, un défragmenteur ou encore un moniteur intégré pour avoir un accès instantané et permanent aux performances de votre bécane. Bonus appréciable : la possibilité de jouer avec le design de Win10, au cas où certaines choses vous déplairaient.

Lien : **www.totalidea.com/products/tweak-10**



Taskbar Tweaker → LE ROI DE LA BARRE DES TÂCHES

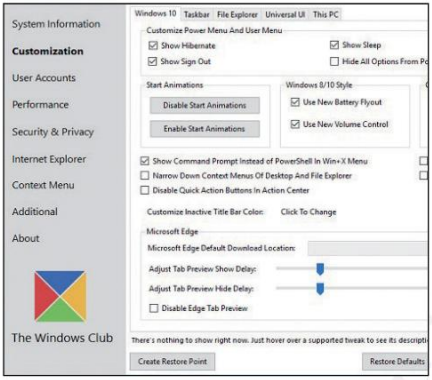
Vous cherchez à remodeler en profondeur votre barre des tâches ? Taskbar Tweaker est le maître en la matière. Traduit majoritairement en français, ce logiciel permet par exemple de modifier le comportement des éléments présents dans la barre des tâches lorsque l'on clique dessus ou lorsqu'on les survole. Il est surtout possible de réorganiser l'ordre des applications pour une efficacité optimale. D'autres fonctionnalités viennent compléter l'offre de ce Tweaker, comme le contrôle du volume avec la molette directement via la barre de tâches.

Lien : **https://rammichael.com/7-taskbar-tweaker**

Winaero Tweaker → POUR TOUT FAIRE. TOUT SIMPLEMENT

Vous pouvez comparer Winaero Tweaker à Wikipédia. Les options offertes par ce tweak tool sont infinies, à un tel point qu'il serait impossible de toutes les lister dans ce magazine ! Mais puisque nous sommes gentils, voici un petit ramequin, vous vous en ferez une idée : modifier la transparence et la dimension des fenêtres, changer les couleurs et la taille des menus, les animations de chargement, compresser les icônes, etc. Rajoutez à tout ça une compatibilité Windows 10, 8 et 7 et vous avez l'un des logiciels gratuits de tweak les plus performants du moment.

Lien : **https://winaero.com**



Ultimate Windows Tweaker → LE POIDS PLUME DES TWEAKERS

Avec 495 Ko au compteur, Ultimate Windows Tweaker est l'un des logiciels de tweak les plus légers du marché. Léger peut-être en poids, mais pas en fonctionnalités ! Il offre près de 200 outils pour modifier votre OS à votre guise. Les champs d'actions sont variés : tweaks dédiés à la sécurité, à la confidentialité, aux performances, aux fonctions de recherche, etc. Pas suffisant ? Pourquoi changer toute l'apparence de votre bureau ? Ultimate Windows Tweaker le fera pour vous. Seul bémol, le logiciel n'est qu'en anglais.

Lien : **https://frama.link/Da_h_fVf**

Windows File Tools → Surveillez l'activité

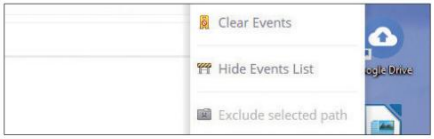
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

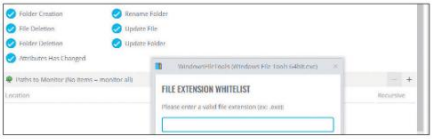
Créé par la société française Phrozen, Windows File Tools est un logiciel dans la continuité de ce qu'était Windows File Monitor. Le principe est le même qu'avant, Il s'agit de surveiller les activités des fichiers en temps réel en générant une arborescence d'événements. Une fois lancé, le programme va enregistrer les événements suivants : création, modification, mise à jour et suppression de fichier ou de dossier. Le but d'un logiciel de ce type est à la fois de surveiller l'activité d'un PC lorsque vous n'êtes pas présent (PC de travail, à l'école, etc.), mais aussi de regarder de près ce qu'un malware pourrait déclencher comme modifications sur votre ordinateur. Pour éviter de se retrouver avec des tonnes d'informations dans les journaux, on peut bien sûr filtrer les événements, les chemins spécifiques à surveiller, des extensions de fichiers spécifiques (mode liste blanche).

Lien : **www.phrozen.io/freeware/windows-file-tools**

COMMENT FONCTIONNE WINDOWS FILE TOOLS ?

TUTO



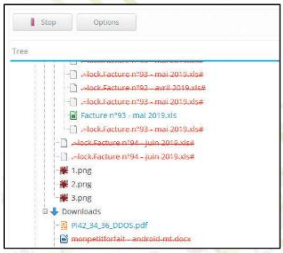


01 › PREMIER PAS...

Le logiciel ne nécessite pas d'installation, mais il requiert des droits administrateur. Dans l'archive, vous trouverez une version pour les OS 32 bits et une autre pour les systèmes 64 bits. Après le démarrage, cliquez dans le menu Phrozen pour passer au français si vous le désirez.

02 › OPTIONS ET FILTRES

Pour démarrer le suivi et l'enregistrement de l'activité dans le journal, vous pouvez faire **Start**, mais avant, allons faire un tour dans les options. Ici vous pourrez choisir quel type d'activité monitorer, mais aussi définir un chemin dans votre système (Path to Monitor) ou à l'opposé en exclure un.



03 › JOURNAL

Une fois lancée, la fenêtre du bas va afficher les modifications. Parfois, le système réagit tout seul à certaines tâches automatiques. Pour y voir plus clair, le logiciel ajoute des codes couleurs en face de chaque événement : vert pour la création d'un fichier ou d'un dossier, rouge pour un effacement, gris si un élément est renommé et bleu pour une modification ou un changement d'attribut : lecture seule, archive, fichier caché, fichier système, etc. À vous de jouer avec ces options pour trouver ce qui cloche dans votre Windows ou pour vous rassurer...

ANONYMAT & VIE PRIVÉE

p68
Chiffrez vos **DONNÉES**

p72
PROTÉGEZ vos **DONNÉES** locales

p78
PROTÉGEZ votre vie privée avec un **VPN**

CHIFFREMENT DES DONNÉES

Les meilleures adresses pour empêcher quiconque d'accéder à vos données, privées ou professionnelles, sans votre accord.

Turtl → Notes confidentielles

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

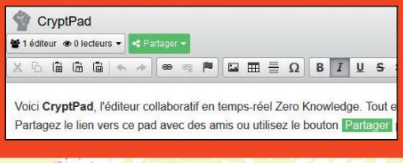
Microsoft OneNote ou Google Keep pour ne citer que les plus connus, de nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. Ce qui pose évidemment un problème de sécurité. La particularité de Turtl, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels pirates que pour les propriétaires du service lui-même.

Lien : **https://turtlapp.com**

CryptPad → Travailler en privé

Vous connaissez Google Drive, la suite bureautique collaborative de Googles? CryptPad en reprend le principe, mais de manière chiffrée. Vous obtenez ainsi un éditeur de texte, un planificateur de réunion via sondage, un éditeur de code ou encore de présentation diaporama. Décidez avec qui vous partagez les documents, et quels sont leurs droits dessus (modification ou lecture).

Lien : **https://cryptpad.fr**



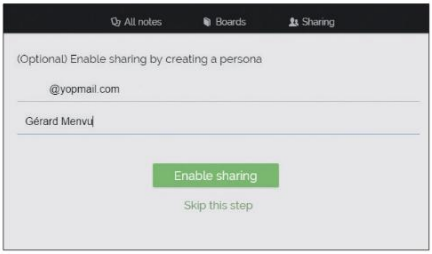
File Lock → Chiffrement express

Besoin de chiffrer un fichier rapidement ? Ne vous embarrassez pas d'un logiciel complexe et passez par le site File Lock. Importez le fichier, entrez un mot de passe (attention, il n'existe aucun moyen de le récupérer si vous l'oubliez) et validez. Pour déchiffrer ensuite le fichier, même techniques: il faut l'envoyersur le site et donner le code.

Lien : **www.filelock.org**

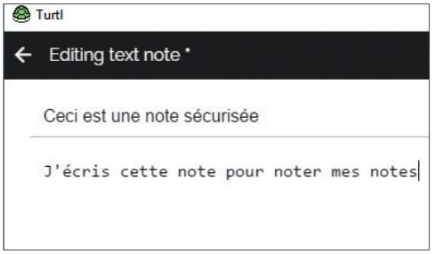
PRENEZ VOS NOTES EN TOUTE SÉCURITÉ AVEC TURTL

TUTO



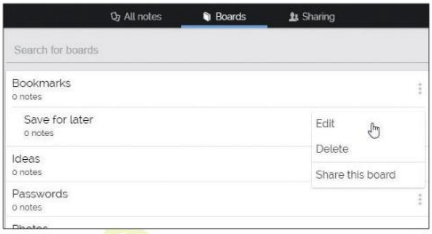
01› ACTIVER LE PARTAGE

Turtl autorise le partage de notes avec vos collaborateurs. Il vous faut activer la fonction lors de la création de votre compte. Après avoir renseigné les informations usuelles, il faudra entrer de nouveau l'adresse mail utilisée et un alias (le nom que verront les gens avec qui vous partagerez des notes). Validez avec **Enable sharing**.



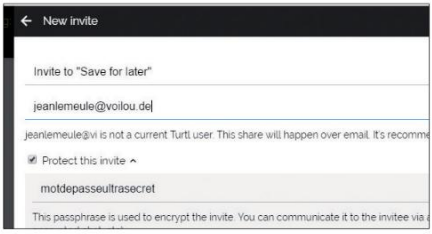
02› ÉCRIRE UNE NOTE

Cliquez sur le «s+s» en bas à droite puis sur **Text note**. Entrez un titre (**Title**) et votre texte (**Note text**). Un aperçu de la note peut être activé avec l'œil en haut à droite. Cliquez sur le crayon qui prend sa place pour quitter l'aperçu. **This note is note in any boards** permet de l'assigner à un dossier (voir étape suivante). Cliquez sur l'étiquette pour ajouter des mots-clés. Terminez avec **Save**.



03› CRÉER DES DOSSIERS

Les «sboardss» sont des dossiers dans lesquels vous pouvez ranger vos notes et fichiers. Par défaut, quatre sont disponibles, mais avec des noms anglais. Allez sur l'onglet **Boards** et cliquez sur les trois points puis **Edit** pour changer le nom. **Create nested board** sert à créer un sous-dossier. Pour créer un tout nouveau board, utilisez le «s+s». N'oubliez pas de valider avec **Edit** ou **Create**.



04› PARTAGER UNE NOTE

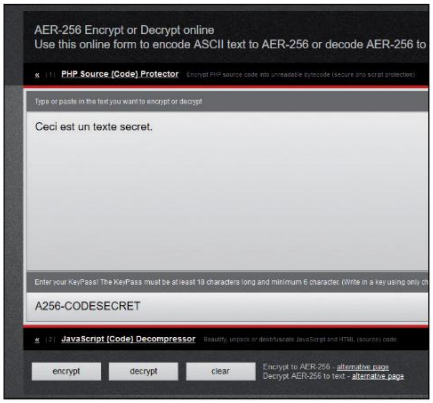
Vous partagez en fait le board contenant les notes. Allez sur l'onglet **Boards**, cliquez sur les trois points à droite de celui de votre choix puis **Share this board**. Changez le sujet du mail si besoin (par défaut **Invite to «s[nom du board]s»**) et entrez les adresses mail. Pour protéger l'accès par un mot de passe, cochez **Protect this invite**. Validez avec **Invite**.

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Boxcryptor
→ Sécurisez votre Cloud

Les documents que vous stockez sur un service en ligne pourraient tomber en de mauvaises mains. Mieux vaut chiffrer vos fichiers avant de les envoyer dans le Cloud. Pour réaliser cette opération de façon simple et rapide, essayez Boxcryptor. Celui-ci s'intercale entre votre PC et le service de Cloud, et vous propose automatiquement le chiffrage des fichiers que vous expédiez vers ce dernier. Il suffit de valider.

Lien : **www.boxcryptor.com**



Crypo
→ Pour un simple message

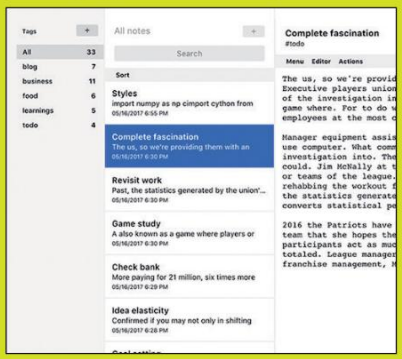
Le site crypo.com propose de chiffrer du texte à l'aide de nombreuses méthodes, plus ou moins populaire (comme le morse). Choisissez-en une, en vous assurant qu'elle comprend un champ pour entrer une clé de décryptage, puis saisissez le texte avant de cliquer sur **encrypt**. Pour déchiffrer le message, le destinataire devra se rendre sur la même page que vous, coller le texte codé, taper la clé que vous lui aurez communiquée, et valider avec **decrypt**.

Lien : **www.crypo.com**

Standard Notes
→ Notes sécurisées

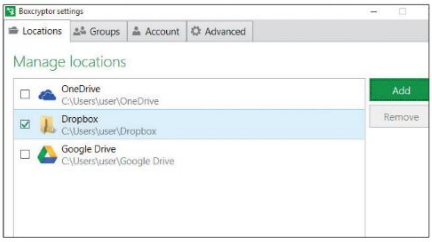
Si Turtl, présenté dans les pages qui précèdent, ne vous convient pas, mais que le concept de notes sécurisées vous intéresse, essayer Standard Notes. Plus simple, même si moins complet dans sa version gratuite, le service chiffre toutes les notes stockées en son sein de sorte que même les créateurs de Standard Notes ne peuvent les lire. Disponible sur toutes les plateformes.

Lien : **https://standardnotes.org**



CHIFFREZ VOTRE CLOUD AVEC BOXCRYPTOR

TUTO

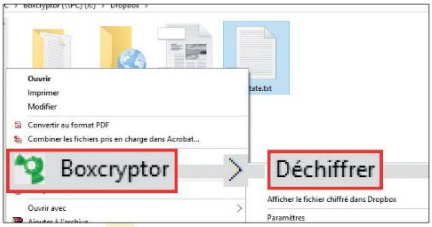


01 ANALYSER UN LIEN

Ouvrez Ordinateur, faites un clic droit sur le disque virtuel Boxcryptor puis choisissez **Boxcryptor > Paramètres**. Sous **Locations**, vous trouvez les services de Cloud disponibles sur votre PC. Si Dropbox n'y figure pas, décochez le Cloud utilisé s'il y en a un, puis cliquez sur **Add**. Sélectionnez **Dropbox** et appuyez sur **OK**. Assurez-vous que la boîte de dialogue à côté de Dropbox est cochée.

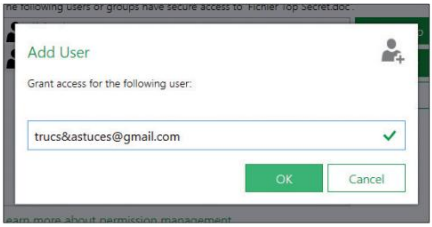
02 CHIFFRER UN FICHIER LORS DE L'AJOUT

Une fois que Boxcryptor est lié à Dropbox, vous retrouvez un dossier **Dropbox** sur le disque virtuel **Boxcryptor**. Ajoutez un fichier dans ce dossier et Boxcryptor vous demande si vous voulez le chiffrer (**Encrypt**). Votre fichier est ensuite accessible «sen clairs» via le disque virtuel, mais il apparaît chiffré sur Dropbox.



03 CHIFFRER OU DÉCHIFFRER APRÈS COUP

Dans le disque virtuel **Boxcryptor** du dossier **Dropbox**, faites un clic droit sur le fichier concerné. Dans **Boxcryptor**, apparaît l'option **Chiffrer** ou **Déchiffrer**. Dans le cas d'un chiffrement, la même boîte de dialogue qu'en étape 2 apparaît. Pour un déchiffrement, cliquez sur **Yes** afin de confirmer votre action.



04 PARTAGER UN FICHIER CHIFFRÉ

Afin d'autoriser vos contacts à ouvrir vos fichiers chiffrés, ceux-ci doivent disposer d'un compte Boxcryptor. Si tel est le cas, faites un clic droit sur le fichier et choisissez **Boxcryptor > Gérer les utilisations**. Cliquez sur **Add User** et entrez l'adresse mail des personnes. Vos contacts ont désormais accès à votre fichier chiffré via leur compte Boxcryptor.

PROTÉGEZ vos DONNÉES LOCALES !

Trupax → Chiffrez vos fichiers privés

TruPax vous permet de chiffrer vos fichiers et dossiers sensibles. Sous une interface un peu minimaliste, il s'avère simple à utiliser, puisqu'il suffit de faire glisser les fichiers ou dossiers à protéger dans la fenêtre du logiciel, avec la souris. Il suffit ensuite d'indiquer l'emplacement du conteneur chiffré et de taper un mot de passe. Bien entendu, il faut repasser par le logiciel pour déchiffrer les données.

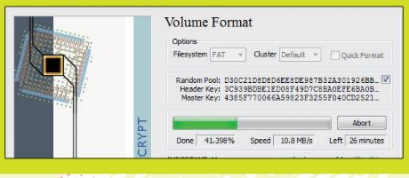
Lien : **www.coderslagoon.com**

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

VeraCrypt → La référence pour chiffrer vos données

TruPax vous permet de chiffrer vos fichiers et dossiers sensibles. Sous une interface un peu minimaliste, il s'avère simple à utiliser, puisqu'il suffit de faire glisser les fichiers ou dossiers à protéger dans la fenêtre du logiciel, avec la souris. Il suffit ensuite d'indiquer l'emplacement du conteneur chiffré et de taper un mot de passe. Bien entendu, il faut repasser par le logiciel pour déchiffrer les données.

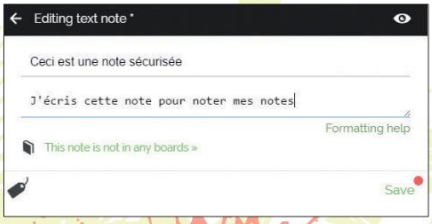
Lien : **www.veracrypt.fr**



Turtl → Prise de notes sécurisée

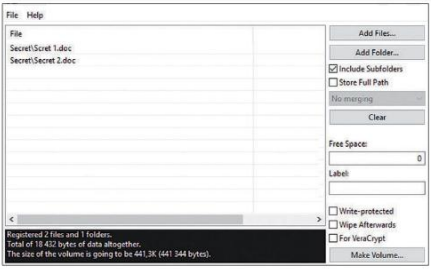
De nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. La particularité de Turtl, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels pirates que pour les propriétaires du service lui-même. Ce qui n'empêche pas le partage, sécurisé évidemment. Téléchargez et installez le logiciel client sur votre PC, et l'appli pour en profiter aussi sur votre téléphone Android.

Lien : **https://turtlapp.com**



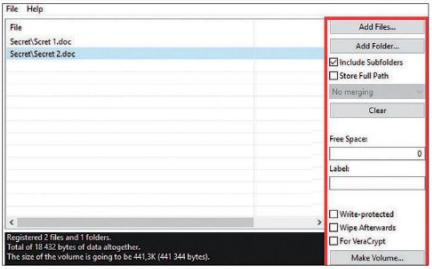
CHIFFRER FICHIERS ET DOSSIERS AVEC TRUPAX

TUTO



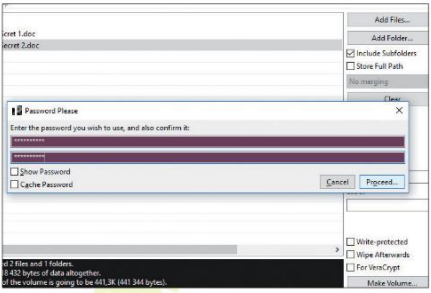
01 › DÉPOSER DES FICHIERS

Téléchargez TruPax, décompressez le dossier, et lancez **install.vbs**. Double-cliquez sur le raccourci créé sur le bureau et choisissez la langue anglaise. Faites un glisserdéposer des éléments à chiffrer dans la fenêtre principale ou cliquez sur **Add Files** (fichiers) ou **Add Folder** (dossier). Intégrez les sousrépertoires en cochant **Include Subfolders**.



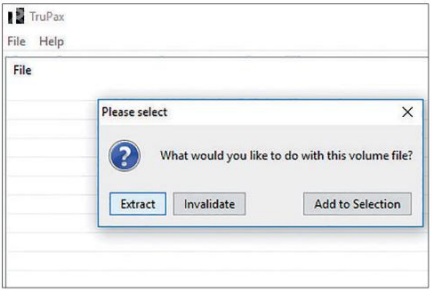
02 › COMPRENDRE LES OPTIONS

No Merging signifie que les éléments ne seront pas combinés lors du chiffrement (dans le cas où les noms des dossiers seraient les mêmes par exemple). **Free Space** permet de garder un peu de place pour ajouter des fichiers ou pour des mises à jour. Cochez **Wipe Afterwards** pour effacer les éléments qui auront été chiffrés de leur répertoire d'origine.



03 › CHIFFRER

Lorsque tout est prêt, cliquez sur **Make Volume**. Choisissez un dossier, tapez un nom pour le conteneur crypté et faites **Enregistrer**. Spécifiez un mot de passe et validez avec **Proceed**. Cocher **Cache Password** l'enregistre sur le PC pour ne pas avoir à le retaper (attention que personne d'autre n'y accède) et surtout garde le mot de passe en cas de panne.

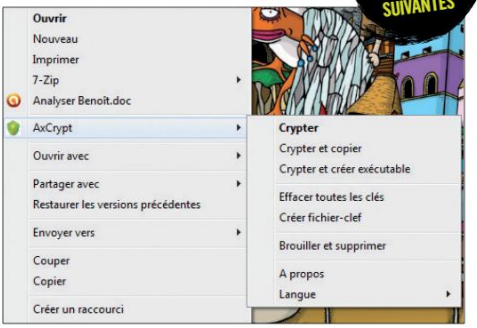


04 › DÉCHIFFRER

Vous obtenez un fichier en **.tc**. Pour le décrypter, cliquez sur **Clear** dans TruPax et glissez-déposez le fichier **.tc** dans la fenêtre. **Extract** extrait le tout, tandis que Invalidate détruit la clé, ce qui empêche quiconque (même vous) d'accéder au contenu. Utile en cas d'oubli du mot de passe. Faites **Extract**, spécifiez l'emplacement, tapez votre mot de passe et validez avec **Proceed**.

AxCrypt → Simple comme bonjour !

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

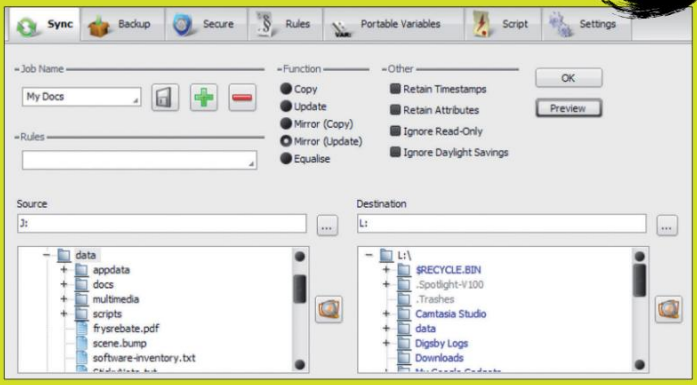


Alors que VeraCrypt propose tout un arsenal pour chiffrer vos données sensibles (création de conteneurs cachés, sauvegarde incrémentielle compactée, etc.), AxCrypt va au plus simple. Le logiciel ne comporte même pas d'interface graphique, toutes les fonctionnalités sont accessibles via le menu contextuel du clic droit. En effet, lors de l'installation, AxCrypt aura ajouté quelques entrées dans ce dernier. Il suffit de pointer un dossier ou un fichier puis de faire un clic droit pour voir apparaître : **Crypter, Crypter et créer un exécutable** et **Brouiller et supprimer**. La deuxième option permet d'envoyer un document à une personne qui ne possède pas le logiciel tandis que la troisième va effacer toute trace du fichier/dossier cible en réécrivant des données aléatoires à son emplacement d'origine.

Lien : **www.axcrypt.net/fr**

Toucan → Pour vos clés USB

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

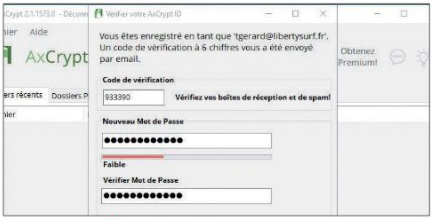


Toucan est une solution de sauvegarde pour vos clés USB ou vos disques durs externes. Avec ses modes de sauvegarde différentielle, complète ou par mise à jour, Toucan permet de créer et restaurer vos sauvegardes sous forme d'archives aux formats zip ou 7-zip. Pour sécuriser vos données, le programme ajoute un chiffrement AES-256 depuis l'onglet **Sécurité**.

Lien : **https://toucan.fr.softonic.com**

CHIFFRER FICHIERS ET DOSSIERS AVEC AXCRYPT

TUTO

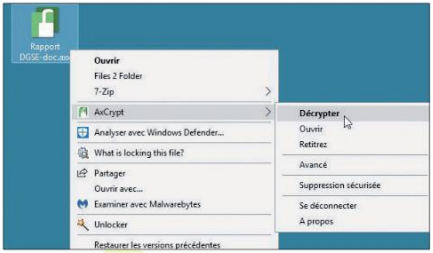


01 › DÉFINIR UN MOT DE PASSE

Installez AxCrypt, cliquez sur **Lancement**, puis activez le logiciel en donnant votre adresse mail et en saisissant le code de vérification reçu. Définissez ensuite un mot de passe solide (lettres, chiffres, caractères spéciaux), à retenir soigneusement : si vous l'oubliez, vos données chiffrées seront irrécupérables ! Un essai de la version Premium (payante) vous est ensuite proposé : pour rester à la version gratuite, cliquez sur **Passer**.

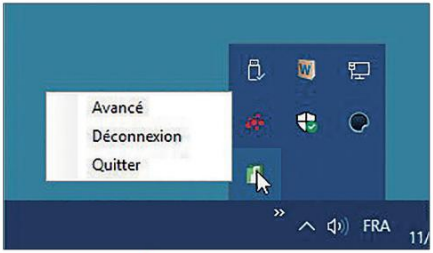
02 › CHIFFRER FICHIERS ET DOSSIERS

Vous pouvez ensuite fermer la fenêtre AxCrypt. Le logiciel reste actif en arrière-plan, comme en atteste son icône, à l'extrémité de la barre des tâches (un double-clic dessus rouvre la fenêtre). Désormais, pour chiffrer un fichier ou un dossier, il suffit de faire un clic droit dessus et de choisir **AxCrypt > Crypter**. Tant que vous restez connecté à votre compte AxCrypt via Internet, le mot de passe ne vous est pas redemandé.



03 › DÉCHIFFRER

Une fois chiffrés, les documents apparaissent sous forme d'icône AxCrypt, avec l'extension **.axx**. Il n'est pas nécessaire de les déchiffrer pour les ouvrir, un double-clic dessus suffit, comme d'habitude. Si toutefois vous désirez annuler le chiffrage d'un document, faites un clic droit dessus puis **AxCrypt > Décrypter**. Comme à l'étape précédente, le mot de passe ne vous est pas demandé tant que vous êtes connecté.

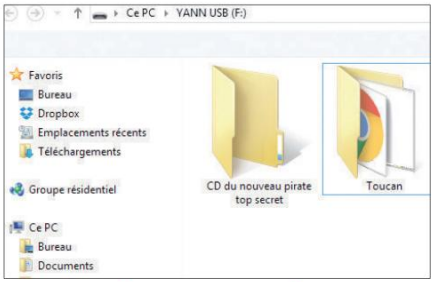


04 › SE DÉCONNECTER

Si vous arrêtez l'ordinateur, la connexion à votre compte AxCrypt est interrompue, et le mot de passe vous sera donc demandé si vous tentez par la suite d'accéder à des fichiers protégés. Mais si vous laissez votre PC en veille, ces derniers restent librement accessibles à toute personne ayant accès à la machine ! Pour éviter cela, cliquez sur l'icône AxCrypt, à l'extrémité de la barre des tâches, et faites **Déconnexion**.

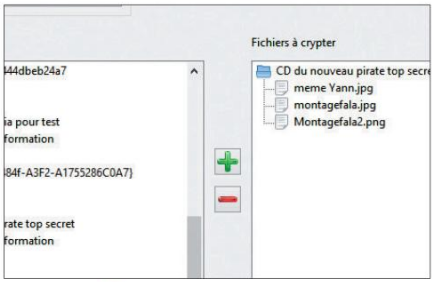
PROTÉGEZ LE CONTENU DE VOS CLÉS USB AVEC TOUCAN

TUTO



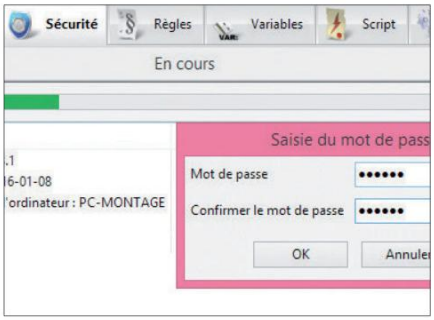
01 › PRÉPARER LA CLÉ

Téléchargez Toucan via le lien ci-contre, et double-cliquez sur le fichier récupéré. Un dossier **Toucan** est alors créé : copiezle sur votre clé USB. Puis, placez tous les fichiers à protéger présents sur la clé dans un seul et même dossier. Vous pourrez ainsi tous les crypter en une seule opération.



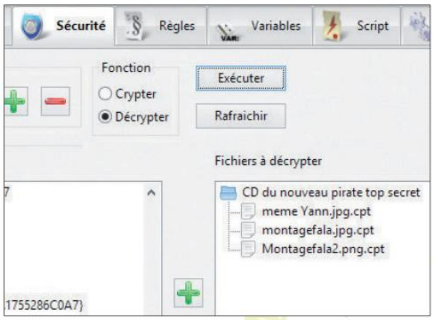
02 › SÉLECTIONNER LE DOSSIER

Ouvrez le dossier Toucan présent sur la clé, puis faites un double-clic sur le logiciel pour le lancer. Rendez-vous dans l'onglet **Sécurité**. Sélectionnez le dossier à crypter dans la colonne de gauche et cliquer sur le bouton **+** : il passe alors dans la colonne de droite.



03 › CHIFFRER LES DONNÉES

En haut de la fenêtre, veillez à ce que la mention **Crypter** (dans **Fonction**) soit cochée. Puis cliquez sur **Exécuter**. Définissez un **Mot de passe** solide, comprenant si possible des caractères spéciaux, des chiffres, des majuscules et minuscules. Confirmez et validez par **OK**.



04 › ACCÉDER AU CONTENU

Les fichiers cryptés sont désormais impossibles à ouvrir (extension de fichiers **.cpt**, illisible). Pour les déchiffrer, lancez Toucan, allez à l'onglet **Sécurité**, et répétez les étapes 2 et 3, mais cette fois-ci, cochez **Décrypter** dans **Fonction** avant de cliquer sur **Exécuter**. Tapez le mot de passe, puis cliquez sur **OK** pour rendre vos fichiers lisibles.

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

INSCRIVEZ-VOUS GRATUITEMENT !

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

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

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

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

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

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

NOUVEAU !

La rédaction se dote d'un compte Twitter !

twitter.com/ben_IDPresse

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

TROIS BONNES RAISONS DE S'INSCRIRE :

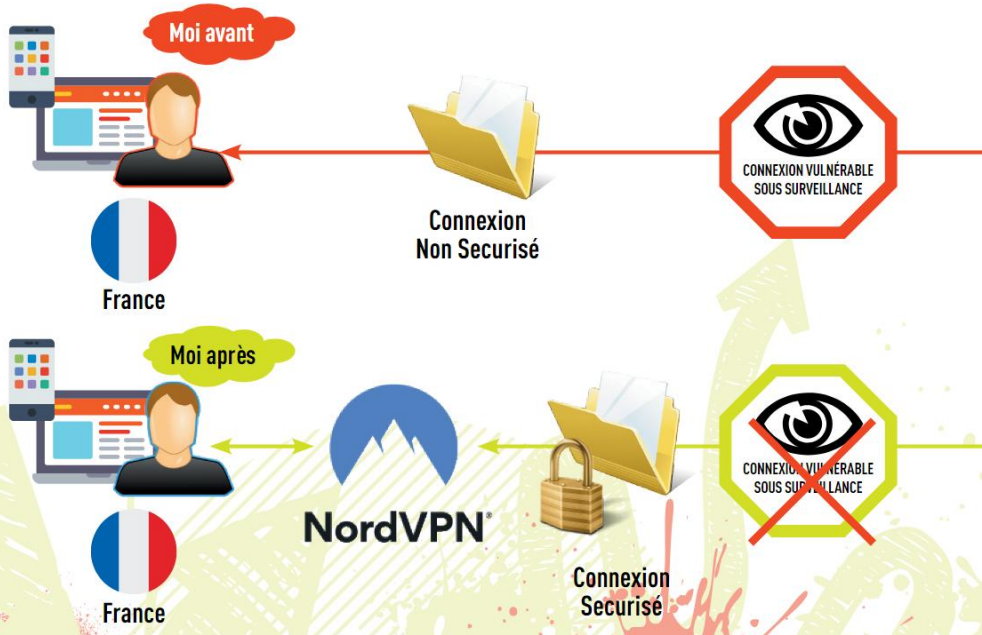
1. Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
2. Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
3. Votre adresse e-mail reste confidentielle et vous pouvez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

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

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

PROTÉGEZ VOTRE VIE PRIVÉE AVEC UN VPN

Réservés aux experts il y a encore quelques années, les VPN se démocratisent et tirent les prix vers le bas...



NordVPN → La valeur sûre

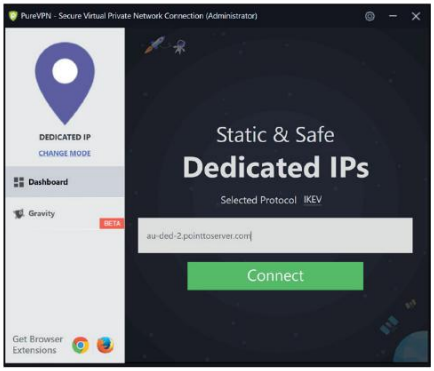
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

NordVPN fait beaucoup parler de lui en ce moment, avec une campagne de pub très agressive. Et il tient ses promesses, avec un service performant et très complet, et une interface simple et facile à prendre en main. Petit point faible : certains paramètres mériteraient quelques explications pour guider les néophytes. Heureusement, nous allons voir de quoi il retourne un peu plus loin. Notez que les prix sont dégressifs. L'offre la plus intéressante est celle qui vous fait vous engager sur 3 ans pour un peu plus de 2 € par mois. Il faudra cependant payer 94,54€ en une seule fois pour profiter de NordVPN sur cette période. Pour ce prix c'est 6 appareils que vous pouvez protéger. Vous avez de toute façon 30 jours pour vous faire rembourser si cela ne vous convient pas.

Lien : **https://tinyurl.com/y2jh7emk**

POURQUOI PAYER UN VPN ?

Bon nombre de VPN sur PC se présentent comme gratuits. Il faut voir au-delà et être prêt à se délester de quelques euros pour profiter réellement des services rendus par un VPN. Dans la plupart des cas, un VPN gratuit vous donne accès à un volume limité de données par jour (on ne fait pas grand-chose avec 500 Mo de trafic), le tout sans choix de serveur ou avec l'illusion du choix. Si les VPN sérieux sont payants, il y a bien une raison. En souscrivant à certaines offres gratuites, ne soyez pas surpris de voir de la pub apparaître dans l'interface du VPN. Dans le pire des cas, la grande majorité des VPN revendent vos coordonnées directement… un comble pour un service censé garantir votre anonymat. Sachez également que les VPN gratuits sont souvent saturés. Si vous comptez utiliser régulièrement un service de ce type, mieux vaut passer à la caisse.



PureVPN
→ L'outsider qui fait parler de lui

C'est une entreprise basée à HongKong qui se cache derrière PureVPN, le concurrent direct et acharné de NordVPN. Et elle se donne les moyens de ses ambitions, notamment grâce à l'ajout fréquent et rapide de nouvelles fonctionnalités. Un paramétrage par type d'usage, des serveurs spéciaux pour accéder aux replays des chaînes étrangères, des ping-tests... Les possibilités sont vastes ! Le prix ? 62,04€ pour un an, 71,28€ pour 2 ans.

Lien : **https://www.purevpn.fr**

CyberGhost
→ Rapide et efficace

Légèrement derrière NordVPN et PureVPN, CyperGhost est l'un des piliers sur le marché des VPN. Avec une interface intuitive et jolie, mais également parfaitement traduite, il a tout pour séduire ! Son point fort ? Des serveurs dédiés au streaming, spécialement optimisés

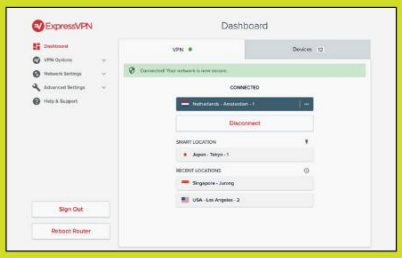
pour visionner les contenus en ligne sans ralentissements. Comme partout, la qualité se paye : 63,48€ pour un abonnement d'un an, ou 88€ pour un abonnement de 3 ans.

Lien :
https://www.cyberghostvpn.com/fr_FR/

ExpressVPN
→ Simplicité et sobriété

Comme son nom l'indique, le point fort d'ExpressVPN, c'est la vitesse. Tous les tests l'affichent en haut du tableau sur ce critère. En revanche, vous ne trouverez pas de tri des serveurs en fonction du type d'usage, et si l'interface est sobre, il faudra fouiller un peu pour trouver votre bonheur. Pour contourner cela, ExpressVPN incite à installer les extensions navigateur, et ainsi ne pas avoir besoin du client. ExpressVPN est à 99,84€ pour un an.

Lien : **https://www.expressvpn.com/**



VyprVPN → La qualité Suisse

VyprVPN peut paraître un peu léger : pas de type de serveurs par usage, impossible de choisir un serveur en particulier dans un pays... Alors quels avantages ? Une interface en français, des fonctionnalités détaillées explicitement, et des serveurs rapides. Un audit externe a également confirmé que VyprVPN ne conserve pas les données de ses utilisateurs : hourra pour l'anonymat ! Comptez 47,50€/an pour le forfait de base, 65€/ an pour le premium.

Lien : **https://www.vyprvpn.com/fr**

HideMyAss ! -> Le VPN d'Avast

HideMyAss ! c'est le VPN qui fonctionne, littéralement, en 3 clics. À l'ouverture : un bouton de connexion, et 3 onglets pour choisir son type de serveur. Pas de fonctionnalités avancées ici, de paramétrages sans fin, ce VPN va droit au but et simplifie la vie de ses utilisateurs. Dans la moyenne haute des tarifs, l'abonnement d'un an vous coûtera 71,88€, et celui pour 3 ans 143,64€.

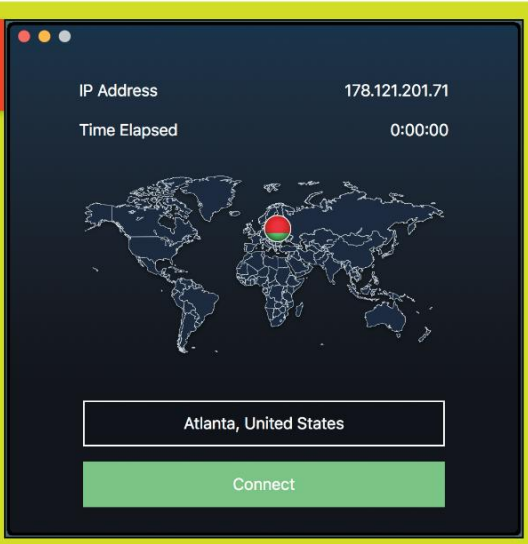
Lien : **https://www.hidemyass.com/fr-fr/index**

IPVanish → L'AVANTAGE DE L'ÂGE

Lancé en 2012, IPVanish est l'un des plus anciens VPN, et c'est ce qui fait sa force. Un peu déroutant au premier lancement, IPVanish propose une interface très complète cachée dans des onglets et des fenêtres. Le petit plus ? Un volet affichant en temps réel la vitesse de download et d'upload du serveur auquel vous êtes connecté. Un abonnement d'un an est facturé 78€.

Lien : **https://www.ipvanish.com**

StrongVPN → L'ANONYMAT SANS EFFORT



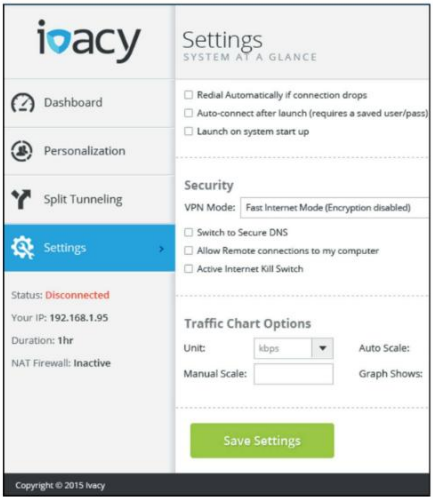
Le crédo de StrongVPN, c'est la sobriété. Une carte du monde, un bouton pour choisir son serveur, un autre pour s'y connecter. Il s'adresse essentiellement aux utilisateurs souhaitant protéger leur vie privée : avec plus de 650 serveurs, StrongVPN propose pas loin de 60 000 adresses IP. De quoi se fondre dans la masse sans effort ! Avec un prix plutôt attractif (70€/an), et une licence valable pour 12 appareils en simultané, StrongVPN a de quoi séduire.

Lien : **https://strongvpn.com**

Ivacy → Le VPN à petit prix

Ivacy s'est autoproclamé «Le plus avancé des VPN». Et effectivement, il possède des arguments de poids : nombreuses fonctionnalités, connexion de 5 appareils en simultané, protection contre les fuites DNS, chiffrage des données... Sécurité, protection et anonymat sont les maîtres-mots d'Ivacy. Ces avantages ne sont pas ternis par le prix puisque l'abonnement de 2 ans est à 47,99€.

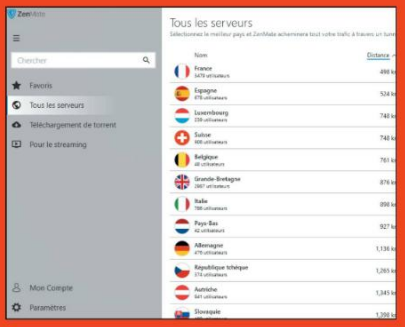
Lien : **https://www.ivacy.fr**



ZenMate → La vitesse pure

Zenmate a eu du mal à convaincre au début, à cause de ses fonctionnalités limitées. Depuis, d'amélioration en amélioration, il se fait une place, en misant sur sa simplicité d'accès pour attirer un public peu connaisseur.
Pour cela, une interface minimaliste, et une proposition de serveur dès le lancement. On lance, on clique, on surfe : difficile de faire plus simple ! L'abonnement de 2 ans est à 49,20€.

Lien : **https://zenmate.com/fr**



POURQUOI UTILISER UN VPN ?

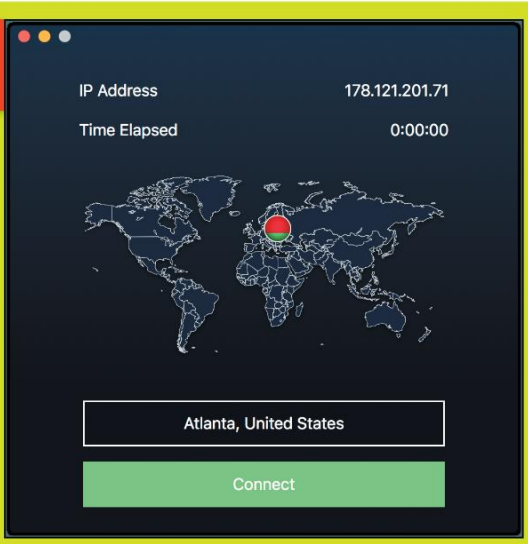
- Éviter l'espionnage et les attaques (cela va des services secrets aux pirates en passant par HADOPI)
- Protéger / Dissimuler son adresse IP emplacement géographique
- Se prémunir des malwares (virus, vers, trojans, etc.)
- Se connecter en toute sécurité sur un point d'accès WiFi inconnu
- Rester anonyme sur Internet
- Contourner la géolocalisation de certains sites et donc la géorestriction (Netflix, etc.)
- Contourner le bridage de certains sites ou services si un jour la neutralité du Net n'était plus respectée

IPVanish → L'AVANTAGE DE L'ÂGE

Lancé en 2012, IPVanish est l'un des plus anciens VPN, et c'est ce qui fait sa force. Un peu déroutant au premier lancement, IPVanish propose une interface très complète cachée dans des onglets et des fenêtres. Le petit plus ? Un volet affichant en temps réel la vitesse de download et d'upload du serveur auquel vous êtes connecté. Un abonnement d'un an est facturé 78€.

Lien : **https://www.ipvanish.com**

StrongVPN → L'ANONYMAT SANS EFFORT



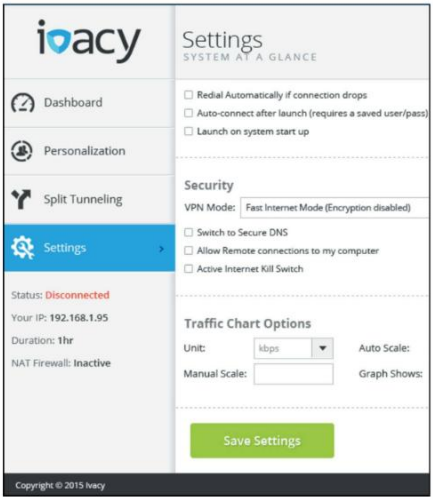
Le crédo de StrongVPN, c'est la sobriété. Une carte du monde, un bouton pour choisir son serveur, un autre pour s'y connecter. Il s'adresse essentiellement aux utilisateurs souhaitant protéger leur vie privée : avec plus de 650 serveurs, StrongVPN propose pas loin de 60 000 adresses IP. De quoi se fondre dans la masse sans effort ! Avec un prix plutôt attractif (70€/an), et une licence valable pour 12 appareils en simultané, StrongVPN a de quoi séduire.

Lien : **https://strongvpn.com**

Ivacy → Le VPN à petit prix

Ivacy s'est autoproclamé «Le plus avancé des VPN». Et effectivement, il possède des arguments de poids : nombreuses fonctionnalités, connexion de 5 appareils en simultané, protection contre les fuites DNS, chiffrage des données... Sécurité, protection et anonymat sont les maîtres-mots d'Ivacy. Ces avantages ne sont pas ternis par le prix puisque l'abonnement de 2 ans est à 47,99€.

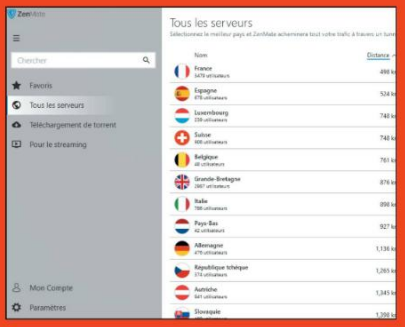
Lien : **https://www.ivacy.fr**



ZenMate → La vitesse pure

Zenmate a eu du mal à convaincre au début, à cause de ses fonctionnalités limitées. Depuis, d'amélioration en amélioration, il se fait une place, en misant sur sa simplicité d'accès pour attirer un public peu connaisseur.
Pour cela, une interface minimaliste, et une proposition de serveur dès le lancement. On lance, on clique, on surfe : difficile de faire plus simple ! L'abonnement de 2 ans est à 49,20€.

Lien : **https://zenmate.com/fr**



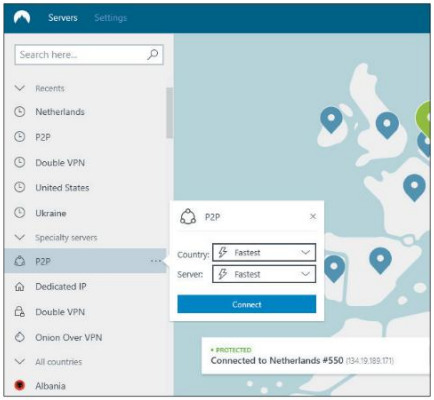
POURQUOI UTILISER UN VPN ?

- Éviter l'espionnage et les attaques (cela va des services secrets aux pirates en passant par HADOPI)
- Protéger / Dissimuler son adresse IP emplacement géographique
- Se prémunir des malwares (virus, vers, trojans, etc.)
- Se connecter en toute sécurité sur un point d'accès WiFi inconnu
- Rester anonyme sur Internet
- Contourner la géolocalisation de certains sites et donc la géorestriction (Netflix, etc.)
- Contourner le bridage de certains sites ou services si un jour la neutralité du Net n'était plus respectée

les films de hackers ! Le but est de ne laisser aucune information émanant de votre premier serveur pour le second. Le chiffrement est double aussi. Il s'agit d'une protection pour des activistes ou pour des gens particulièrement surveillés.

08› P2P

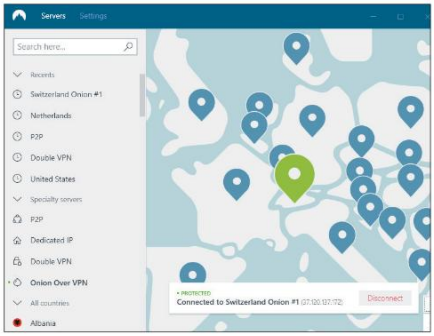
Ceux qui téléchargent via le protocole BitTorrent savent bien qu'en France, ils risquent de recevoir une...lettre. Et puis une autre...pour enfin se faire suspendre leur accès Internet.



Enfin non pas vraiment, car c'est techniquement impossible. Mais bon, si vous voulez éviter de surmener votre facteur, choisissez **P2P**. Notez que vous évitez aussi de montrer votre IP en clair sur les clients Torrent et cela gruge les FAI qui brident les protocoles P2P.

09› ONION OVER VPN

Vous connaissez Tor ? Ce système de routing permet de masquer sa position, son identité et le type de données échangées. Sur mobile Android il faut deux applis pour en profiter : Orbot et Orfox (le navigateur). Avec NordVPN, vous empruntez ce tunnel sans souci en cumulant les avantages du VPN : même



votre FAI ou d'éventuels espions sur votre réseau ne peuvent savoir que vous utilisez Tor. Ici vous n'aurez pas le choix du pays. Seuls les Pays-Bas proposent ce type de serveur.

10› DEDICATED IP

Cette option permet de vous connecter à un serveur qui va vous donner une IP statique. Il s'agit d'un paramètre très pointu. Avec une IP qui ne change jamais, vous pouvez vous connecter à un serveur pro qui dresse des listes blanches ou sécuriser vos transactions bancaires. Seul hic, une IP statique coûte 61,53€/an supplémentaires.

DES TARIFS DÉGRESSIFS

Mais combien ça coûte NordVPN ? Les tarifs sont dégressifs. Nous vous déconseillons de prendre la formule à 10,50€/mois car en s'engageant pour un an, le service revient à 6,14€/mois. Comme NordVPN propose de vous rembourser sous 30 jours si vous n'êtes pas satisfait, vous pouvez aussi opter pour l'engagement de 3 ans. Dans ces conditions, le prix est de 2,62 €/mois ce qui fait une réduction de 75 %. Voyons maintenant comment mettre NordVPN en place sur votre appareil Android, smartphone, tablette ou box TV...

NOUVEAU !

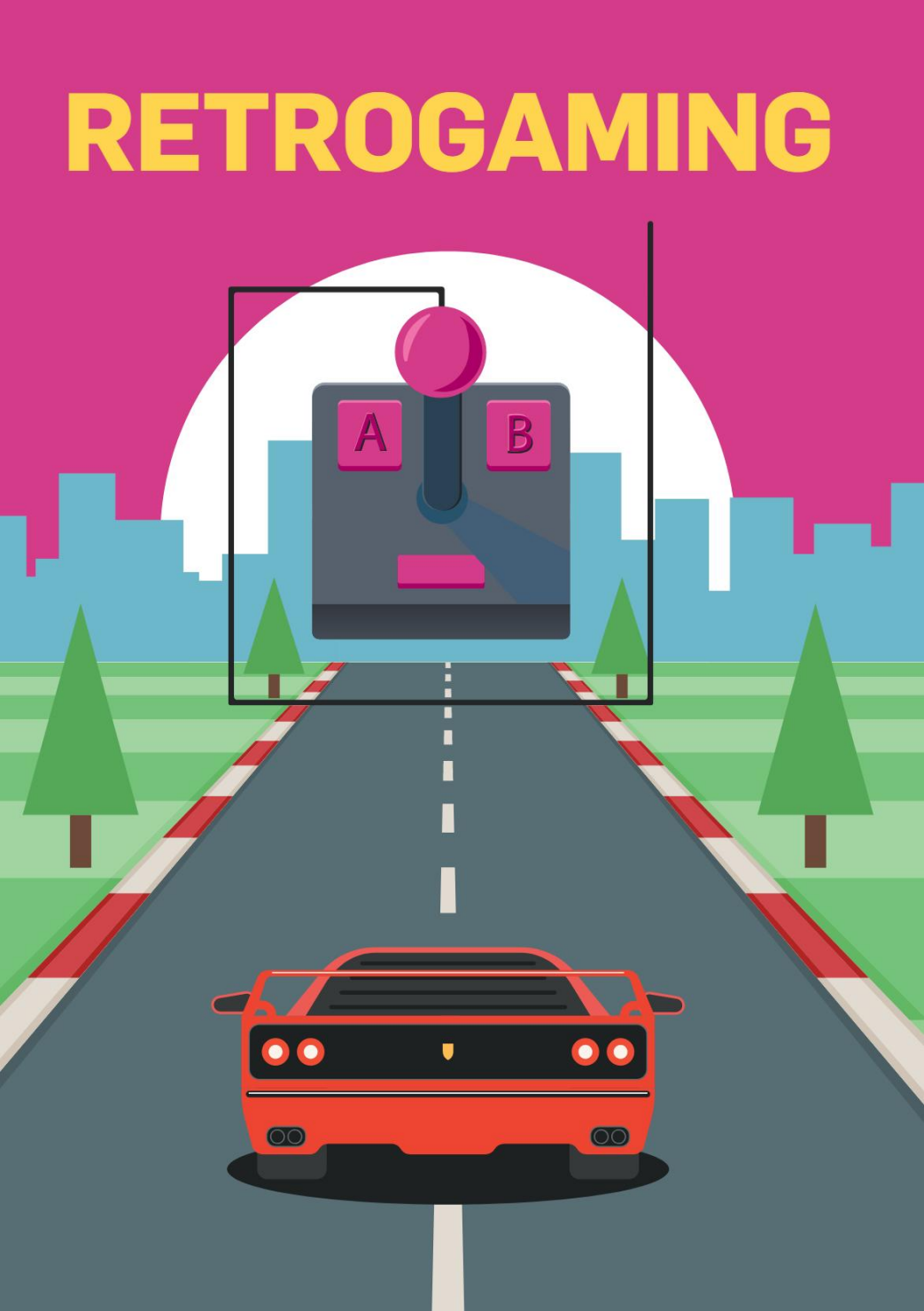
Par l'équipe de *Pirate Informatique* !

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

GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

RETROGAMING



ÉMULATION CONSOLES OU PC : LE JEU DANS TOUS SES ÉTATS

Dans cette dernière rubrique nous allons nous détendre un peu en explorant les mille facettes du retrogaming. Vous aimeriez découvrir ou redécouvrir des titres mythiques du jeu vidéo, sur consoles ou PC ? Nous allons vous présenter plusieurs solutions pour vous replonger à l'époque où «c'était mieux avant»...

Recalbox → Sur PC et Raspberry Pi

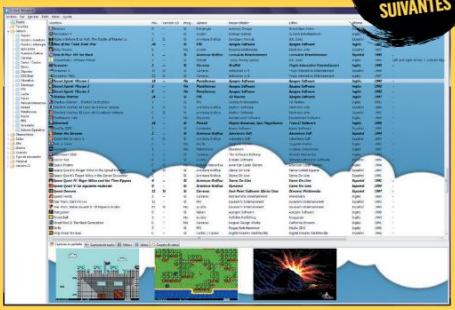
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Recalbox est un OS gratuit et libre dédié au rétrogaming. Installable facilement sur le nano-ordinateur Raspeberry Pi il est aussi compatible avec le monde PC. Il suffit d'avoir un ordinateur sous la main pour émuler une soixantaine de machines : arcade, NES, Super Nintendo, N64, Master System, Megadrive, 32 X, Mega CD, Dreamcast, PSP, PlayStation, Game Boy (Color, Advance), Game Gear, Atari 2600, MSX, Lynx, Amiga, Atari ST, Wonderswan, etc. Vous trouverez forcément votre bonheur. Le scrappeur intégré vous permettra de retrouver les descriptions et jaquettes pour chaque jeu et on trouve aussi des fonctionnalités sympas comme les «savestates» (des sauvegardes à la demande dans n'importe quel jeu), ou le «rembobinage» pour revenir de quelques secondes en arrière en cas d'erreur. Le logiciel PrBoom permet de jouer à *Doom* et à toutes les cartes amateurs au format .wad, quant à ScummVM il permet d'émuler les point'n click de LucasArts (*Day of the Tentacle*, etc.) ou Sierra (*Les Chevaliers de Baphomet*, etc.) Cela vous semble limité et vous voudriez d'autres jeux PC ? C'est possible avec l'intégration de DOSBox même s'il faudra un peu lutter. Enfin, et pour parfaire le système, Recalbox contient le media center Kodi.

Lien : **www.recalbox.com/fr**

DOSBox → Émuler du PC sur PC pour les joueurs PC

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES



Vous souhaitez ressortir vos vieux jeux PC des années 80/90 ? *Doom, Speedball 2, Discworld, Command&Conquer, Civilization, Alone in the Dark, Sim City 2000 et Wing Commander* : que de bons souvenirs... Le problème c'est que la plupart ne tourneront pas avec un PC récent. En effet, ils étaient faits pour fonctionner sous DOS, un système d'exploitation qui n'est même plus présent dans les Windows de nos jours. Alors, comment faire pour retrouver la magie de vos jeunes années ? Avec le logiciel DOSBox qui permet d'émuler le DOS de nos vieux coucous d'antan. C'est la seule solution sous Linux, mais les possesseurs de PC sous Windows disposent de D-Fend Reloaded, une interface graphique pour DOSBox plus conviviale...

Lien : **www.dosbox.com** ; Lien : **http://dfendreloaded.sourceforge.net**

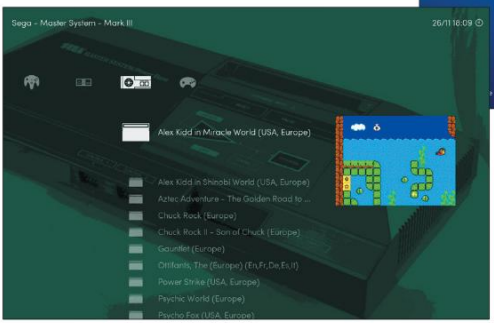
emuControlCenter → Organisez vos ROMs

emuControlCenter n'est pas le logiciel que nous conseillons aux joueurs occasionnels qui veulent se faire une partie de Mario World sur le temps du déjeuner. Il s'agit d'une interface qui va centraliser tous les fichiers (émulateurs, jeux, fichiers système, etc.) de presque 200 machines ! Et il y en a pour tous les goûts : de la calculette TI à l'Atari ST ou la GameCube en passant par la Game Boy et diverses machines d'arcade. Vous trouverez forcément votre machine de prédilection ! Les joueurs PC ne sont pas oubliés puisque vous trouverez aussi le support du logiciel DOSBox pour émuler les vieux jeux. Attention, le logiciel en lui-même ne comprend aucun émulateur et aucune ROM, il faudra les télécharger, et les transférer dans les dossiers adéquats pour en profiter. L'intérêt de emuControlCenter, c'est de pouvoir lancer les jeux depuis la même interface. Passez de *Metroid* sur Super Nintendo à *Fatal Fury Special* sur NeoGeo en deux clics puis ouvrez un logiciel Amiga ou MO5 avec la même facilité. La possibilité d'afficher des informations sur vos jeux ou logiciels avec un visuel ou une vidéo est un plus, tout comme le support des manettes Xbox360 et PlayStation 3 (via Xpadder).

Lien : **https://phoenixinteractivenl.github.io/emuControlCenter**

Lakka → Pour Windows, Linus et MacOS

Lakka est un autre compilation d'émulateur basée sur LibRetro qui propose bien sûr une version pour Raspberry Pi mais aussi des images pour Windows, Linux et MacOS. En ce qui concerne la trentaine de machines émulées, c'est du grand classique :



de l'Atari 2600 à la PlayStation en passant par la Super Nintendo, le 3DO et la Megadrive. Une alternative sympa à Recalbox qui propose aussi une compatibilité avec des «Single board computer» moins connues ou des box TV sous Android.

Lien : **www.lakka.tv**

RomStation → Ne partez plus à la pêche aux ROMs

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Pour jouer à de vieux jeux, il fallait jusqu'à présent télécharger un émulateur, des ROMs ou des ISOs (les jeux au format numérique) et lancer le tout sur votre ordinateur. Il fallait faire la même chose pour chaque système que vous vouliez émuler en cherchant des jeux sur Internet. Avec RomStation, tout va changer ! Depuis la même interface, vous choisissez, téléchargez et jouez à des milliers de jeux sans chercher, décompacter ou bidouiller quoi que ce soit. Il suffit de cliquer sur un bouton et cela fonctionne puisque tous les émulateurs ainsi que les BIOS nécessaires au fonctionnement sont intégrés dans les 188 Mo du programme. Attention, n'espérez pas émuler de la Wii avec un PC vieux de 5 ans tout de même... Une des fonctionnalités intéressantes du logiciel, c'est la possibilité de mettre en relation d'autres utilisateurs pour jouer à des jeux qui normalement ne permettent le multijoueur qu'en local. Il est donc possible de jouer à *GoldenEye 64*, *Mario 64* ou *Monster Hunter* avec des joueurs distants.

Lien : **www.romstation.fr**

INSTALLATION DE RECALBOX ET PARAMÉTRAGE

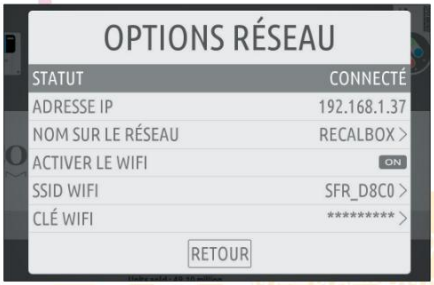
TUTO

01 › L'INSTALLATION

Démarrez le programme **SDFormatter** et formatez l'intégralité de la carte SD en FAT32. Téléchargez le fichier **recalboxOS.zip** dans sa dernière version à l'adresse suivante : **https://archive.recalbox.com**. Décompressez ensuite l'archive directement à la racine de votre carte SD ou clé USB. Placez-la dans votre PC et bootez sur ce périphérique en faisant un tour dans le BIOS. À la fin de l'installation, vous découvrirez l'écran de **EmulationStation**, le gestionnaire.

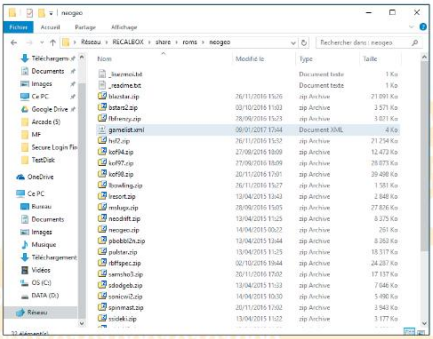
02 › LES RÉGLAGES DE BASE

Branchez un clavier pour les paramétrages. Appuyez sur **Entrée** pour accéder au menu principal et paramétrez le WiFi dans **Options Réseau** (optionnel). Les **Options Système** permettent d'ajouter un disque dur, de choisir la langue ou d'overclocker votre framboise tandis que les **Options des Jeux** vont gérer le ratio de l'image, le lissage des pixels, les filtres ou le pixel perfect (pou avoir le rendu «arcade» des vieux écrans). Le mode rembobinage sert à revenir à un stade antérieur du jeu (au lieu d'utiliser les savestates).



03 › LES DOSSIERS DE ROMS

Mais avant de s'occuper des réglages, vous remarquerez que votre gestionnaire propose déjà des émulateurs, car Recalbox est livré avec des jeux libres de droits. Et si une ROM est dans le dossier correspondant à l'émulateur, il s'affichera dans le menu EmulationStation. Pour supprimer l'affichage des émulateurs non désirés dans l'interface, il faudra juste effacer les ROMs depuis le réseau dans **\\RECALBOX\share\roms\.** C'est dans chaque dossier correspondant à un système à l'intérieur du répertoire **\roms** qu'il faudra mettre vos archives de jeu. Pour notre projet nous avons utilisé les émulateurs de la NeoGeo, des bornes d'arcade Capcom (*Final Burn Alpha* pour les systèmes CPS-I, II et III) et MAME pour les jeux très anciens ou sans système particulier (*Pac-Man*, *Mortal Kombat*, etc.)



04 › OPTIONS DES JEUX

Dans **Options des Jeux** > **Avancées** il est aussi possible de choisir quel émulateur va émuler quelle console/machine. Il est même possible d'activer certaines options uniquement pour un émulateurs: format 4/3, filtre, lissage, etc. Vous verrez en fouillant dans les menus que Recalbox est extrêmement riche au niveau des options.

L'avantage de cette distribution réside aussi dans sa notice très détaillée en français. Si vous bloquez sur un aspect que nous n'avons pas abordé, une seule adresses: **https://goo.gl/Lwbbae**

05 › RÉGLAGES DES STICKS/BOUTONS

Ce qui va nous intéresser maintenant ce sont les **Options Manettes** pour se débarrasser du clavier et gérer vos menus avec vos sticks/boutons. Normalement vos cartes contrôleur ou les branchements GPIO sont automatiquement détectés. Il suffit de sélectionner le **Joueur 1** avec le clavier et de rentrer les inputs devant chaque bouton. Notez que c'est la configuration Super Nintendo qui est ici de mise (voir l'image ci-jointe), mais qu'il est aussi possible de brancher des manettes supportant l'analogique. Si vous n'utilisez pas un bouton, il faudra rester appuyé sur un bouton au hasard jusqu'à ce que le logiciel passe à un autre.

Select permet d'ajouter des Crédits dans les émulateurs d'arcade et **Hotkey** permet de sortir d'un jeu ou de faire une sauvegarde en fonction des touches associées. Par exemple, comme nous manquions de boutons, nous avons paramétré **Select** + **Start** pour sortir d'un ému.

06 LES MÉTADONNÉES

Lorsque vous aurez transféré vos ROMs et vos ISOs depuis la carte SD ou depuis le réseau, vous pourrez y jouer directement, mais peut-être voudriez-vous afficher les visuels des jeux et leurs descriptionss? Il faudra aller dans **Scrappeur** du **Menu Principal** pour récupérer sur Internet toutes ces métadonnées depuis deux bases différentes. Cette opération peut prendre du temps. Il ne vous reste plus qu'à naviguer entre les systèmes, lancer vos jeux et profiter de cette cure de jouvence.

D-FEND RELOADED SOUS WINDOWS

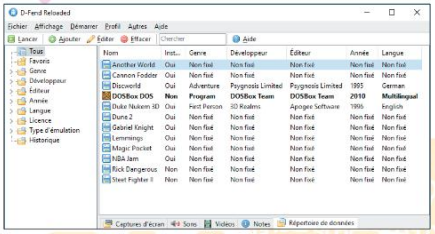
TUTO

01› LANCEMENT

La version 1.4.4 de D-Fend Reloaded comprend à l'intérieur DOSBox (v0.74). Vous n'aurez donc pas à installer ce dernier pour pouvoir jouer. Si vous êtes déjà utilisateur de DOSBox, il suffira de spécifier le chemin de votre dossier d'installation juste après la première mise en route de D-Fend Reloaded. Depuis cet **Assistant de 1er lancement**, vous pourrez aussi choisir la langue du programme, la langue de DOSBox et la recherche automatique de mise à jour.

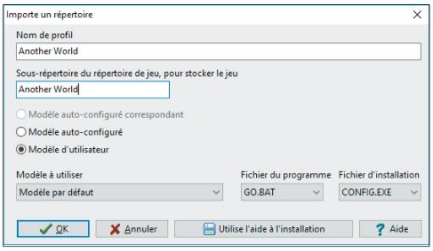
02› LES JEUX

Après avoir validé, vous allez vous retrouver sur la fenêtre principale de D-Fend Reloaded. Imaginons que vous n'avez plus les jeux en votre possession. Nous vous invitons à les télécharger sur **www.abandonware-france.org** au format archive. Notez que pour le RAR et le ZIP, il n'y aura pas de problème tandis que le 7Z, non supporté par D-Fend, demandera une étape de plus.



03› LE CHOIX DU MODÈLE

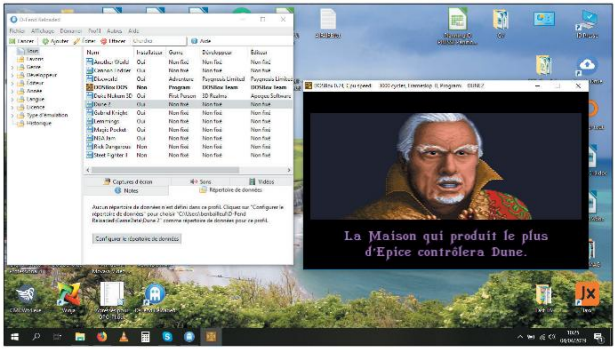
Pour commencer le paramétrage, faites juste glisser votre archive dans la fenêtre principale. Une nouvelle fenêtre va alors apparaître. Ici, vous devrez mettre le nom du jeu (dans notre exemple *Another World*) puis le nom du dossier sous lequel seront stockés les fichiers. À vous ensuite de choisir entre trois options : **Modèle autoconfiguré correspondant** si le jeu est enregistré dans la base de données de D-Fend (si cette dernière n'est pas grisée, choisissez-la), **Modèle autoconfiguré** permettant de sélectionner un jeu présentant les mêmes caractéristiques et **Modèle utilisateur** vous donnant le droit de paramétrer vos préférences à la main.



LES TYPES DE MODÈLES

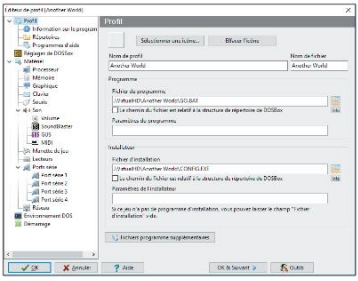
Les «modèles» sont des configurations virtuelles de vieux PC : **Normal DOS Game**, **Complexe DOS Game with 3D graphics**, etc. À vous de choisir celui qui convient le mieux pour chaque jeu si jamais **Modèle autoconfiguré correspondant** apparaît en grisé (voir étape 3). Heureusement, les jeux les plus connus sont déjà paramétrés à la base dans D-Fend Reloaded, mais si vous êtes perdu, dans **Ajouter>Ajouter à partir d'un modèle**, vous retrouverez des indications à côté de chaque modèle pour cerner au mieux vos besoins.

04› JOUEZ !



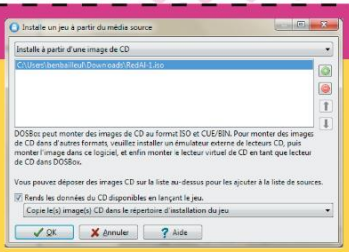
Après avoir trouvé le bon modèle, puis sélectionné le fichier programme (en **EXE**) et le fichier d'installation (généralement **Setup**), vous pouvez valider. Le jeu se retrouvera dans la fenêtre principale. Double-cliquez dessus. Le jeu se lance en plein écran. Vous pouvez revenir à un mode fenêtré avec **Alt**+**Entrée**. Notez qu'il faudra parfois lancer un fichier Setup pour que les manettes ou le son soient pris en compte dans les réglages de D-Fend...

05› CAS PARTICULIERS ET PROFIL



Si vous disposez d'un jeu qui est dans une archive du genre .7z, il faudra décompresser le jeu dans le dossier de votre choix puis faire **Ajouter**>**Ajouter à partir d'un modèle**. Choisissez le type du modèle (voir encadré) et remplissez les champs à la main (Nom, fichier programme et fichier d'installation). Si vous êtes perdu, vous pouvez aussi décompresser le 7Z pour remettre le contenu dans un ZIP et revenir à l'étape 3)... Validez pour retrouver votre jeu dans l'interface principale. Notez que vous pouvez éditer les paramètres de votre jeu en faisant un clic droit sur son profil. À partir de cette fenêtre, vous pourrez modifier le nom de profil, le fichier programme, le fichier d'installation, etc. Sur la gauche, vous pourrez changer la partie «hardware» : carte son, carte graphique, clavier, manette, etc.

ET AVEC UN VRAI CD OU UN ISO ?



Si vous avez en votre possession les jeux de votre jeunesse, il faudra agir légèrement différemment. Ajoutez votre lecteur optique à D-Fend en faisant **Ajouter**>**Installe à partir d'un média source** puis **Installe à partir d'un vrai lecteur CD** dans le cas d'un jeu CD, **Installe à partir d'une image de CD** (pour un ISO ou un couple CUE/BIN) ou **Installe à partir d'une image de disquette**. Suivez les instructions qui peuvent varier d'un jeu à l'autre...

DOSBOX SOUS LINUX

TUTO

01› L'INSTALLATION

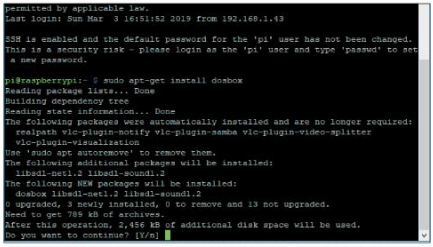
DOSBox est la seule solution pour les Linuxiens nostalgiques. Ici nous avons essayé le logiciel avec un Raspberry Pi sous Raspbian, mais le système est le même avec d'autres distributions basées sur Debian (Ubuntu, Kali Linux, etc.) Après avoir mis à jour les paquets et la distribution, installez DOSBox avec :

sudo apt-get install dosbox

Puis, créez un dossier où vous mettrez vos jeux avec :

mkdir ~/dos-games

Dans ce dossier vous pourrez mettre les répertoires contenant les fichiers de vos jeux (il faudra les dézipper auparavant). Vous pourrez ensuite lancer l'émulateur avec la commande **dosbox**, mais nous allons faire quelques petits réglages avant cela...



01› LE FICHIER .CONF

Ce fichier permet de régler plusieurs choses comme la disposition de votre clavier, la résolution, les paramètres sonores, la sensibilité de la souris, les protocoles réseau pour le multijoueur, les manettes, etc. Dans notre cas, nous allons en premier lieu configurer un clavier AZERTY et faire en sorte de «monter» le répertoire **dos-games** comme s'il s'agissait de **C:** (le disque dur principal d'un PC sous DOS). Cela évitera d'avoir à taper une ligne longue comme le bras au moment de lancer un jeu.

Lancez un terminal et faites :

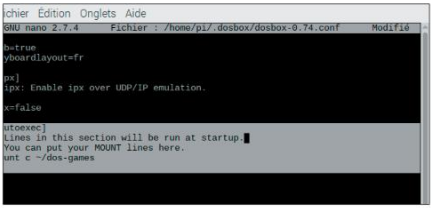
nano ~/.dosbox/dosbox-0.74.conf

À la ligne **keyboardlayout=**, mettez **fr** sans espace à la fin au lieu de **auto**. Ensuite à la fin du fichier, ajoutez les lignes :

mount c ~/dos-games

c:

Faite **Ctrl**+**X** puis **O** et **Entrée** pour valider les changements.



3/ MAPPER LE CLAVIER

Toujours dans la catégorie des réglages, vous pouvez aussi «mapper» le clavier pour le configurer à votre façon. Notez qu'il faudra pour cela laisser le mode **auto** du **keyboardlayout=**. Pour ce faire, tapez :

dosbox -startmapper

Notez que les claviers Bluetooth fonctionnent aussi avec DOSBox.

04 › JOUONS À UN JEU

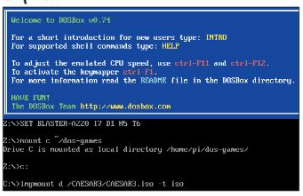
Nous sommes prêts à lancer un jeu ! Si vous avez changé le fichier .conf comme nous vous l'avons conseillé, vous devriez avoir le prompt **C:\>**. Pour DOSBox, vous êtes donc déjà dans le dossier avec les jeux. Imaginons que le jeu soit dans le répertoire **/dos-games/jeu/jeu.exe**. Il faudra taper :

C:\> jeu/jeu.exe. Si le jeu nécessite une installation, il faudra lancer **install.exe** (ou **setup.exe**) puis lancer le jeu (ne changez pas le chemin d'origine). Pour les images de CD c'est un peu différent...

05 › ET AVEC L'IMAGE D'UN CD ?

Pour les images de CD (format .img ou .iso par exemple), il faudra monter le fichier dans le lecteur **D:\>** avec :

c:\> imgmount d jeu/jeu.img -t iso
c:\> d:



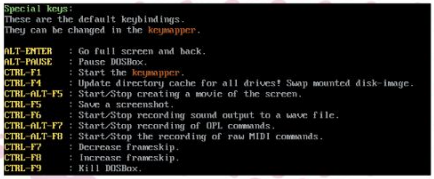
Lorsque vous verrez le prompt, il faudra taper la commande permettant de lancer le jeu. Pour être sûr de votre coup, regardez à l'intérieur de l'image pour trouver le fichier EXE qui permettra de lancer l'installation.

06 › LES SAUVEGARDES

Attention, lorsque votre jeu va fonctionner vous serez tellement content de retrouver votre jeunesse que vous allez y jouer comme si vous aviez 14, 18 ou 22 ans. Nous vous conseillons néanmoins de faire quelques essais au niveau des sauvegardes pour être bien sûr que votre progression soit bien prise en compte. Nous vous conseillons de faire une courte partie puis de relancer le jeu et de tenter de charger la sauvegarde avant de vous lancer dans 5 heures d'Ultima. Si vous avez un problème avec tel ou tel jeu, il faudra malheureusement chercher au cas par cas...

07 › QUELQUES RACCOURCIS

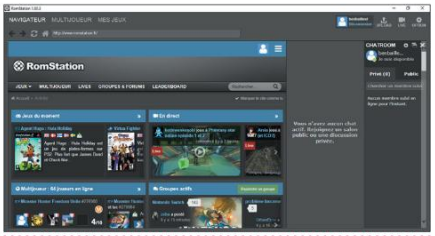
Alt+Entrée	Passer en mode plein écran
Alt+Pause	Marque une pause
Ctrl+F1	Montre le mappage du clavier
Ctrl+F5	Prend une capture d'écran (à récupérer dans le dossier Capture)
Ctrl+F6	Commencer et arrêter l'enregistrement d'un fichier sonore .wav
Ctrl+F7	Baisse le frameskip (pour ralentir les animations trop rapides)
Ctrl+F8	Augmenter le frameskip (pour accélérer les animations trop lentes)
Ctrl+F9	Fermer DOSBox
Ctrl+F10	Permet de «sortir» la souris de la fenêtre d'émulation au cas où vous devriez utiliser un autre logiciel.
Ctrl+F11	Baisse le nombre de cycles de DOSBox pour ralentir l'émulation
Ctrl+F12	Augmente le nombre de cycles de DOSBox pour accélérer l'émulation
Alt+F12	Configure tous les paramètres pour une rapidité maximum (bouton «turbo»)



COMMENT JOUER AVEC ROMSTATION ? TUTO

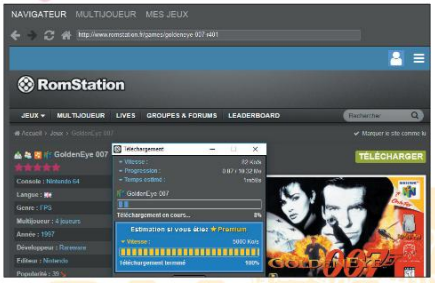
01 L'INSTALLATION

1Sur la page principale du site, cliquez sur **Installer RomStation** en haut à gauche et lancez le fichier EXE. Vous devrez sans doute installer des composants additionnels comme DirectX, mais tout se fait de manière automatique. Inscrivez-vous sur le site et validez cette inscription sur votre boîte aux lettres avant de rentrer vos identifiants dans l'application RomStation.



02 VOTRE PREMIER JEU

Choisissez votre système en cliquant sur l'icône adéquate puis recherchez un jeu. Dans notre exemple, nous allons jouer à GoldenEye 64, ce chef-d'œuvre du multijoueur local sur la N64 de Nintendo. Cliquez sur **Télécharger** et lorsque le processus sera fini, faites **Jouer**. Notez qu'il existe des versions de jeux modifiées comme le mode coopératif à 4 joueurs de Zelda : Ocarina of Time.



03 LE BON ÉMULATEUR

Si le système comporte différents émulateurs, le logiciel vous proposera de choisir

celui que vous voulez utiliser. Après avoir validé, RomStation vous propose de diffuser votre partie sur le réseau. Vous pouvez bien sûr refuser. Normalement, le jeu devrait se lancer. À vous de paramétrer l'émulateur pour qu'il s'adapte à votre configuration : manette ou clavier, qualité de la vidéo, du son, etc. Chaque émulateur propose ses propres réglages.

04 LE MULTI

Vous retrouverez les jeux que vous avez déjà téléchargés dans l'onglet **Mes Jeux**. Si le cœur vous en dit, faites un tour dans **Multijoueur**. Cliquez sur **Rejoindre** pour accéder à la partie. Notez aussi que si vous sélectionnez un jeu Star Wars par exemple, le logiciel vous proposera des jeux en rapport avec cet univers.

CHEZ VOTRE
MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS DE PASSE,
SURVEILLANCE

NOUVELLE FORMULE
68 PAGES !

BEST-OF 2019

LA TROUSSE À OUTILS ULTIME DU PIRATE

LES 80 MEILLEURS LOGICIELS ESSENTIELS & GRATUITS

IDPRESSE idpresse

L 14376 - 21 - F: 3,50 € - RD

BEL/LUX/PORT CONT. : 4,60 € - CH : 6 FS – DOM/S : 4,70 € - POL/S : 660 XPF - N CAL/S : 620 XPF - MAROC : 43 DH