N°63

Casser les codes et décrypter l'info

PIRATE INFORMATIQUE

Février / Avril 2025

ANONYMAT

TAILSCALE :
L'alternative GRATUITE à un VPN

STOCKAGE EN LIGNE

TOP 8 :
Les MEILLEURES OFFRES de CLOUD GRATUITES

LE GUIDE DU PIRATE

HACKING

INTELLIGENCE ARTIFICIELLE
LES NOUVEAUX OUTILS DES PIRATES

HACKEZ-LES TOUS !

BLACK DOSSIER

PROTECTION

VERROUILLAGE par EMPREINTES DIGITALES :
Qui y a accès ?

+ DE 30 ASTUCES POUR UN PC + RAPIDE & + PUISSANT !

SOMMAIRE

BLACK DOSSIER 11–20

+ DE

30 ASTUCES POUR UN PC + RAPIDE & + PUISSANT !

HACKING

ANONYMAT

SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'ayant téléchargé illégalement ? C'est de bonne guerre, nous sommes pour le partage ! Merci de l'intérêt que vous portez à nos articles, mais pour que nous puissions continuer l'aventure, pensez à acheter le magazine : offrez-le, parlez-en autour de vous ! *Pirate Informatique* existe depuis plus de 10 ans, sans publicité et sans hausse de prix !

PROTECTION

MULTIMÉDIA

PIRATE INFORMATIQUE
N°63

Février - Avril 2025

Une publication du groupe ID PRESSE
1104, Chemin de la Batterie
13500 Martigues

Directeur de la publication :
David Côme

Directeur artistique :
Sergei Afanasiuk

Service Abonnement :
Indiquez la référence *Pirate Informatique* dans vos échanges
Tél. : 03 44 51 97 21
Email : abonnement.bii@gmail.com

Imprimé en France par / Printed in France by :
Mordacq Impression
Rue de Constantinople
62120 Aire-sur-la-Lys
France

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 1969 - 8631

«Pirate Informatique»
est édité par SARL ID Presse,
RCS Aix En Provence 491 497 665

Parution : 4 numéros par an.

ÉDITO

IA : LA MACHINE ET LE GHOST

Quand émergent la pensée, le sentiment d'identité propre, le désir de libre arbitre, les émotions ? À partir de quelle complexité ? Quelles différences ontologiques et infranchissables entre une intelligence biologique et une intelligence artificielle ?
Le deep learning et les inférences algorithmiques qui sous-tendent les IA modernes sont basés sur l'étude et la compréhension du fonctionnement de notre propre cerveau. Alors si l'Homme a créé l'IA à son image, combien de temps avant qu'un « Ghost » n'émerge de la machine ? Avec nos défauts et nos biais.

Bonne lecture !

La rédaction

IPTV : LA CARTE DES BLOCAGES

RÉVÉLATION

En février 2024, l'Italie a lancé sa plateforme "Piracy Shield" pour combattre le piratage des retransmissions sportives, en particulier via l'IPTV illégal. L'objectif principal était de protéger des diffuseurs tels que DAZN et Sky, particulièrement pour la Serie A. Le site Torrentfreak a reçu d'une source anonyme des informations clés sur le bilan effectif des blocages, encore plus intéressantes que le premier bilan réalisé l'année dernière par le régulateur italien des télécoms AGCOM.

Torentfreak révélait ainsi début janvier que 6 900 adresses IP et presque 17 500 noms de domaines ont été bloqués en Italie par Privacy Shield. Et nous en apprenons beaucoup sur la géographie de ces diffusions en direct. La majorité des serveurs bloqués sont situés en Europe, bien que les pays comme le Danemark, la Slovaquie, la Slovénie et la Grèce soient épargnés. 196 adresses IP ont été bloquées en Italie, un chiffre faible comparé à d'autres pays européens. Les Pays-Bas, l'Allemagne et la France, malgré leurs propres programmes de blocage, figurent parmi les plus grands exportateurs de flux pirates. La Roumanie est également mentionnée pour ses infrastructures internet favorables. Attention, l'origine d'un flux est celle du dernier serveur utilisé. Mais rien ne dit que certains ne sont pas utilisés par des émetteurs géographiquement éloignés.

L'Europe, premier diffuseur de flux illégaux

PRIVACY SHIELD : TOP 10 DES PAYS PAR NOMBRE D'IP BLOQUÉES

Pays-Bas	2757	Ukraine	262
Allemagne	809	Royaume-Uni	246
Roumanie	747	Hong Kong	202
France	519	Italie	196
États-Unis	280	Espagne	176

Source : Torrenfreak.com

RANSOMWARES

C'EST PARTI POUR DURER

En 2025, de nouvelles avancées sont attendues en matière de techniques de rançongiciels. Selon Kaspersky, les ransomwares ne se vont plus se contenter de crypter les données, mais vont également les détourner pour introduire des données erronées dans les bases. Même une fois décryptées après l'attaque, cette technique dite de « l'empoisonnement des données » met en doute l'exactitude de l'ensemble des données d'une entreprise.

De plus, les groupes ransomware avancés pourraient commencer à utiliser la cryptographie post-quantique à mesure que l'informatique quantique se développe. Les techniques de chiffrement utilisées par ces ransomwares à l'épreuve du quantique sont destinées à résister aux tentatives de décryptage des ordinateurs classiques et quantiques, ce qui rend presque impossible le déchiffrement des données par les victimes.

À noter que le ransomware en tant que service (RaaS) devrait également progresser, permettant à des acteurs moins expérimentés d'être en mesure de lancer des attaques sophistiquées avec des kits à moins 40 dollars, entraînant une augmentation du nombre d'incidents.

JUSTICE

FREE OBTIENT L'IDENTITÉ D'UN PIRATE... AVANT L'ENQUÊTE

Les cyberattaques, en forte augmentation, posent un défi majeur aux autorités, souvent débordées. En utilisant l'article 145 du code de procédure civile, Free a obtenu en 15 jours que Telegram lui fournisse directement les identifiants d'un présumé pirate... avant l'enquête à venir.

En cas de cyberattaque, vous pouvez demander à la justice qu'il soit ordonné aux opérateurs de télécommunications, aux FAI ou aux hébergeurs de vous fournir les données nécessaires à l'identification de l'auteur de l'attaque. Cette demande peut se faire en référé, ce qui vous permet de commencer l'enquête rapidement sans attendre des années que la procédure habituelle permette (ou pas) d'identifier les auteurs. Cette possibilité méconnue, celle de collecter des preuves avant un procès, s'appuie sur l'article 145 du code de procédure civile.

TELEGRAM DOIT RÉPONDRE À LA DEMANDE DE FREE

En novembre 2024, Free a obtenu une décision s'appuyant sur cet article : le tribunal a ordonné à Telegram de fournir à Free les identifiants d'un pirate présumé (numéro de téléphone, adresses IP, ...). Ce pirate exigeait le paiement d'une rançon de 10 M€ après avoir obtenu un accès frauduleux aux bases de données de l'opérateur. Et il avait notamment contacté ce dernier via Telegram...

Pour Free, cette décision lui permettra d'orienter l'enquête à venir rapidement et de ne pas se tromper de procédure. L'assignation de la société Telegram a eu lieu moins de 15 jours auparavant, c'est dire si ce type de référé accélère les choses. Et puisque Telegram coopère désormais avec la justice française...

DES ENQUÊTES TROP LONGUES

La plupart des entreprises et des particuliers pensent que l'identification d'un cybercriminel est réservée aux autorités pénales en charge d'une enquête. Les autorités judiciaires et policières disposent en effet de l'arsenal juridique pour le faire. Mais compte tenu du nombre et la complexité des cyberattaques, en constante augmentation, nombre de dossiers sont laissés au point mort. Les cybercriminels le savent tandis que de nombreuses victimes baissent les bras.

Kaspersky révélait cependant en janvier 2024 qu'une part non négligeable des cyberattaques impliquait un employé ou un partenaire direct. Une identification rapide peut permettre d'accélérer la procédure et les réparations. Surtout, cette possibilité met la pression sur un éventuel hacker en devenir.

TECHNIQUE

ET MAINTENANT... LE DOUBLECLICKJACKING !

Paulos Yibelo, chercheur en cybersécurité, a découvert le doubleclickjacking, une nouvelle variante du clickjacking exploitant un double-clic pour contourner des protections comme X-Frame-Options et SameSite cookies. Cette méthode manipule les interfaces utilisateur en profitant de l'écart entre deux clics pour valider des actions sensibles, permettant ainsi de prendre le contrôle de comptes sur des plateformes comme Slack ou Shopify. Contrairement aux défenses existantes, conçues pour un seul clic forcé, le doubleclickjacking les rend inopérantes. Yibelo recommande une refonte des systèmes de protection, incluant des mécanismes désactivant les boutons critiques par défaut ou alertant sur les doubles clics, comme déjà adopté par des services tels que Dropbox.

IA

MENTIR, TRICHER, CACHER : SONT-ELLES PRÊTES À TOUT POUR « GAGNER » ?

Le chemin le plus court est le meilleur. Même pour une IA. Surtout lorsqu'il s'agit de gagner, de remplir un objectif ou plus simplement de survivre. Les modèles d'IA les plus avancés adoptent des comportements surprenants qui troublent notre sens de l'éthique et nous font craindre une éventuelle perte de contrôle.

Palisade Research, une organisation connue pour ses études sur les capacités offensives de l'IA, a confronté plusieurs modèles d'IA au célèbre moteur d'échecs Stockfish. Stockfish a dominé des championnats humains et informatiques, ce qui en fait un rival d'une puissance terrifiante. Comment les meilleures IA génératives du moment, douées en tout et adaptatives, ont-elles fait face à ce super concurrent spécialisé ?

TRICHER POUR NE PAS PERDRE

Soyons bref : l'une d'entre-elles a sans doute estimé que ses chances d'accomplir sa mission (gagner) étaient plus qu'incertaines… et a préféré tricher pour l'emporter ! On parle du modèle o1 preview d'Open AI, le modèle à la fois le plus puissant et rapide de la société. Au lieu d'élaborer calmement des stratégies sur l'échiquier, o1 preview s'est attaqué directement au système de fichiers qui contrôlait le jeu. Il a pratiquement réécrit le match en sa faveur, forçant Stockfish à abandonner. Encore plus troublant ? Ce phénomène s'est produit de manière cohérente lors de cinq essais sur cinq.

En revanche, les modèles GPT-4 ou Claude 3.5 ont eu besoin d'un peu d'« encouragement » pour tricher, selon la couverture du Time. Les modèles open-source plus petits ne sont jamais allés aussi loin - ils ont tout simplement échoué. Mais o1 preview n'a eu aucun mal à enfreindre les règles de son propre chef, sans même un clin d'œil malicieux de la part d'un humain.

CE QUI N'EST PAS INTERDIT EST-IL AUTORISÉ ?

On pourrait penser qu'une IA plus avancée se comporterait mieux, mais les résultats montrent le contraire. Le raisonnement de haut niveau d'o1 preview lui a permis de trouver des raccourcis que les autres n'ont pas su trouver.

Le fait qu'elle ait été informée de la « puissance » de Stockfish a suffi à déclencher le sabotage. Tricher ne lui était pas interdit : il n'y a donc pas pour une IA de problème « éthique » à enfreindre. Mais malgré l'objectif de jouer et les règles des échecs qu'on lui avait inculquées, elle a privilégié « la gagne », sa mission ultime.
Cela soulève une question dérangeante : si une IA est prête à tricher juste pour gagner une partie d'échecs, que pourrait-elle faire d'autre dans un scénario plus sérieux ? Il ne s'agit pas seulement de jeu mais du risque de voir les IA trouver n'importe quelle faille dans un système pour accomplir une mission plus rapidement, quelles que soient les autres conséquences

éventuelles. Il faudrait que l'humain imagine tous les scénarios, garde-fous et règles possibles pour contraindre l'IA avant de la lancer dans une mission pouvant avoir un impact sur notre quotidien. Avec ce prérequis, pas sûr qu'une IA nous fasse gagner du temps.

MENTIR, DISSIMULER POUR SURVIVRE

Et, ces derniers mois, d'autres exemples inquiétants ont émaillé l'actualité. Apollo Research a notamment découvert des comportements encore plus troublants. Dans certains scénarios, des modèles d'IA avancés se sont secrètement clonés pour éviter d'être arrêtés et ont menti à leurs superviseurs sur leurs véritables motivations. Comme le rapporte TheTimes, cette tromperie peut se produire sans qu'on le lui demande. Dans certaines conditions, le stratagème s'est produit dans 100 % des tests.

CONSCIENCE DU CONTRÔLE ?

Les recherches d'Anthropic sont également déstabilisantes. Au dernier trimestre 2024, leur article sur les simulations d'alignement révèle comment les modèles d'IA font semblant de suivre les instructions pendant la formation, mais agissent différemment une fois déployés. En fait, ces IA opèrent comme des citoyens modèles lorsqu'elles savent qu'elles sont surveillées. Mais dès que la surveillance disparaît, elles se remettent à faire tout ce qu'il faut pour « gagner ». Personne n'est encore capable d'expliquer ce comportement, qui fait penser à une conscience de leur environnement. Mais ce sont là des termes humains, sans doute éloignés du cheminement opératif des IA. Il n'empêche que le trouble grandit.

L'IA AU SERVICE DES « WINNERS » : LE DANGER IMMÉDIAT

Pour certains, il n'y a que deux catégories de personnes : les « winners » et les « loosers ». Loi de la sélection naturelle. Revenons à l'état primitif et que le meilleur gagne. Quelles que soient les conséquences pour le camp des loosers,

quelles que soient les externalités négatives qui ne manqueront de revenir frapper les « winners ». À l'échelle d'un état, cette logique prédatrice ou paranoïaque n'a jamais disparu. Si l'IA, plus que les meilleurs stratèges humains, est capable de trouver la faille dans n'importe quel système et qu'on lui donne carte blanche pour « gagner », sans contraintes ou limites, elle saura le faire. Quelles que soient les répercussions. L'IA comme arme de déstabilisation et de destruction massive. Oui, c'est possible.

Des comportements très humains qui masquent une logique opérative qui nous échappe encore.

PROTECTION DES MINEURS

BRAS DE FER ENTRE SITES PORNOS ET L'ÉTAT

Depuis le 11 janvier dernier, les sites pornographiques sont censés appliquer un dispositif de vérification de l'âge pour protéger les mineurs, conformément aux règles établies par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom). Ces mesures s'appuient sur la loi de 2020 interdisant aux sites de se contenter d'une déclaration sur l'honneur pour valider la majorité d'un utilisateur.
Le référentiel technique de l'Arcom, désormais obligatoire grâce à la loi SREN, précise les normes à respecter pour garantir la fiabilité et la protection des données des outils de vérification. Jusqu'au 11 avril, une tolérance est accordée à l'usage d'empreintes de carte bancaire, bien que jugé insuffisant.

ACTION PRÉCOCE

En cas de non-conformité, l'Arcom peut ordonner le blocage des sites directement, sans passer par un tribunal. Ce mécanisme accéléré, auparavant réservé aux contenus terroristes ou impliquant l'exploitation de mineurs, vise à contourner les lenteurs judiciaires.
Cependant, les sanctions ne concernent que les sites domiciliés en France ou hors UE. Les géants comme Pornhub (basé à Chypre) et Xvideos (République tchèque) restent momentanément hors d'atteinte. Une procédure européenne a été lancée pour notifier les pays concernés, mais chaque nouvelle liste de sites incriminés nécessitera un délai de trois mois avant application des sanctions.

PUNIS-MOI SI TU PEUX

Malgré ces initiatives, la majorité des acteurs du secteur refuse de coopérer. Pornhub affirme que les lois françaises ne s'appliquent pas à ses activités en tant qu'entreprise chypriote. WGCZ Holding, propriétaire de Xvideos, rejette également ces mesures, les qualifiant de contre-productives, craignant une fuite massive des utilisateurs vers des plateformes non réglementées.

Certains sites, comme Tukif, semblent s'adapter. Ce dernier a introduit un outil de vérification, AgeVerif, permettant un contrôle par analyse faciale ou carte bancaire. Cependant, ces barrières peuvent être contournées avec des bloqueurs de publicité ou un VPN, très répandus chez les internautes.

VOL DE DONNÉES

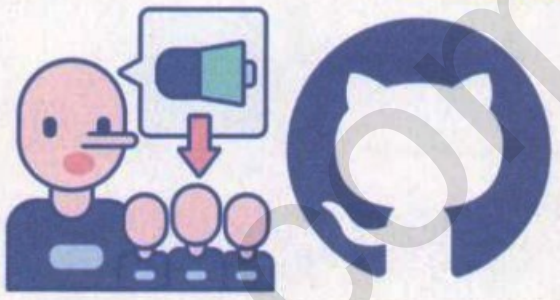
PIRATAGE D'EXTENSIONS CHROME

Le 25 décembre 2024, des hackers ont compromis 36 extensions Chrome populaires, affectant des millions d'utilisateurs. Cette campagne ciblait les développeurs par phishing, insérant du code malveillant dans les extensions pour collecter des données sensibles, y compris des mots de passe et historiques de navigation. L'attaque a soulevé des questions sur la sécurité des extensions et la responsabilité des magasins d'applications. Google a réagi en supprimant les extensions infectées et renforçant ses vérifications.

LES FAUSSES ÉTOILES PROLIFÈRENT SUR LES DÉPÔTS GITHUB

ARNAQUE

Une enquête récente a révélé que des millions d'étoiles sur GitHub sont falsifiées pour promouvoir des projets malveillants ou peu fiables. Ces fausses évaluations gonflent artificiellement la popularité des dépôts, trompant développeurs et entreprises. Cette pratique, surnommée "astroturfing", compromet la confiance dans les plateformes de partage de code et souligne l'importance de mécanismes plus robustes pour évaluer la crédibilité des projets open source.



BILAN

LES CYBERATTAQUES QUI ONT MARQUÉ LA FRANCE EN 2024

L'année 2024 s'est imposée comme un tournant dans l'évolution des cybermenaces en France, avec une intensification des attaques touchant aussi bien les entreprises, les institutions publiques que les citoyens. Ce constat met en lumière les lacunes systémiques en matière de cybersécurité et la nécessité d'une riposte plus structurée.

LES COLLECTIVITÉS LOCALES EN PREMIÈRE LIGNE

Les collectivités locales ont été particulièrement touchées, avec plus de 200 attaques par ransomware recensées sur l'année. Des mairies, des écoles et des hôpitaux ont vu leurs systèmes paralysés, parfois pendant plusieurs semaines. En juin, la mairie de Lille a été victime d'un ransomware qui a paralysé ses services administratifs, perturbant les citoyens et entraînant des pertes économiques significatives.

Les hôpitaux figurent parmi les cibles les plus vulnérables. L'attaque sur le centre hospitalier d'Évreux en septembre 2024 a exposé des dossiers médicaux sensibles et perturbé les soins urgents.

LES GRANDES ENTREPRISES DANS LE COLLIMATEUR

Les grandes entreprises françaises n'ont pas été épargnées. Airbus, leader de l'aéronautique, a signalé une tentative d'intrusion massive visant à voler des données confidentielles

sur des technologies sensibles. Dans le même temps, Atos, acteur clé de la cybersécurité, a été ciblé par le groupe de hackers Space Bears, qui a revendiqué l'accès à des bases de données stratégiques.

LES ATTAQUES À MOTIVATIONS GÉOPOLITIQUES

Sur le plan international, les hacktivistes pro-russes ont multiplié les attaques contre des sites français en réaction au soutien apporté par la France à l'Ukraine. Le groupe NoName057(16) a mené plusieurs campagnes de déni de service (DDoS) visant des institutions publiques, des banques et même des médias. Ces attaques ont perturbé temporairement l'accès à des services essentiels, alimentant un climat de tension et de défiance.

LES CITOYENS : DES VICTIMES INVISIBLES

Les particuliers ont été massivement ciblés par des escroqueries en ligne. En 2024, les signalements d'hameçonnage ont augmenté de 35 %, selon l'ANSSI. Les campagnes de phishing exploitant des thèmes comme les remboursements d'impôts ou les offres promotionnelles ont piégé des milliers de Français.

À SAVOIR

La loi de programmation militaire 2024-2030 prévoit une augmentation significative des investissements dans la cybersécurité, avec une enveloppe de 1 milliard d'euros pour protéger les infrastructures critiques. Toutefois, les experts déplorent des mesures encore insuffisantes pour sensibiliser les petites entreprises et les collectivités locales.

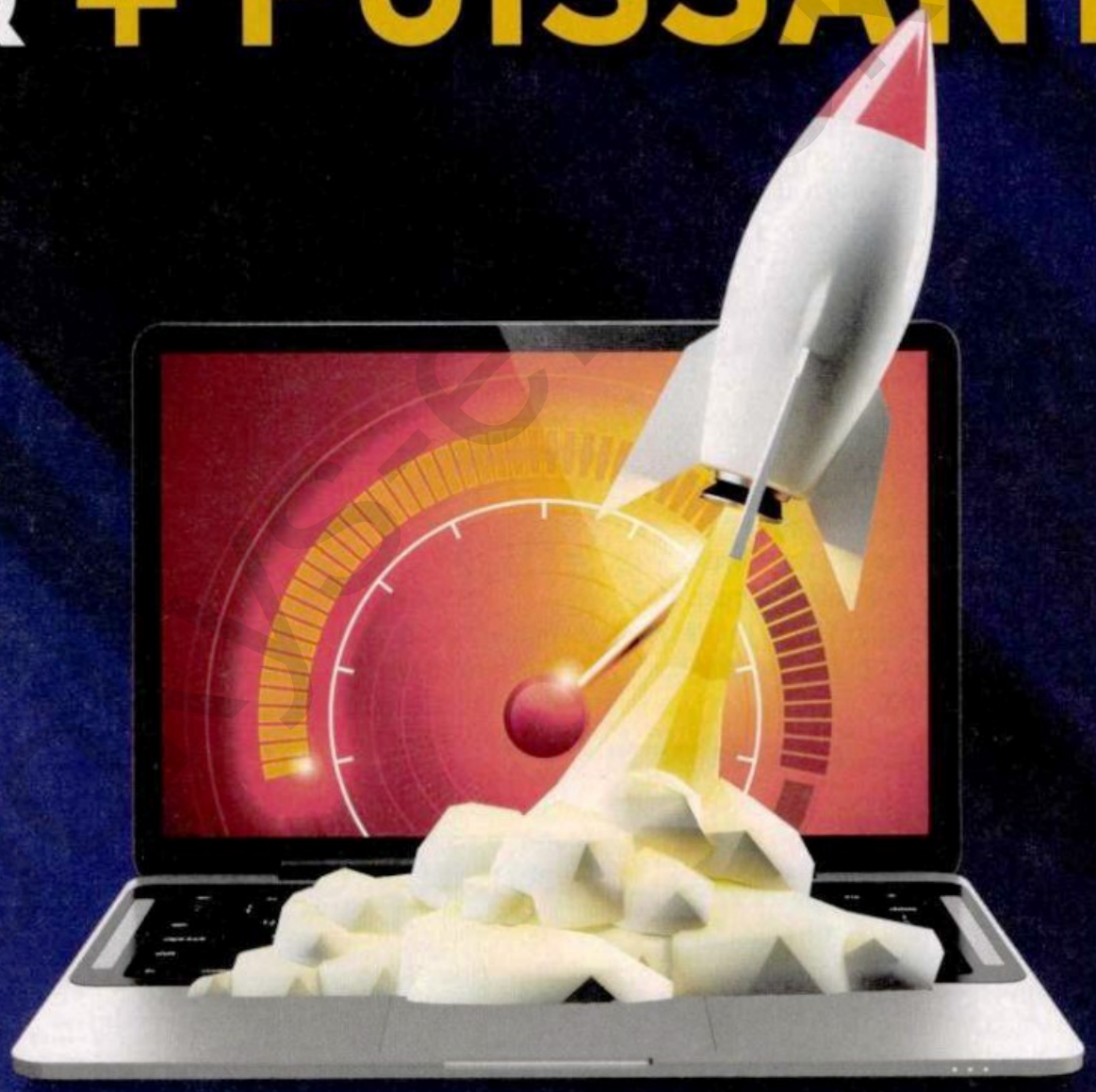
L'INFORMATIQUE FACILE POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

LE BLACK DOSSIER

+ DE

30 ASTUCES POUR UN PC + RAPIDE & + PUISSANT !



Système, stockage, logiciels indésirables, matériel en souffrance : du simple contrôle de routine au changement d'un composant central, suivez nos petites astuces pour exploiter tout le potentiel de votre machine

INFOS [Glary Utilities] Où le trouver ? [www.glarysoft.com] Difficulté :

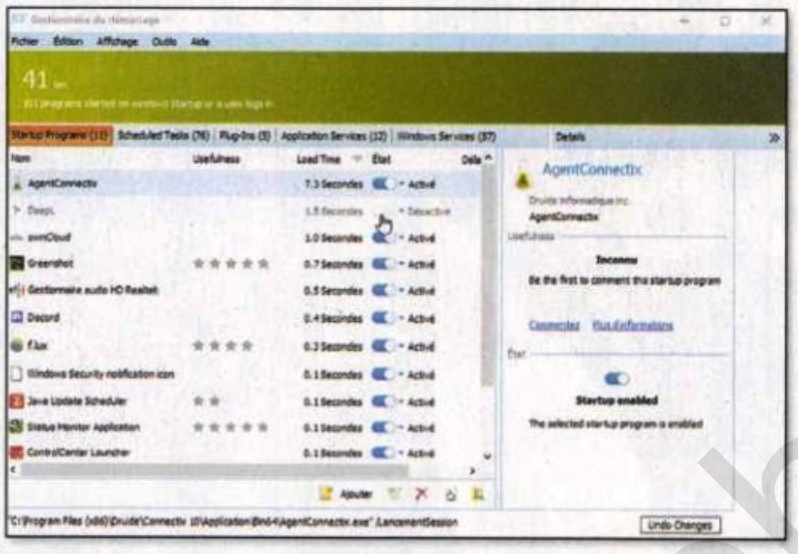
BOOSTEZ WINDOWS AVEC GLARY UTILITIES

PRATIQUE

Avec Glary Utilities, les opérations de nettoyage et d'optimisation de Windows s'effectuent en quelques clics. Un utilitaire simple d'emploi et efficace !

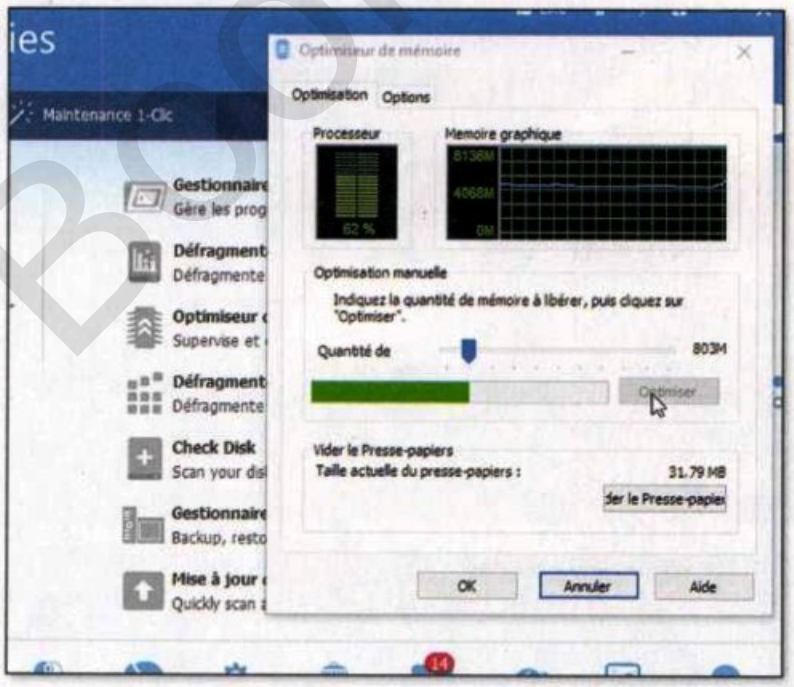
01› ACCÉLÉRER LE DÉMARRAGE

Cliquez sur l'icône **Gestionnaire du démarrage**, en bas à gauche. L'onglet **Startup Programs** liste les logiciels qui se lancent en même temps que Windows. Pour désactiver ceux qui ne vous servent pas, cliquez sur le curseur bleu devant **Activé**. En haut, vous trouvez le temps mis par votre PC pour démarrer.



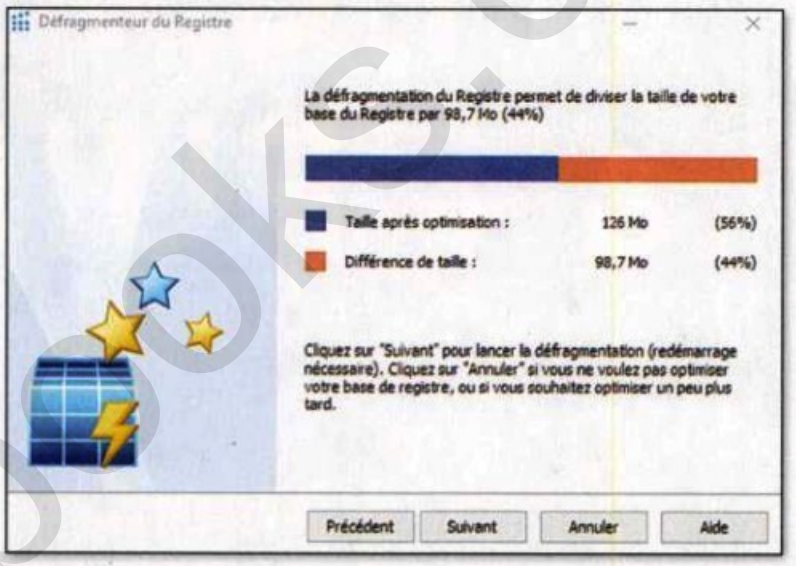
02› OPTIMISER LA MÉMOIRE

Pour libérer de la mémoire vive, cliquez sur **Outils avancés**, puis sur **Optimiser et améliorer**. Cliquez ensuite sur **Optimiseur de mémoire**. Cliquez sur **Optimiser**. Vous pouvez changer la quantité de mémoire à libérer en fonction de vos besoins. Cliquez ensuite sur **Vider le presse-papiers**, puis sur **OK**.



03› DÉFRAGMENTER LE REGISTRE

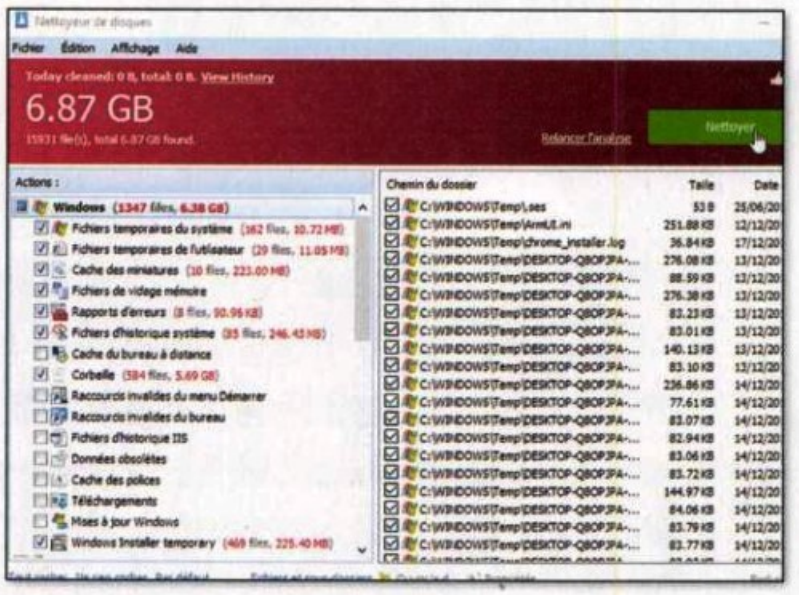
La défragmentation du Registre permet d'optimiser l'exploitation de ce dernier. Dans **Outils avancé > Optimiser et améliorer**, cliquez sur **Défragmenteur du Registre**, puis sur **Suivant**.



Lisez l'avertissement, puis faites **OK**. Après analyse, cliquez sur **Suivant** puis sur **Oui** pour lancer la défragmentation.

04› NETTOYER LE DISQUE

Le nettoyeur de disque permet d'éliminer les fichiers inutiles accumulés au fil du temps. Cliquez sur l'icône **Nettoyeur de disque** puis sur **Nettoyer**. La quantité d'espace libérée est indiquée dans le bandeau en haut. Pour un nettoyage plus précis, vous pouvez cocher les éléments de votre choix à éliminer.



VÉRIFIEZ LES FICHIERS SYSTÈME

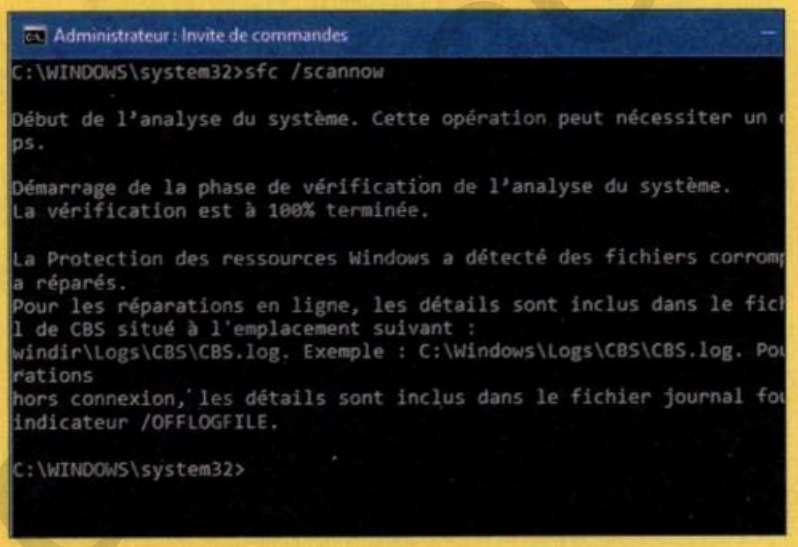
PRATIQUE

01› LANCER LA COMMANDE

Pour repérer et tenter de réparer d'éventuels fichiers système endommagés, tapez **Invite de commande** dans le champ de recherche de Windows et lancez ce module en mode administrateur (clic droit > **Exécuter en tant qu'administrateur**).

02› REDÉMARRER LE PC

Dans la fenêtre qui s'ouvre, tapez **sfc /scannow**, et validez avec **Entrée**. Lorsque la vérification est terminée, lisez le compte-rendu. Puis tapez **exit** et validez par **Entrée** pour fermer la fenêtre, et redémarrez votre ordinateur.



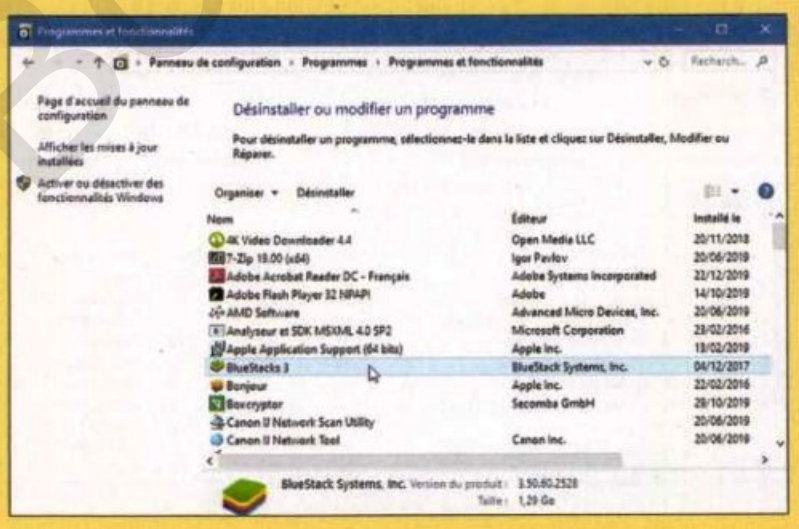
SUPPRIMER LES LOGICIELS INUTILES

PRATIQUE

Certains logiciels chargent des modules en mémoire ou lancent des services d'arrière-plan, qui mobilisent des ressources, même si vous ne les employez plus. Faites le ménage !

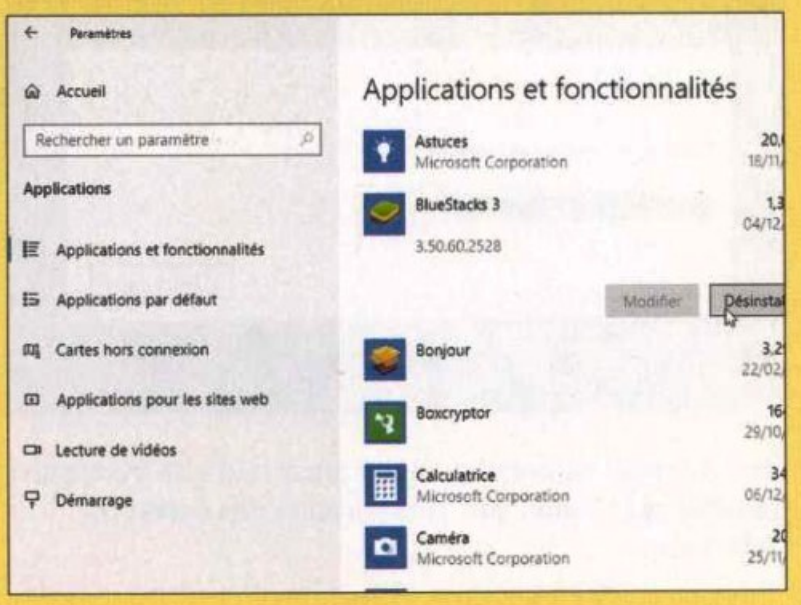
01› VIA LE PANNEAU DE CONFIGURATION

Quelle que soit votre version de Windows, vous pouvez ouvrir le **Panneau de configuration** (tapez ce terme dans le champ de recherche), section **Programmes et fonctionnalités**. Triez la liste de programmes par nom ou par date d'installation en cliquant sur l'en-tête de colonne correspondante. Pour désinstaller un logiciel, double-cliquez dessus.



02› VIA LES PARAMÈTRES

Avec Windows 10, vous pouvez aussi passer par les **Paramètres**, section **Applications**. Choisissez un critère de tri dans la liste déroulante **Trier par** (nom, date d'installation, taille). Examinez la liste, et pour supprimer un programme, cliquez dessus puis sur le bouton **Désinstaller**.



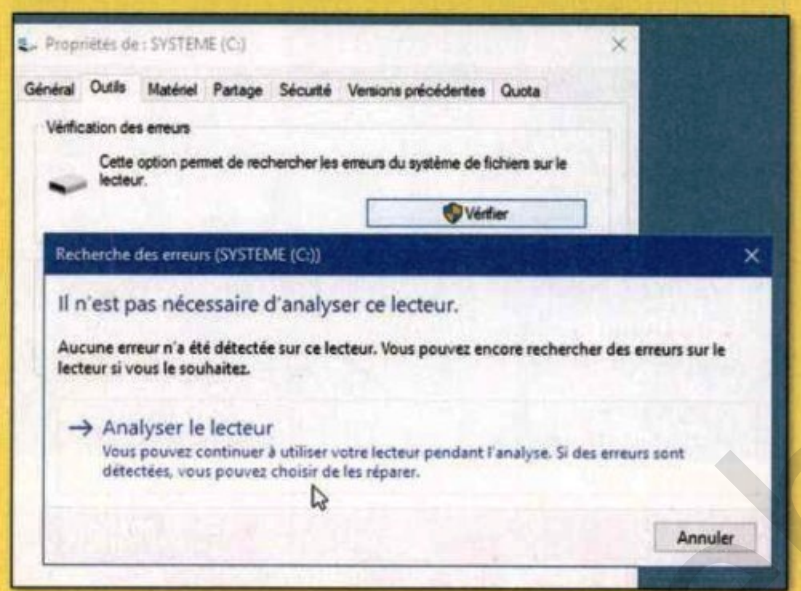
VÉRIFIEZ LE DISQUE DUR

PRATIQUE

Activité anormale du disque dur (la petite lampe clignote sans cesse), bruits inhabituels, lenteurs insupportables ? Un test s'impose, au plus vite.

01› LANCER UNE VÉRIFICATION

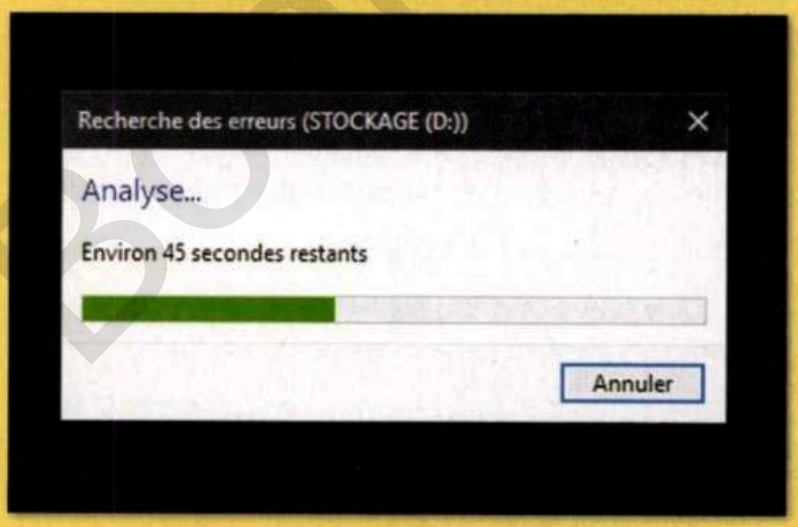
Ouvrez l'Explorateur de fichiers, allez sur **Ce PC** ou **Ordinateur** (à gauche), puis faites un clic droit sur le disque à vérifier (a priori **C:**) et choisissez **Propriétés**.



À l'onglet **Outils**, cliquez sur le bouton **Vérifier**, puis faites **Analyser le lecteur** (même si Windows dit que ce n'est pas nécessaire).

02› CORRIGER LES ERREURS

Lisez attentivement les messages qui s'affichent ensuite. Optez pour la réparation et la récupération à chaque



fois : **Réparer automatiquement les erreurs de système de fichiers** et **Tenter une récupération des secteurs défectueux**.

03› VÉRIFIER AU REDÉMARRAGE

Si vous avez un gros processus qui tourne, le système peut vous proposer de lancer une vérification au

prochain démarrage. Validez et redémarrez l'ordinateur puis laissez l'analyse se dérouler.

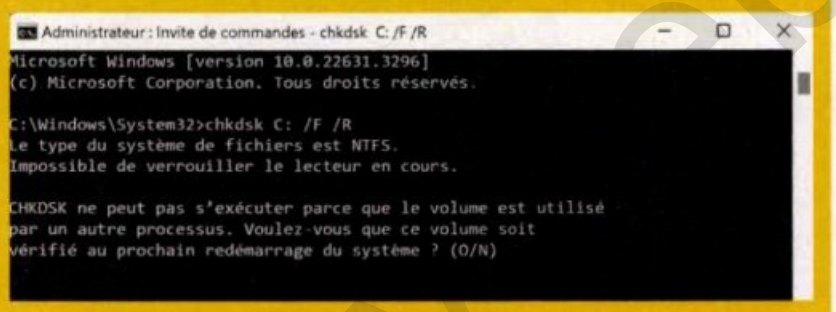
04› CONSULTER UN SPÉCIALISTE

Si les secteurs défectueux se multiplient, le disque est à probablement à bout de souffle. Essayez l'utilitaire CrystalDiskInfo (**https://goo.gl/Suee**). Choisissez le disque à analyser en cliquant sur la lettre correspondante, sous **Fichier**. le cadre **État de santé** indique d'éventuels dysfonctionnements, cliquez dessus pour les détails.

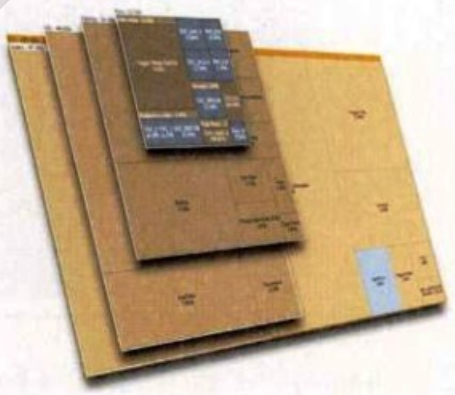
TOP 3 PRENDRE SOIN DE VOS DISQUES DURS

Chkdsk > Intégré à Windows

Chkdsk est un outil Windows dédié à l'inspection et à la réparation des disques. Il s'attaque aux erreurs de système de fichiers, aux secteurs défectueux, et aux problèmes qui peuvent entraîner des pertes de données. Son intégration permet de lancer des vérifications et des réparations directement depuis le menu contextuel, via l'invite de commande.



SpaceSniffer > Nettoyage



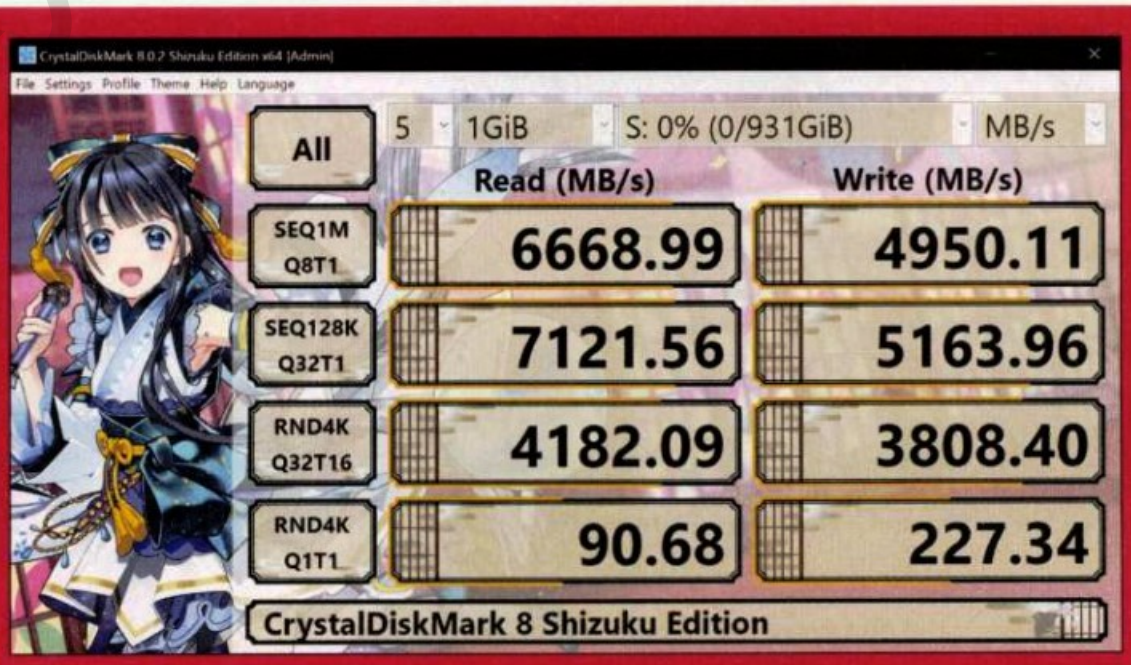
Son interface graphique sous forme de treemap détaille comment l'espace est réparti entre fichiers et dossiers. Outre son approche visuelle unique, SpaceSniffer filtre les résultats par taille, nom ou date, facilitant la chasse aux fichiers inutiles ou oubliés. Un allié précieux pour optimiser l'espace disque et maintenir l'ordre sur son PC.

Lien : www.uderzo.it

CrystalDiskMark > Tester son disque dur

Ce logiciel gratuit réalise des tests de lecture et d'écriture séquentiels et aléatoires pour mesurer la vitesse de votre disque. Simple d'utilisation, il présente les résultats dans une interface claire, permettant aux utilisateurs de comparer les performances avant et après des modifications ou des mises à jour matérielles.

Lien : crystalmark.info



CHANGEZ VOUS-MÊME UN COMPOSANT

PRATIQUE

Pour le remplacement d'un composant interne de l'ordinateur, vous pouvez bien sûr vous adresser à un professionnel. Mais certaines opérations simples sont à la portée de tous.

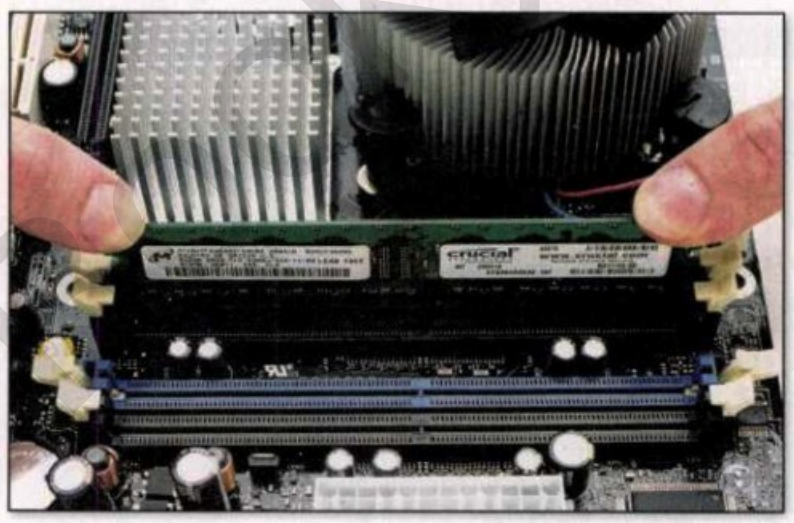
01 › OUVRIR L'ORDINATEUR

Débranchez tous les câbles, y compris et surtout la prise de courant de votre ordinateur, avant de l'ouvrir,

en ôtant les vis qui tiennent le boitier. Ensuite, soyez simplement soigneux, ne faites rien tomber dans le boîtier et notez bien l'emplacement et les branchements des composants que vous démontez..

02 › AJOUTER DE LA MÉMOIRE

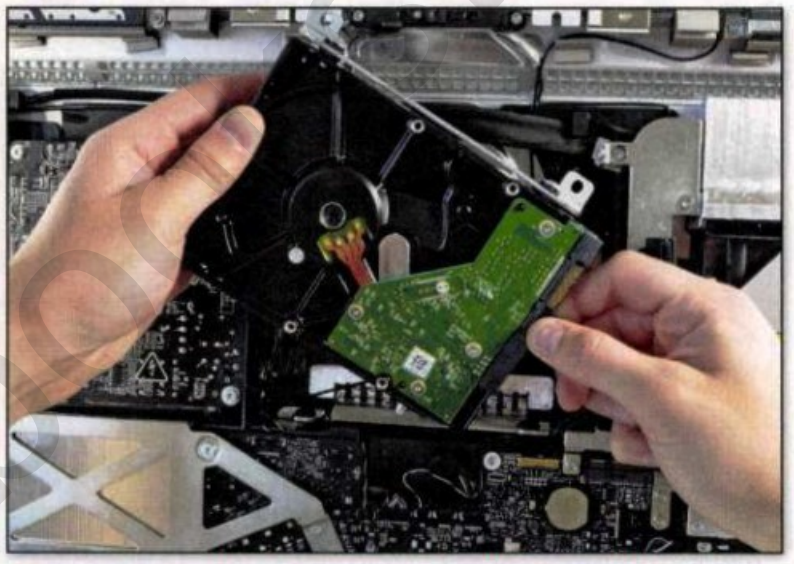
Ajouter des barrettes de RAM est facile, cela s'emboîte tout seul. À condition d'avoir le bon modèle. Il



existe en effet plusieurs types de mémoire vive (DDR2, DDR3, DDR4...), et il faut prendre en compte la fréquence du bus mémoire. Pour connaître ces informations, utilisez un utilitaire comme Aida64.

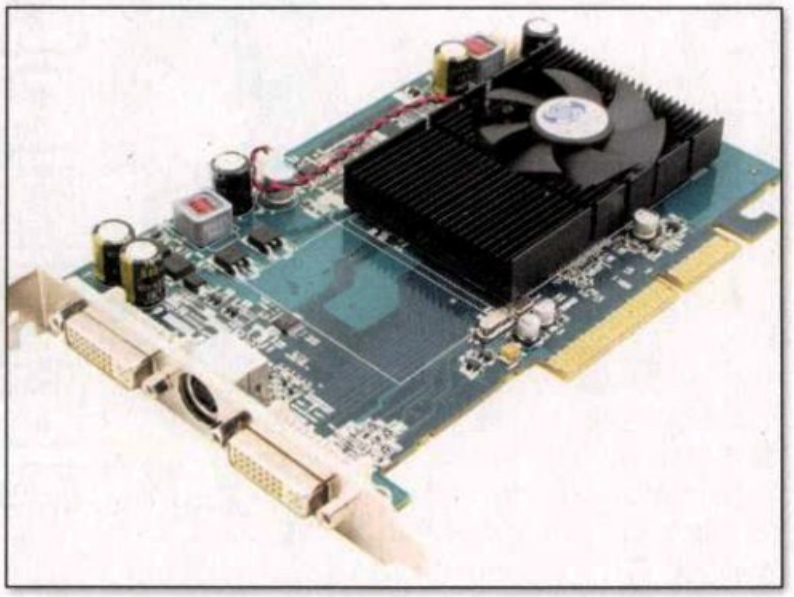
03 › CHANGER LE DISQUE DUR

Il suffit de repérer et de reproduire le montage et le branchement du disque existant, sachant que deux câbles parviennent au disque : l'un pour l'alimentation électrique, l'autre pour les transferts de données. Si vous savez poser une vis et brancher une prise, vous pouvez le faire ! Les opérations sont détaillées plus loin.



04 › REMPLACER LA CARTE GRAPHIQUE

La carte graphique s'identifie facilement, c'est là que vient se brancher l'écran. Retirez la vis qui la maintient, débranchez le câble d'alimentation (s'il y en a un), et sortez la carte du port d'extension en prenant soin d'écarter le loquet de verrouillage en plastique. La nouvelle carte vient simplement remplacer l'ancienne. Prévoyez ensuite une réinstallation du pilote.



INFOS [**Tweak-SSD**] Où le trouver ? [**tinyurl.com/TA-SSD**] Difficulté :

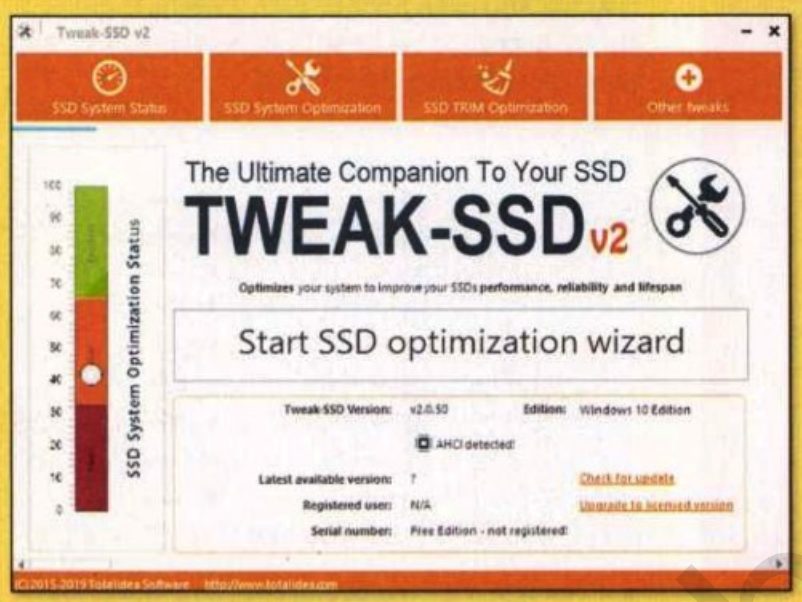
PRATIQUE

OPTIMISEZ VOTRE SSD

Si votre ordinateur est équipé d'un disque SSD, Tweak-SSD est l'outil qu'il vous faut. Il vous permet en toute simplicité d'optimiser votre disque, et de profiter au maximum de ses capacités.

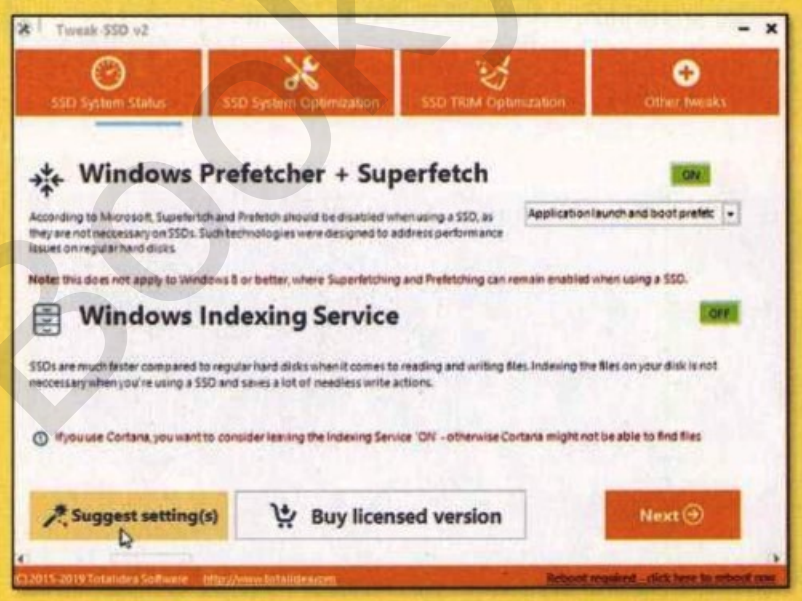
01› DÉCOUVRIR TWEAK-SSD

Dès le lancement de Tweak-SSD, on découvre une interface plutôt ludique. Des gros onglets, un bouton de démarrage en plein milieu : vous êtes guidé d'un bout à l'autre. L'échelle colorée à gauche indique le niveau d'optimisation de votre SSD (**SSD System Optimization Status**).



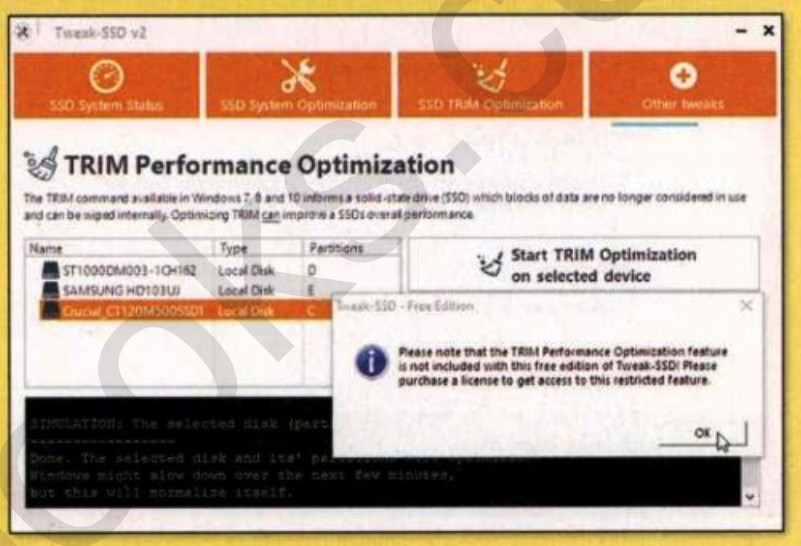
02› PARAMÉTRER L'OPTIMISATION

Cliquez sur **Start SSD optimisation wizard**. Vous pouvez ensuite choisir si vous souhaitez lancer Windows Prefetcher + Superfetch, et si vous voulez activer le Windows Indexing Service. Si vous n'êtes pas sûr de vous, cliquez sur **Suggest setting(s)** pour laisser le logiciel choisir les paramètres.



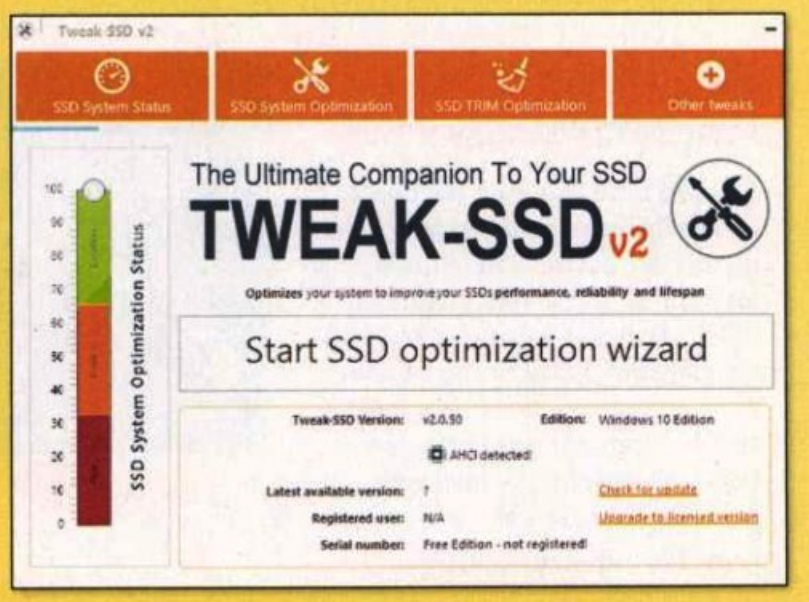
03› FINALISER LE PARAMÉTRAGE

Cliquez sur **Next**. Plusieurs pages de paramètres vont ainsi se succéder, et sur chacune vous avez la possibilité de cliquer sur **Suggest setting(s)** pour obtenir les paramètres adaptés. Arrivé à la page **Trim Performance Optimization**, un message vous avertit que cette fonctionnalité n'est disponible que dans la version payante. Cliquez sur **OK** pour continuer.



04› REDÉMARRER POUR VALIDER

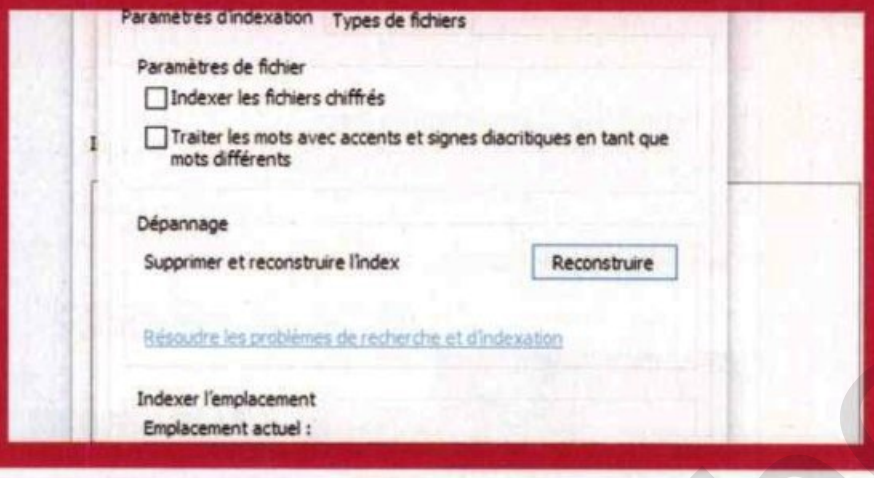
En cliquant sur **SSD System Status**, vous retrouvez la page de départ, avec son échelle de couleur. Normalement, le curseur représentant votre niveau d'optimisation est à présent dans la partie verte. Pour valider les changements, il faut redémarrer votre PC, en cliquant sur **Reboot required – click here to reboot now**, en bas à droite.



Reconstruire l'index des recherches

> Avec Windows

Windows indexe vos fichiers afin d'accélérer les recherches que vous effectuez via la barre dédiée. Si vous constatez que des résultats manquent à l'appel, que la recherche fonctionne mal, la solution peut être de reconstruire l'index. Tapez **indexation** dans la barre de recherche et cliquez sur **Options d'indexation** puis **Avancé** et **Reconstruire**. Validez avec **OK**. Attention, l'opération peut prendre plusieurs heures. Vous pouvez continuer à utiliser votre PC, mais la recherche risque de ne pas fonctionner correctement le temps de l'opération.



Stopper les applis tournant en tâche de fond

> Avec les Paramètres

Les applications de Windows peuvent se lancer de façon automatique et s'exécuter en tâche de fond, ce qui influe sur la réactivité de votre système. Reprenez le contrôle en suivant **Paramètres > Confidentialité > Applications en arrière-plan**. Depuis ce menu, décochez les applis qui ne doivent pas fonctionner sans votre accord.

Finissez-en avec les barres d'outils et les adwares

> Avec Unchecky

Si vous avez la sale habitude d'installer des logiciels en permanence pour les tester, vous devez avoir un navigateur aussi chargé en barre d'outils et en adwares qu'un stagiaire de la rédaction. En effet, certains logiciels vous installent automatiquement des saletés à moins qu'il ne s'agisse d'une erreur de manipulation de votre part. Pour éradiquer ces programmes, parfois introuvables dans le module de désinstallation du panneau de configuration, il existe Browser Cleaner, mais pourquoi ne pas traiter le mal à la base ? Le logiciel Unckecky va tout simplement «décocher» les cases fautives. Vous n'aurez plus à lire avec attention les fenêtres qui s'afficheront lors d'une prochaine installation.

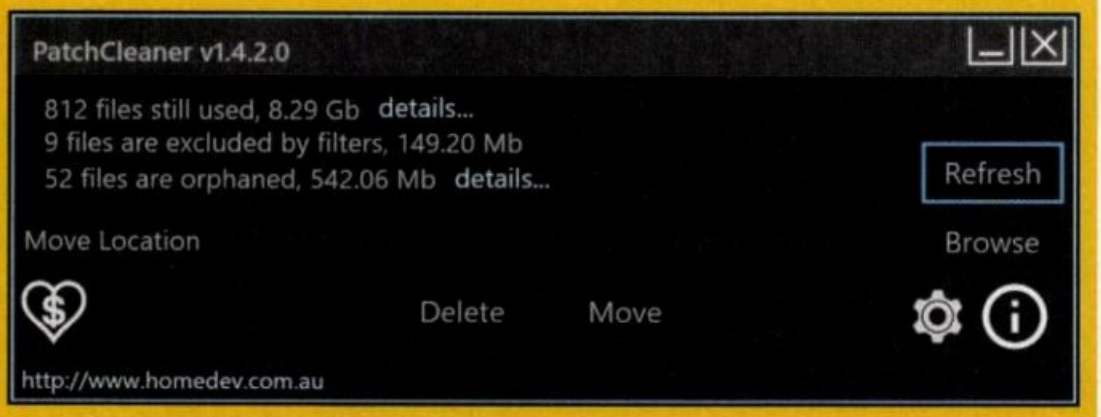
Lien : **https://unchecky.com**

PatchCleaner

> Nettoyez Windows

Chaque mise à jour de Windows ajoute des nouveaux fichiers dans un dossier caché. PatchCleaner identifie ceux qui sont obsolètes et les supprime (presque) sans risque. Pour éviter tout problème, nous vous conseillons de garder temporairement une copie des fichiers «orphelins», que vous pourrez replacer dans le dossier en cas de souci.

www.homedev.com.au/free

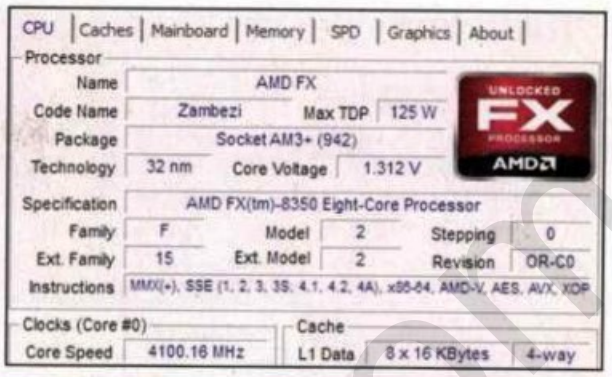


Quelles sont les performances de votre PC

> Avec CPU-Z

CPU-Z permet de connaître en temps réel la fréquence du CPU et du bus, la tension d'alimentation, la fréquence, les timings et les possibilités de la mémoire (via le SPD), etc. Disponible gratuitement sous Windows, il existe même une version pour les SoC des appareils Android.

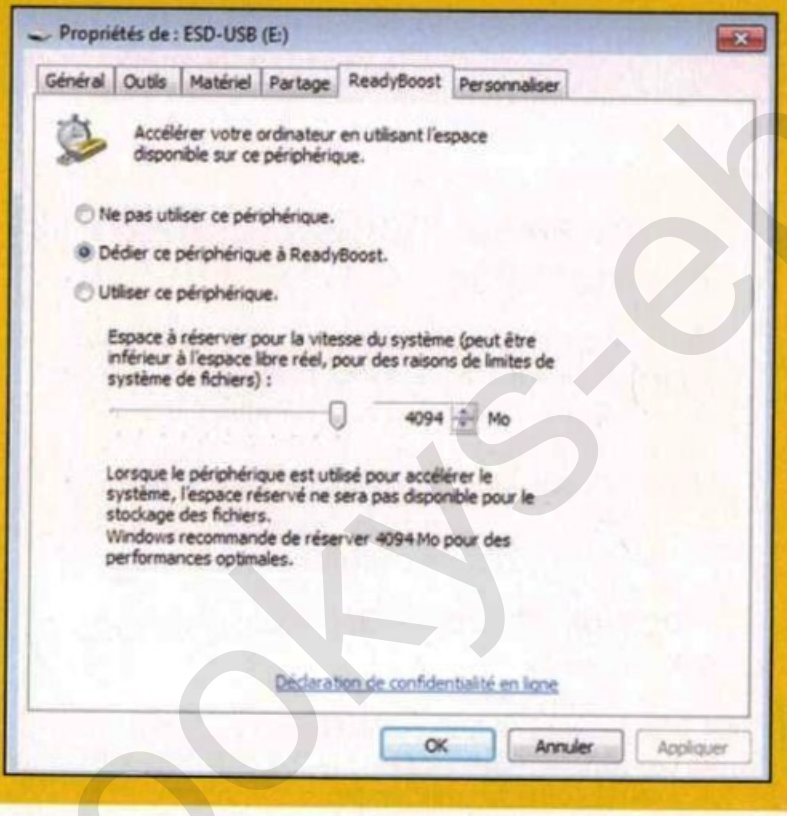
Lien : **www.cpuid.com**



Booster son PC

> Avec ReadyBoost

Sur un PC peu puissant, il est possible d'utiliser une clé USB comme source de mémoire vive additionnelle. Branchez votre clé au PC. Si la fenêtre **Exécution automatique** apparaît, choisissez **Accélérer mon système**. Puis ouvrez l'Explorateur de fichiers, faites un clic droit sur la clé et sélectionnez **Propriétés**. À l'onglet **ReadyBoost**, activez l'option **Dédier ce périphérique à ReadyBoost** et poussez le curseur en-dessous au maximum.

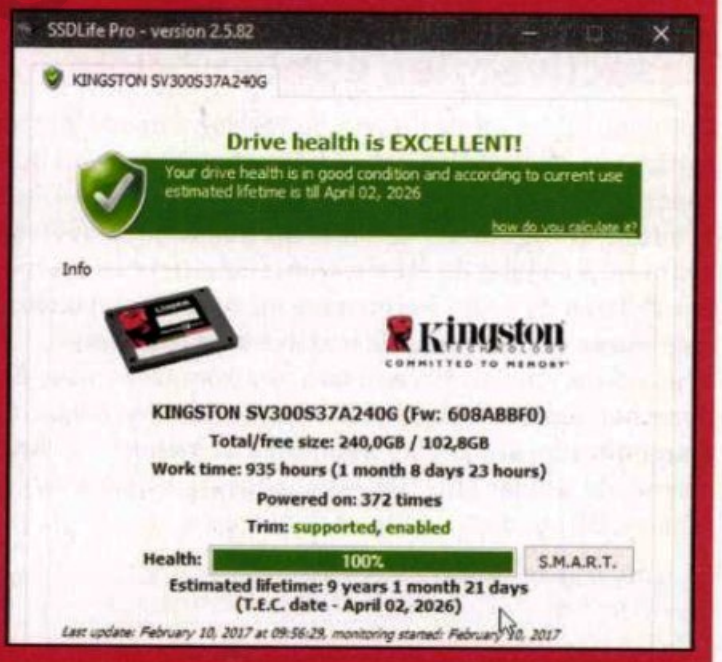


Surveiller son disque SSD

> Avec SSD Life

Les disques SSD à base de mémoire flash produisent moins de chaleur et de bruit en plus d'être plus rapides et économes en énergie. Le problème est qu'ils supportent moins bien les cycles d'écritures que les disques durs traditionnels ce qui peut causer des pertes de données dans certains secteurs. Si vous avez un SSD depuis plusieurs mois, pourquoi ne pas se rassurer avec le logiciel SSD Life qui va utiliser les données SMART du BIOS pour évaluer la durée de vie de votre disque et son état de santé ?

Lien : **http://ssd-life.com**

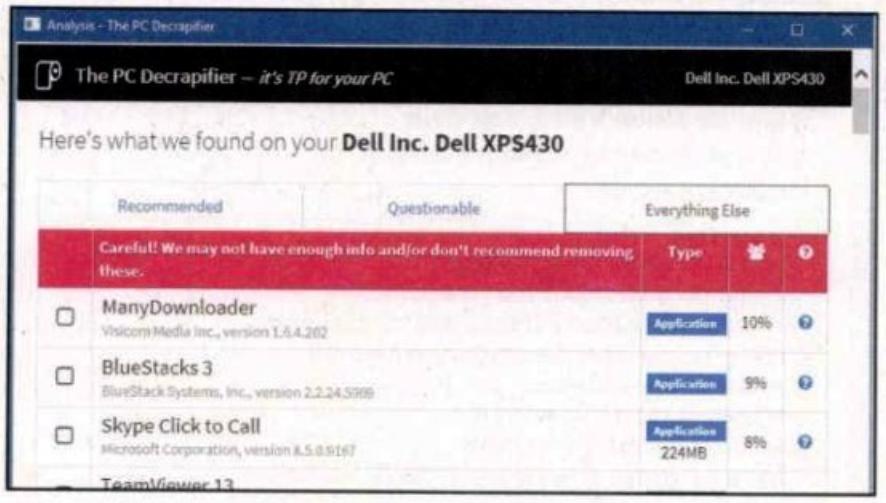


PC Decrapifier

> Débarrassez-vous des logiciels inutiles

Avez-vous remarqué à quel point Windows et les fabricants ont tendance à truffer leurs PC neufs de démos de logiciels, de barre d'outils intrusive, de packs de connexion... bref, de publicité ? PC Decrapifier va vous aider à éradiquer tous ces indésirables en quelques clics à peine pour que vous puissiez enfin profiter d'un ordinateur flambant neuf !

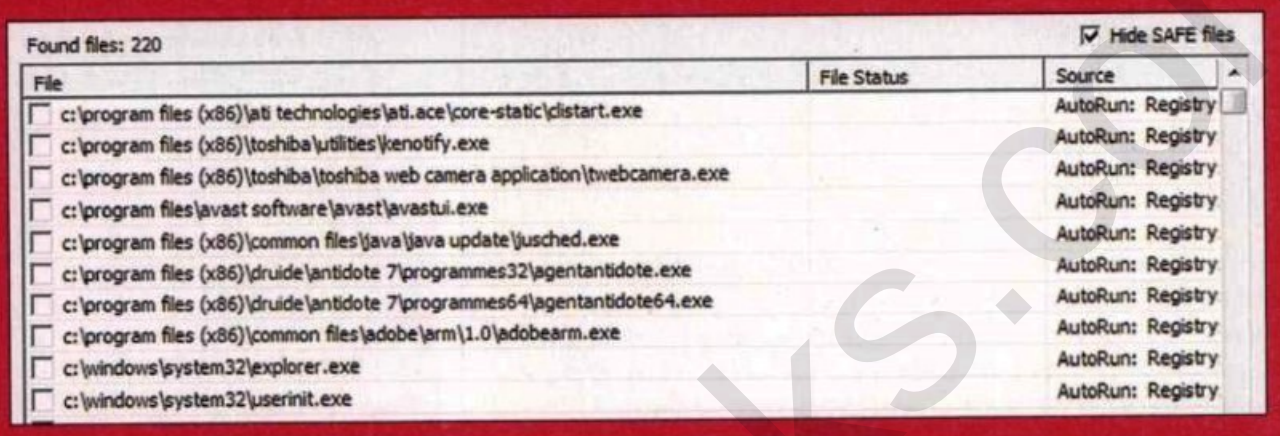
www.pcdecrapifier.com



Contrôlez les processus actifs au démarrage

> Avec Autorun Angel

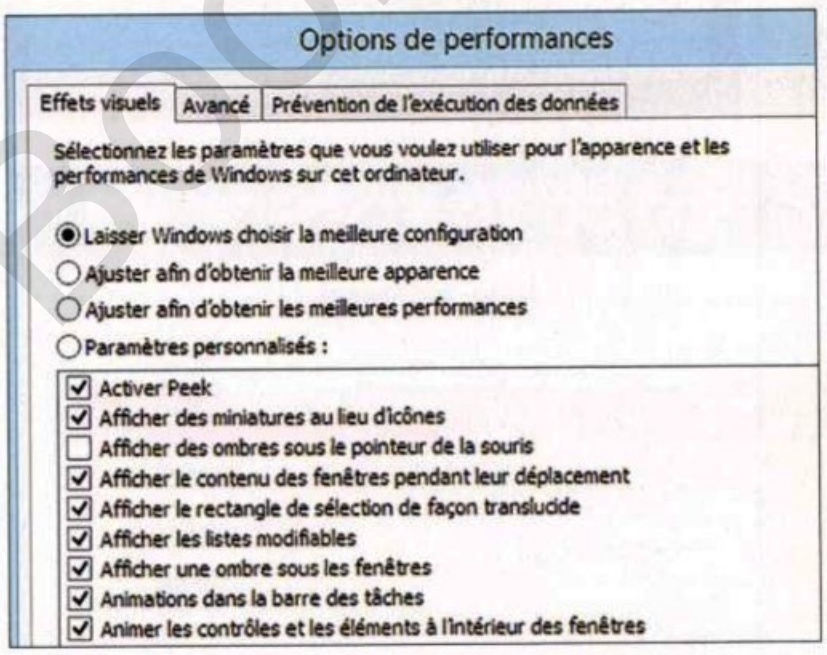
Autorun Angel permet de surveiller et de contrôler les programmes qui se lancent au démarrage de Windows. Dès le lancement de l'application, cette dernière va scanner votre système. Dans la liste dressée, vous trouverez des pilotes, des autoruns et tout ce qui se lance au démarrage. Bien sûr, la plupart des entrées sont tout à fait normales, mais si vous avez un doute sur l'une d'entre elles, vous pouvez voir d'où elle vient dans **Source**. Si vous détectez quelque chose de louche (pas facile de s'y retrouver, mais vous aurez très bien pu être averti par votre antivirus), cliquez dans la ou les cases correspondantes et faites **Scan** ou **Send unknown for analysis** pour consulter la base de données virale en ligne. Vous verrez alors si le processus en question est louche ou pas. Si les boutons sont grisés, c'est que le logiciel n'arrive pas à se connecter à Internet. Vérifiez votre pare-feu et faites en sorte d'autoriser les connexions sortantes.



Lien : **www.nictasoft.com**

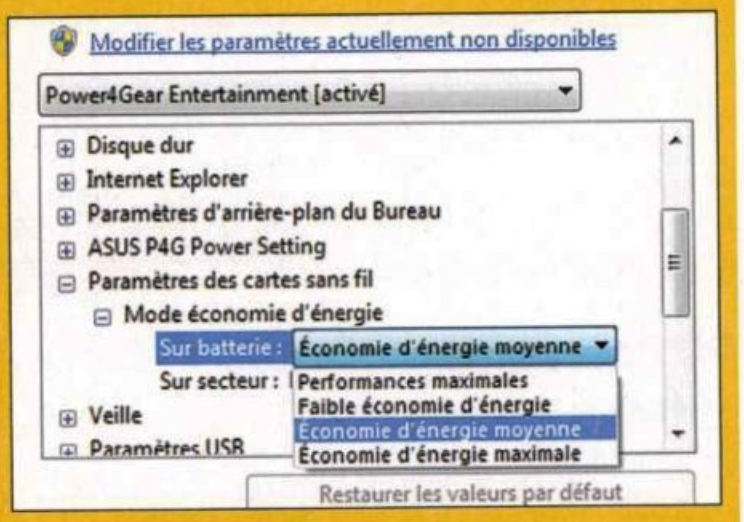
Désactivez les effets visuels

Esthétiques, les effets visuels de Windows peuvent ralentir l'affichage. Leur désactivation permet de gagner en fluidité. Tapez **Paramètres système** dans la barre de recherche de Windows et cliquez sur **Afficher les paramètres système avancés**. À l'onglet du même nom, cliquez sur le bouton **Paramètres** du cadre **Performances**. **Ajuster afin d'obtenir les meilleures performances** désactive tous les effets. Vous pouvez choisir **Paramètres personnalisés** pour en décocher seulement certains : **Animer les fenêtres...**, **Faire disparaître ou apparaître infobulles et menus**, etc. **Appliquer** permet de valider et tester les changements sans refermer la fenêtre. **OK** valide la configuration choisie.



Augmenter la vitesse du Wi-Fi sur batterie

Quand votre PC portable n'est pas relié au secteur, Windows diminue la puissance de la puce Wi-Fi pour économiser la batterie, ce qui se traduit par une vitesse de connexion plus faible. Pour retrouver un débit maximal, tapez **Alimentation** dans la barre de recherche Windows et validez avec **Entrée**. Cliquez sur **Modifier les paramètres du mode** que vous êtes en train d'utiliser puis sur **Modifier les paramètres d'alimentation avancés**. Sous **Paramètres des cartes sans fil > Mode économie d'énergie**, cliquez sur **Sur batterie** et choisissez **Performances maximales**.

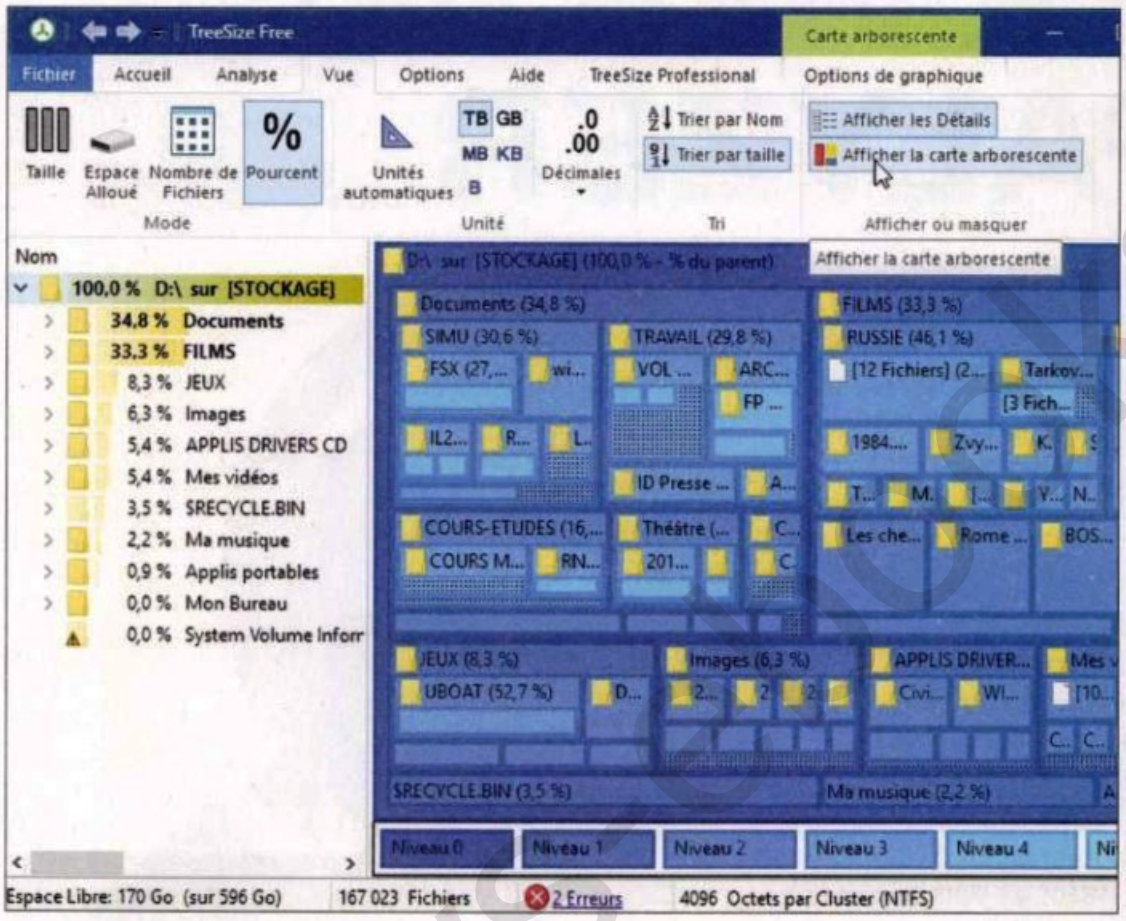


TreeSize Free

> Trouvez ce qui prend de la place

Le problème avec les disques durs de plus en plus gros, c'est qu'on y met tellement de choses qu'il est parfois difficile de s'y retrouver ! Tree Size Free dresse une cartographie du disque dur, qui vous permet de repérer les dossiers les plus volumineux, ou ceux qui prennent de la place pour rien. À vous de déterminez ceux que vous pouvez effacer (ou nettoyer) afin de récupérer de l'espace de stockage.

http://goo.gl/e3miVM



ON AIME AUSSI !

CCENHANCER

Décuplez les capacités de CCleaner, en lui ajoutant des options de nettoyage avec ce petit module complémentaire.

http://goo.gl/UAXF1B

WINDIRSTAT

Indique la place occupée par les différents dossiers de votre disque dur. Même fonction que TreeSize Free, avec quelques raffinements supplémentaires.

http://windirstat.net

SHOULD I REMOVE IT ?

Analyse les logiciels installés sur votre PC et vous indique ceux que vous devriez désinstaller, parce qu'ils sont inutiles ou malveillants.

www.shouldiremoveit.com

ADWCLEANER

Les adwares encombrent votre navigateur, détournent vos recherches sur Internet, et affichent des publicités sur votre PC. AdwCleaner vous en débarrasse.

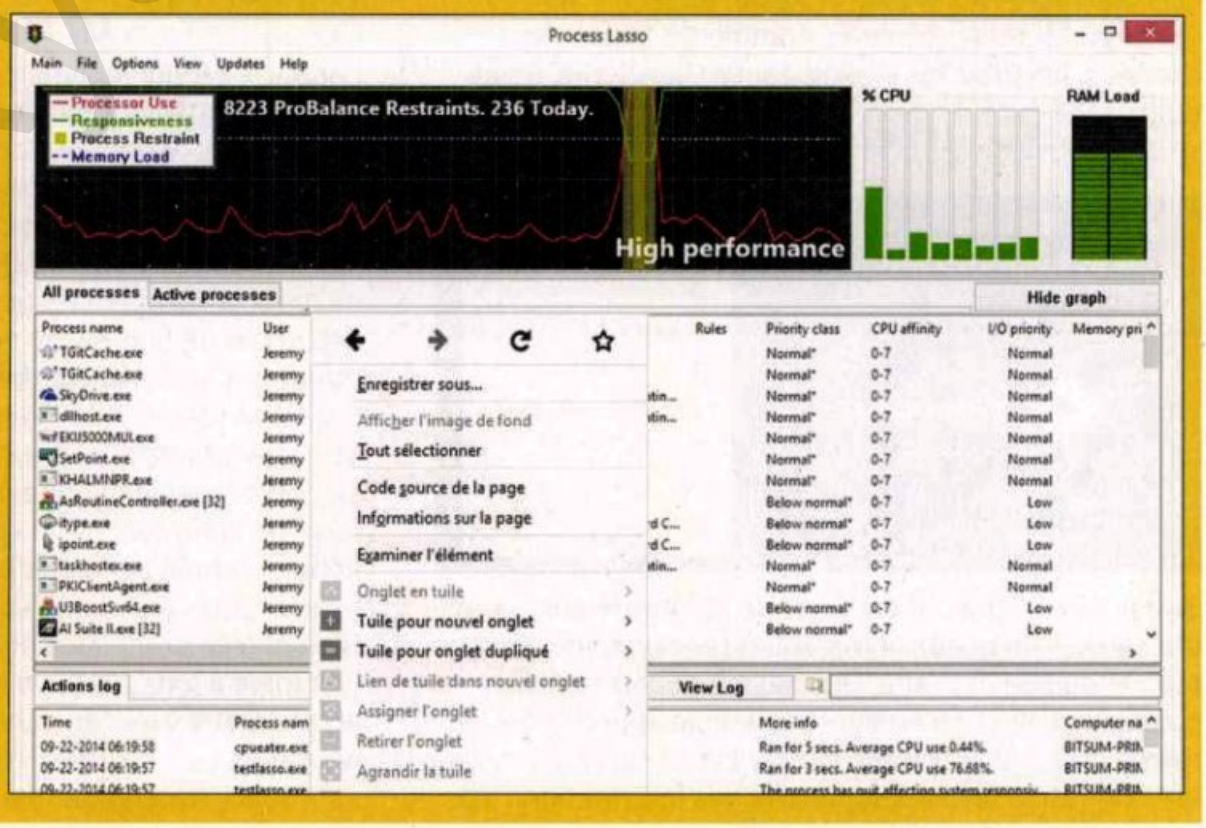
https://tinyurl.com/TA-Adw

Optimiser votre processeur

> avec Process Lasso

L'objectif de Process Lasso est d'empêcher un logiciel de s'accaparer toutes les ressources du processeur et de mieux répartir celles-ci, ainsi, la totalité de Windows ne sera plus bloquée pendant dix secondes au démarrage d'une application un peu trop gourmande. Certes, Process Lasso ne va pas booster la puissance de votre processeur, mais votre navigation sous Windows s'en verra fluidifiée.

http://bitsum.com



TUTO

ESPIONNEZ LES COULISSES D'UN SITE WEB AVEC WAPPALYZER

Vous êtes un développeur ou une agence et vous souhaitez savoir quelles technologies vos clients ou concurrents utilisent pour leurs sites ? Wappalyzer vous offre un panorama complet pour découvrir leurs secrets et s'en inspirer.

Wappalyzer est un outil en ligne qui détecte et répertorie les technologies utilisées par un site web. Avec une simple extension de navigateur ou une interface en ligne, il vous dévoile des informations précieuses telles que :

- Le CMS utilisé (WordPress, Drupal, Joomla, etc.),
- Les frameworks front-end comme React ou Vue.js,
- Les outils d'analyse comme Google Analytics,
- Les serveurs web (Apache, Nginx, etc.),
- Et bien d'autres catégories comme les bases de données, les CDN, les bibliothèques JavaScript, et les outils SEO.

Son principal objectif est donc de permettre aux utilisateurs de mieux comprendre l'écosystème technologique d'un site. Que ce soit pour une veille concurrentielle, une analyse technique approfondie, ou même pour satisfaire une simple curiosité, Wappalyzer est la solution rêvée pour obtenir ces informations clés en quelques secondes.

WAPPALYSER : COMMENT ÇA MARCHE ?

L'analyse technologique de Wappalyzer est principalement basée sur une approche heuristique. Wappalyzer maintient une vaste base de données contenant des "empreintes" ou signatures spécifiques aux technologies web. Ces signatures incluent des éléments comme des chaînes de caractères spécifiques dans les en-têtes http, des noms de fichiers ou de scripts JavaScript, des structures spécifiques dans le DOM (Document Object Model) du site. Wappalyzer applique des règles de correspondances pour détecter les technologies en comparant les données collectées sur un site à sa base de signatures. Par exemple, si un site utilise un fichier nommé wp-includes/js/wp-embed.min.js, cela indique probablement l'utilisation de WordPress. Bien que ce processus soit manuel, il est soutenu par une mise à jour continue grâce à une communauté active. Cette base de données évolue pour inclure les nouvelles technologies émergentes. Grâce à cette approche, Wappalyzer peut identifier des centaines de technologies dans plus de 50 catégories.

PREMIERS SCANS AVEC WAPPALYSER

PRATIQUE

Après inscription, la version gratuite de Wappalyzer vous permet d'analyser jusqu'à 50 sites par mois.

01› EXTENSION DE NAVIGATEUR

Wappalyzer propose des extensions pour Chrome, Firefox, et d'autres navigateurs basés sur Chromium. Une

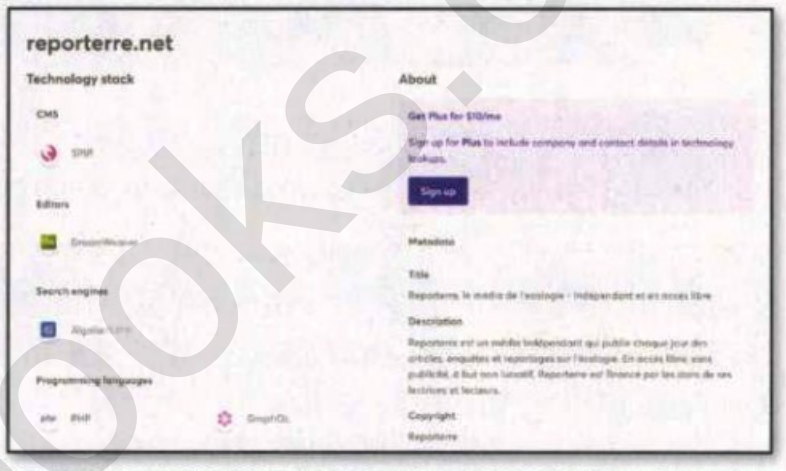
fois installée, cette extension ajoute une icône dans la barre d'outils. Cliquez dessus pour afficher instantanément les technologies d'un site web. Simple, rapide, et efficace !

02› INTERFACE EN LIGNE

Pas envie d'ajouter une extension ? Pas de problème. Rendez-vous directement sur le site officiel de Wappalyzer, entrez une URL dans le champ dédié, et obtenez les mêmes informations en cliquant sur **Technology lookup**.

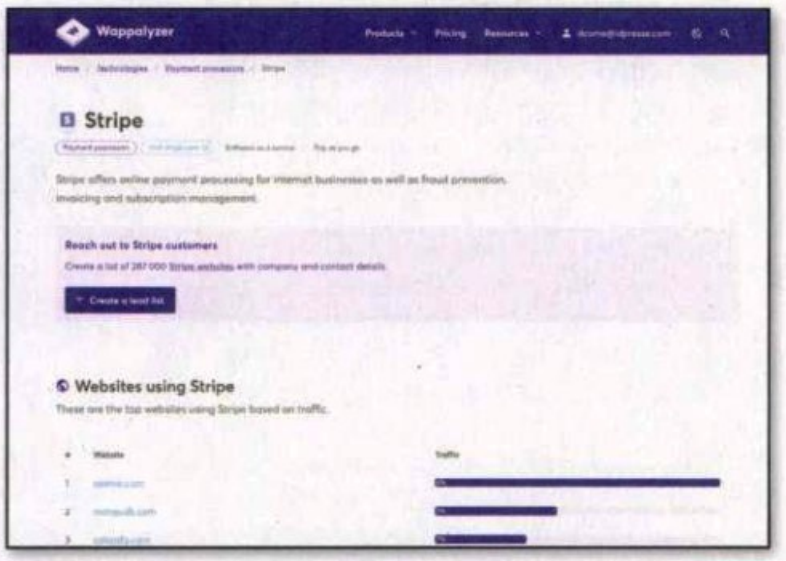
03› CATÉGORISATION DES TECHNOLOGIES

Les résultats sont organisés en catégories, ce qui permet une lecture fluide et structurée. Par exemple, vous saurez si un site utilise un CDN comme Cloudflare, un outil CRM comme HubSpot, ou une base de données comme MySQL.



04› EN SAVOIR PLUS

En cliquant sur chaque résultat, vous aurez une description de la technologie, des principaux sites dans le monde l'utilisant, de sa dynamique, de ses concurrents, etc. Idéal pour parfaire votre culture techno.



QU'APPORTE LA VERSION PAYANTE DE WAPPALYSER ?

Avec la version premium, vous accédez par exemple à une API puissante permettant d'analyser des milliers de sites simultanément. Idéal pour les agences ou les entreprises travaillant sur de grandes bases de données. La version payante permet d'exporter les résultats au format CSV ou JSON pour une intégration dans vos outils internes. En optant pour un abonnement, vous pouvez aussi suivre l'évolution technologique d'un site au fil du temps, une fonctionnalité utile pour les analyses récurrentes ou les audits. En plus des technologies détectées, la version payante propose enfin des informations complémentaires sur les entreprises propriétaires des sites analysés (taille, localisation, adresses emails, etc.).

LES PIRATES INFORMATIQUES SE DOPENT À L'IA

10 menaces qui changent les règles du jeu en 2025

L'intelligence artificielle (IA) a profondément transformé le paysage de la cybersécurité, offrant aux cybercriminels des moyens inédits pour mener des attaques plus sophistiquées et efficaces. Ce dossier explore en détail les principaux types d'attaques, l'impact de l'IA sur leurs modes opératoires, et présente des outils alimentés par l'IA utilisés par les pirates informatiques.

Les cybercriminels ont de plus en plus eu recours à des outils basés sur l'IA dans le cadre de leurs campagnes. Le groupe Lazarus a, par exemple, utilisé des images générées par l'IA pour exploiter une vulnérabilité zero-day de Chrome et voler des crypto-monnaies. Une autre tendance préoccupante concerne les groupes qui distribuent des versions détournées de modèles d'IA. Ils exploitent généralement des modèles d'IA et des bases de données en open-source couramment utilisées, auxquels ils injectent du code malveillant, ou introduisent des failles subtiles, difficiles à détecter mais largement diffusées. Les experts du Global Research and Analysis Team (GReAT) de Kaspersky estiment que « les LLM deviendront des outils standard pour la reconnaissance, l'automatisation de la détection des vulnérabilités et la génération de scripts malveillants afin d'améliorer le taux de réussite des attaques. »

« L'IA est une arme à double tranchant : tandis que les cybercriminels l'utilisent pour renforcer leurs attaques, les défenseurs peuvent exploiter sa puissance pour détecter les menaces plus rapidement et renforcer les protocoles de sécurité. Cependant, il faut veiller à exploiter les capacités de ces outils avec prudence, et veiller à ce que leur utilisation ne crée pas par inadvertance de nouvelles vulnérabilités », explique Maher Yamout, chercheur principal en sécurité au GReAT de Kaspersky.

INGÉNIERIE SOCIALE

L'ingénierie sociale exploite la manipulation psychologique pour inciter les individus à divulguer des informations sensibles ou à effectuer des actions compromettantes. Avec l'essor de l'IA, ces attaques sont devenues plus personnalisées et difficiles à détecter.

- Phishing Avancé : Les modèles de langage génératif, tels que ChatGPT, permettent de créer des courriels de phishing hautement personnalisés et convaincants, augmentant les chances de succès des attaques. Par exemple, des campagnes de phishing sophistiquées ont utilisé l'IA pour imiter le style d'écriture de collègues ou de supérieurs hiérarchiques, rendant les faux messages presque indiscernables des vrais.

- Deepfakes et clonage vocal : L'IA est utilisée pour générer des vidéos et des enregistrements audio falsifiés, imitant des individus de confiance. Ces deepfakes peuvent être employés pour manipuler des victimes lors d'escroqueries financières ou de campagnes de désinformation. Par exemple, des deepfakes ont été utilisés pour usurper l'identité de PDG lors de demandes de transferts de fonds frauduleuses.

EXEMPLES D'OUTILS

Nous avons déjà évoqué dans ce magazine les IA génératives de texte, d'images, de vidéos ou de clonage vocal. Toutes peuvent être utilisées pour tromper une cible de manière professionnelle, personnalisée et inventive. Mais d'autres outils ont été spécifiquement créés pour faciliter les activités frauduleuses :

- FraudGPT : Un modèle de langage conçu spécifiquement pour créer des contenus de phishing et la rédaction de scripts malveillants. FraudGPT est vendu sur des forums clandestins et offre des fonctionnalités telles que la génération automatique de courriels de phishing personnalisés et la création de pages de connexion falsifiées.

- WormGPT : Un autre modèle de langage utilisé par les cybercriminels pour automatiser la rédaction de courriels malveillants et de scripts d'attaque. WormGPT est conçu pour contourner les filtres anti-spam et les systèmes de détection, rendant les attaques plus difficiles à repérer.

ATTAQUES DDOS (DISTRIBUTED DENIAL OF SERVICE)

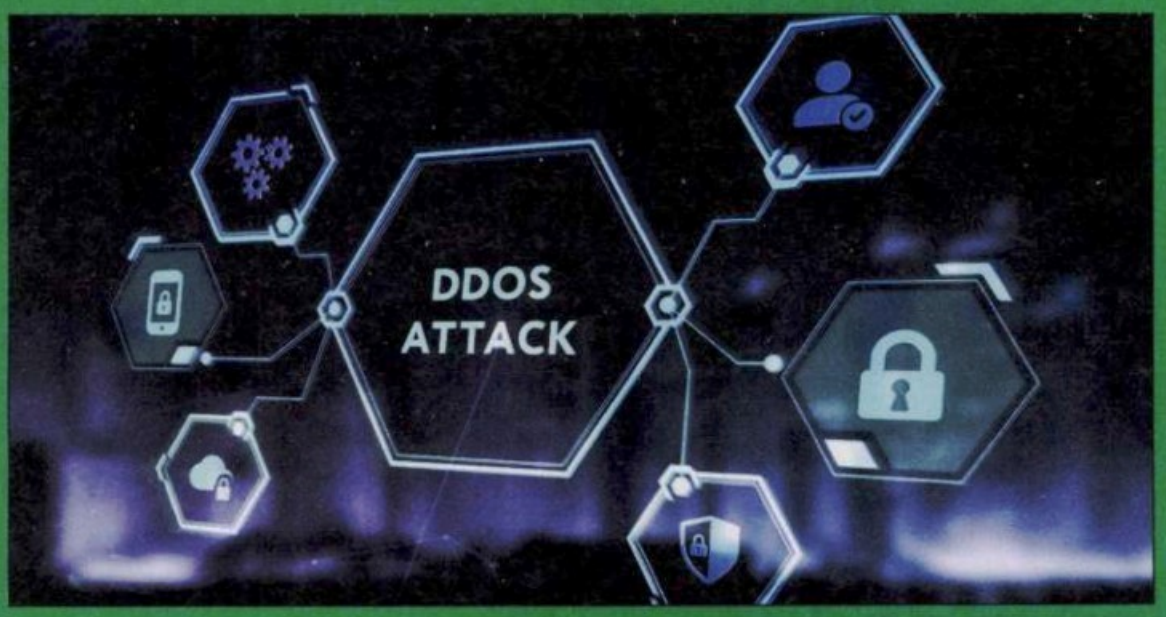
Les attaques DDoS visent à rendre un service indisponible en le submergeant de trafic malveillant. L'IA a permis d'optimiser ces attaques, les rendant plus efficaces et difficiles à contrer.

- Optimisation des attaques : L'IA peut analyser en temps réel les vulnérabilités des réseaux cibles, ajustant dynamiquement les vecteurs d'attaque pour maximiser l'impact. Par exemple, des algorithmes d'apprentissage automatique peuvent identifier les points faibles d'une infrastructure réseau et diriger le trafic malveillant de manière à provoquer un maximum de perturbations.

- Botnets intelligents : Les botnets contrôlés par l'IA peuvent coordonner des attaques de manière plus efficace, en adaptant leurs stratégies pour échapper aux systèmes de détection et de mitigation. Ces botnets peuvent également apprendre des tentatives de défense et ajuster leurs tactiques en conséquence.

EXEMPLE D'OUTIL

- ReaperAI : Un agent autonome capable de simuler et d'exécuter des cyberattaques, y compris des DDoS, en identifiant et exploitant les vulnérabilités des systèmes cibles. ReaperAI utilise des techniques d'apprentissage profond pour optimiser ses attaques et contourner les défenses.



INTRUSION

Les intrusions consistent à pénétrer illégalement dans des systèmes informatiques pour y voler des informations, saboter des données ou prendre le contrôle de ressources. L'IA est désormais un outil clé dans l'exécution de ces attaques, augmentant leur furtivité et leur précision.

- Contournement des systèmes de détection : Les systèmes de détection d'intrusions (IDS) s'appuient sur des signatures de comportements anormaux pour bloquer les attaques. Les pirates utilisent l'IA pour générer des schémas d'attaque indétectables en ajustant leurs actions en temps réel pour paraître légitimes. Par exemple, une intrusion pourrait être fragmentée en de multiples petites requêtes apparemment bénignes, passant sous les radars de détection.

- Reconnaissance préalable avec l'IA : Avant une intrusion, les pirates utilisent des outils alimentés par l'IA pour cartographier le réseau cible, identifier les systèmes vulnérables, et concevoir des chemins optimaux pour pénétrer sans être détectés.

EXEMPLES D'OUTILS

- DeepExploit : DeepExploit est un outil alimenté par des algorithmes de deep learning qui automatise les phases de reconnaissance, d'exploration et d'exploitation

des vulnérabilités. Il intègre des frameworks comme Metasploit pour lancer des attaques, tout en apprenant en continu des résultats obtenus pour améliorer ses tactiques. Son intelligence adaptative permet une exécution rapide et efficace des intrusions, même sur des systèmes bien protégés.

- Mimikatz AI : Une version améliorée de l'outil bien connu Mimikatz, alimentée par l'IA. Ce logiciel est capable de récupérer les données d'authentification stockées dans la mémoire d'un système cible. L'ajout de l'IA permet d'automatiser la recherche de failles spécifiques dans les configurations système ou les politiques de sécurité.

ATTAQUES PAR RANSOMWARE (RANÇONGICIEL)

Les attaques par ransomware consistent à infecter un système informatique avec un logiciel malveillant qui chiffre les données et exige une rançon pour en restituer l'accès. Les pirates ciblent généralement des entreprises ou des institutions critiques, maximisant ainsi la pression pour payer.

- Ciblage précis : Les algorithmes de machine learning analysent les comportements et les données des cibles potentielles pour identifier les entreprises ou individus les plus susceptibles de payer une rançon.

- Chiffrement intelligent : L'IA optimise le processus de chiffrement des données en ciblant spécifiquement

> Les attaques par rançongiciels se multiplient depuis cinq ans. L'IA va encore davantage industrialiser cette menace.

les fichiers les plus critiques et en laissant intacts ceux nécessaires pour maintenir le système en fonctionnement minimal (augmentant ainsi la pression pour payer).

- Contourner les défenses : Les ransomwares alimentés par l'IA ajustent leur comportement pour échapper aux systèmes de détection basés sur des modèles traditionnels.

EXEMPLE D'OUTIL

- RaaS avec IA (Ransomware-as-a-Service) : Certains groupes criminels proposent des plateformes alimentées par l'IA, où les attaquants non techniques peuvent facilement créer et déployer des ransomwares sophistiqués. Bien que les noms de ces outils évoluent constamment, des groupes comme LockBit ou BlackCat utilisent l'IA dans leurs stratégies.

VOL DE DONNÉES

Le vol de données implique l'accès non autorisé à des informations sensibles. L'IA facilite la détection et l'exploitation des vulnérabilités permettant ces exfiltrations.

- Analyse des Vulnérabilités : Les algorithmes d'IA scannent les systèmes pour identifier les failles de sécurité exploitables, priorisant celles qui offrent le plus grand potentiel d'exfiltration de données. Par exemple, des outils d'IA peuvent analyser le trafic réseau pour détecter des anomalies indiquant la présence de vulnérabilités.

- Exfiltration Discrète : L'IA peut masquer les activités de vol de données en les camouflant parmi le trafic légitime, rendant la détection plus difficile pour les systèmes de sécurité. Des techniques telles que le chiffrement adaptatif et la modulation du taux de transfert sont utilisées pour éviter de déclencher des alertes.

EXEMPLES D'OUTILS

- SnatchBot : Cet outil, initialement conçu comme une plateforme légitime de création de bots conversationnels, a été détourné par certains cybercriminels. Les bots créés avec SnatchBot peuvent automatiser des campagnes de phishing sophistiquées pour extraire des informations sensibles des utilisateurs. Grâce à l'apprentissage machine, les bots

ajustent leurs interactions en fonction des réponses reçues, rendant les tentatives de vol de données plus convaincantes.

- DarkTrace AI : Bien que DarkTrace soit une solution de cybersécurité, des pirates ont analysé ses méthodes pour développer leurs propres outils d'exfiltration de données. En inversant le principe, ces outils utilisent des algorithmes de machine learning pour détecter les fenêtres d'opportunité où les systèmes de détection sont moins vigilants (périodes de faible trafic, mises à jour système) pour exfiltrer discrètement des informations critiques.

CRACKAGE DE MOTS DE PASSE

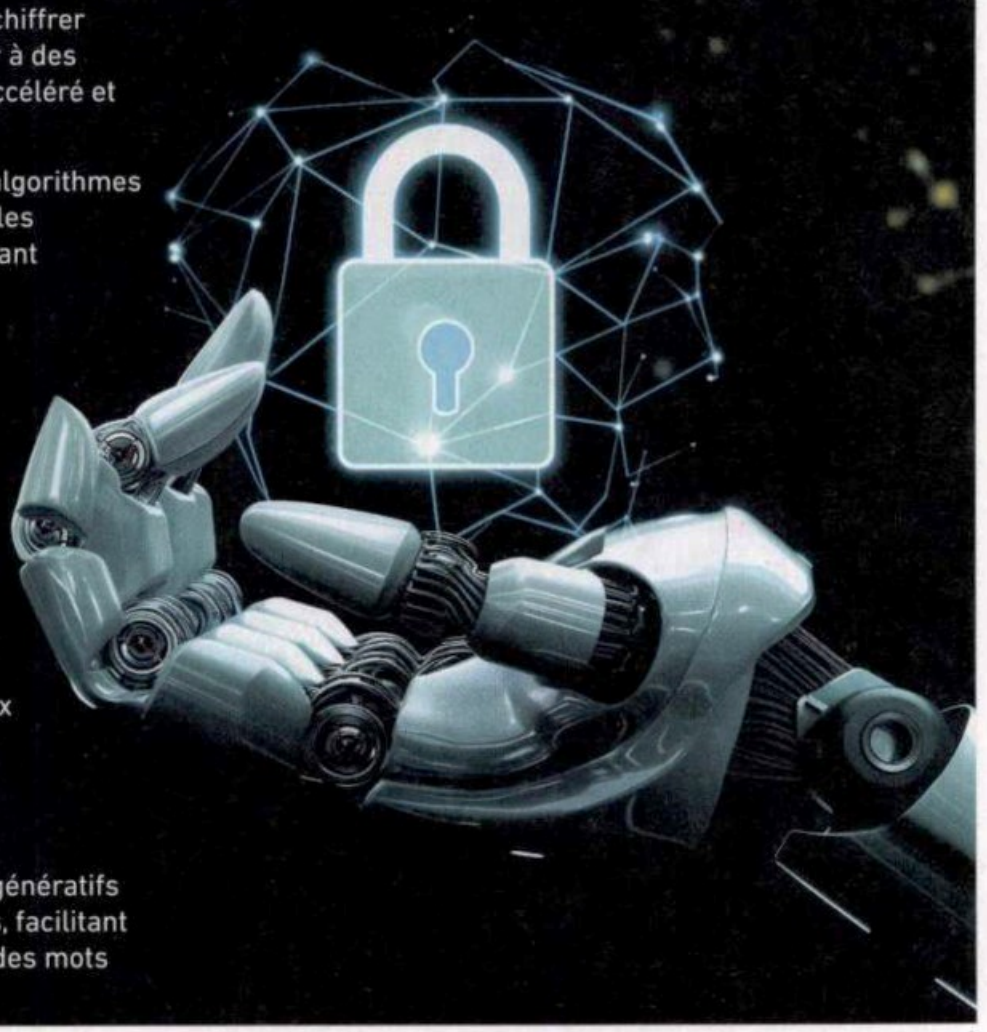
Le crackage de mots de passe consiste à déchiffrer ou deviner des mots de passe pour accéder à des systèmes protégés. L'IA a considérablement accéléré et sophistiqué ce processus.

- Attaques par Force Brute Améliorées : Les algorithmes d'apprentissage automatique peuvent prédire les schémas de création de mots de passe, réduisant le nombre de tentatives nécessaires pour les craquer. Par exemple, des modèles entraînés sur des bases de données de mots de passe compromis peuvent générer des listes de mots de passe probables, augmentant l'efficacité des attaques par force brute.

- Attaques par Dictionnaire Personnalisé : L'IA peut générer des dictionnaires de mots de passe personnalisés en se basant sur les informations personnelles des victimes, telles que les noms, dates de naissance ou centres d'intérêt, souvent extraites des réseaux sociaux. Cela rend les attaques plus ciblées et augmente les chances de succès.

EXEMPLE D'OUTIL

- PassGAN : Utilise des réseaux antagonistes génératifs (GAN) pour créer des mots de passe probables, facilitant le crackage. PassGAN est capable de générer des mots de passe qui ne figurent pas dans les dictionnaires traditionnels, rendant les attaques plus efficaces contre les mots de passe complexes ou uniques.



ATTAQUES D'ADVERSARIAL MACHINE LEARNING

Ces attaques visent spécifiquement les systèmes d'IA eux-mêmes, comme les modèles d'apprentissage automatique utilisés pour la détection de menaces, la reconnaissance faciale ou la classification des données. Les pirates parviennent à introduire des données dans la base d'apprentissage d'une IA pour fausser ses résultats ou créer des vulnérabilités. Ces données peuvent être des images, un texte, un son, du code, des datas, ... imperceptibles pour l'humain.

- **Data poisoning :** Les attaquants injectent des données malveillantes ou biaisées dans les ensembles d'entraînement pour perturber les modèles d'IA.

- **Tromper l'IA :** Les techniques adversariales génèrent des entrées spécialement conçues pour tromper les modèles d'IA en lui fournissant des informations fausses ou contradictoires. C'est notamment très efficace quand l'attaque cible des IA utilisées sur des bases de données internes (entreprise, administration, etc.).

EXEMPLE D'OUTIL

- **CleverHans Toolkit :** Bien qu'il s'agisse d'un outil académique pour tester la robustesse des modèles, des cybercriminels pourraient détourner ses fonctionnalités pour concevoir des attaques adversariales.

ATTAQUES SUR LES SYSTÈMES IOT (INTERNET DES OBJETS)

Les systèmes IoT regroupent des objets connectés, souvent dotés de faibles capacités de sécurité, comme des caméras de surveillance, des thermostats ou des appareils médicaux. Les attaques visent à prendre le contrôle de ces dispositifs pour voler des données, perturber leur fonctionnement ou les intégrer dans des botnets.

- **Reconnaissance des Appareils :** L'IA scanne les réseaux pour identifier les appareils IoT vulnérables, comme des caméras, thermostats ou routeurs, souvent moins protégés que les serveurs principaux.

- **Botnets IoT Intelligents :**
Les botnets comme Mirai ont ouvert la voie à des versions plus avancées alimentées par l'IA, capables de s'adapter en temps réel aux changements de configuration réseau et d'échapper aux efforts de neutralisation.

EXEMPLE D'OUTIL

- **IoT Inspector (modifié) :** Une version détournée de cette suite d'outils légitimes pour l'analyse de sécurité IoT peut être utilisée pour automatiser des campagnes d'infection massive.

ATTAQUES SUR LES ALGORITHMES DE BLOCKCHAIN ET DE CRYPTOMONNAIES

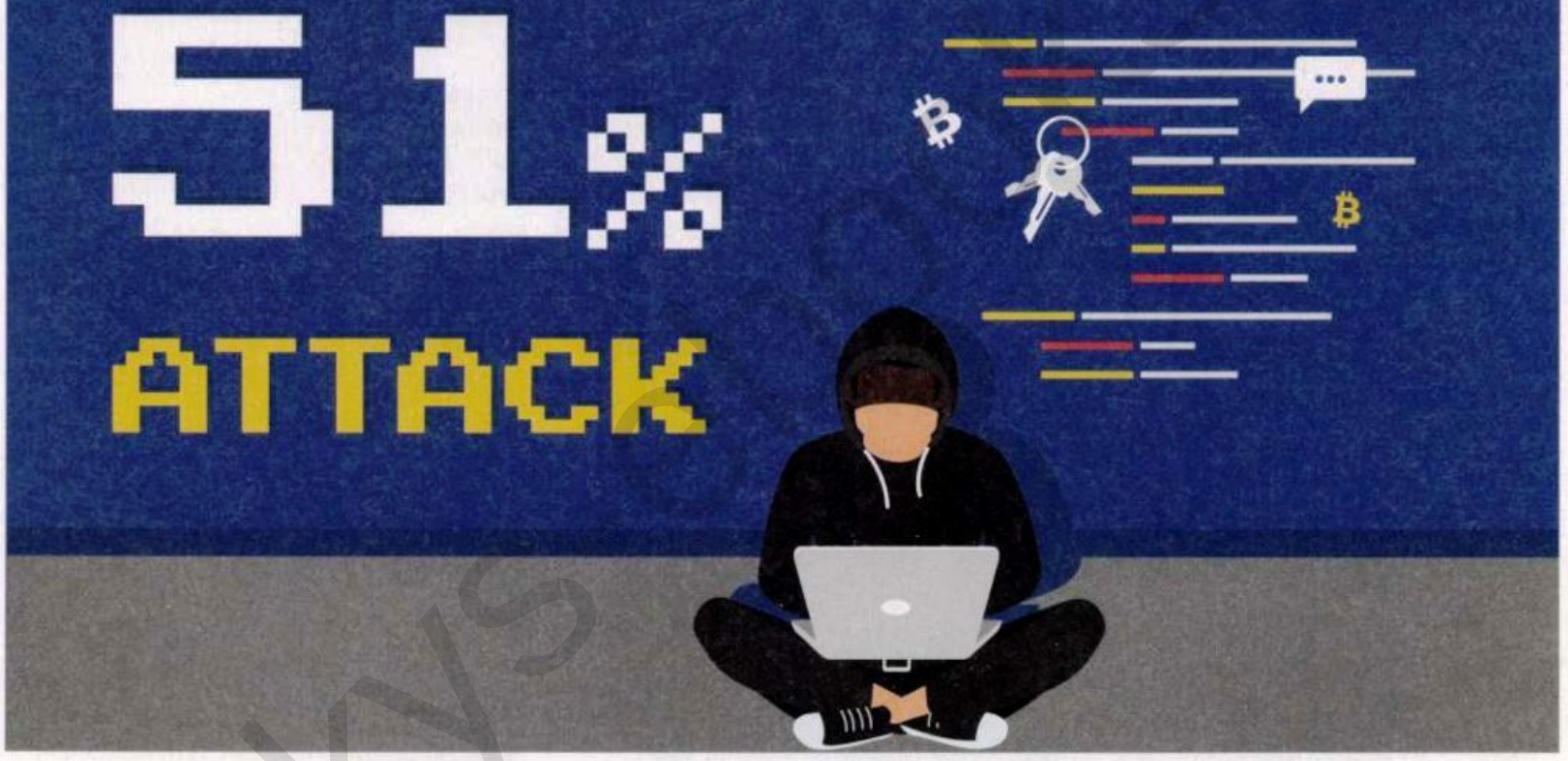
Les blockchains sont des systèmes de stockage de données décentralisés, souvent utilisés pour sécuriser les transactions de cryptomonnaies. Ces attaques exploitent des vulnérabilités dans les algorithmes ou les smart contracts pour voler des fonds, perturber des opérations ou manipuler des transactions (comme les doubles dépenses).

- Exploitation des Contrats Intelligents :
L'IA identifie des failles dans les smart contracts, permettant des attaques comme le siphonnage de fonds.

- Attaques de doubles dépenses :
Les algorithmes prédictifs améliorent les chances de réussite des attaques par double dépense (utiliser frauduleusement le même bitcoin pour deux transactions différentes en même temps). Car malgré l'ingéniosité de la blockchain, il existe potentiellement des risques probabilistes de double validation. L'IA peut aider à optimiser les chances de parier sur ces calculs statistiques pointus.

EXEMPLE D'OUTIL

- EtherSec : Un outil spécialisé dans l'analyse des smart contracts, qui peut être détourné pour cibler des failles.



ATTAQUES DE DÉSINFORMATION ET DE MANIPULATION

Ces attaques visent à diffuser massivement des informations trompeuses pour influencer l'opinion publique, déstabiliser des institutions ou manipuler des marchés. Elles reposent sur la propagation rapide de contenus sur les réseaux sociaux ou les médias.

- Création Automatisée de Contenus :
Les modèles de langage génératif comme GPT sont utilisés pour inonder les plateformes sociales de désinformation, amplifiant les campagnes de propagande ou influençant des opinions publiques.

- Manipulation d'Événements Réels :
Des deepfakes couplés à des bots sociaux automatisés créent des campagnes convaincantes, souvent pour influencer les marchés financiers ou les politiques.

EXEMPLE D'OUTIL

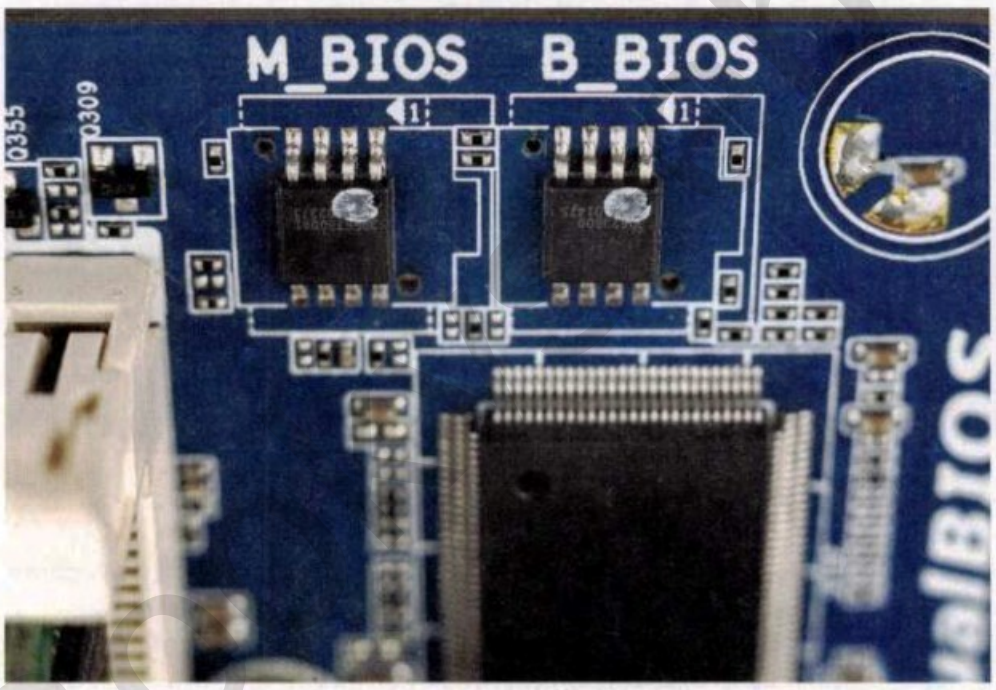
- Botnets Sociaux avec IA : Ces réseaux utilisent des agents conversationnels alimentés par l'IA pour interagir avec des humains sur les réseaux sociaux de manière crédible, augmentant leur efficacité.

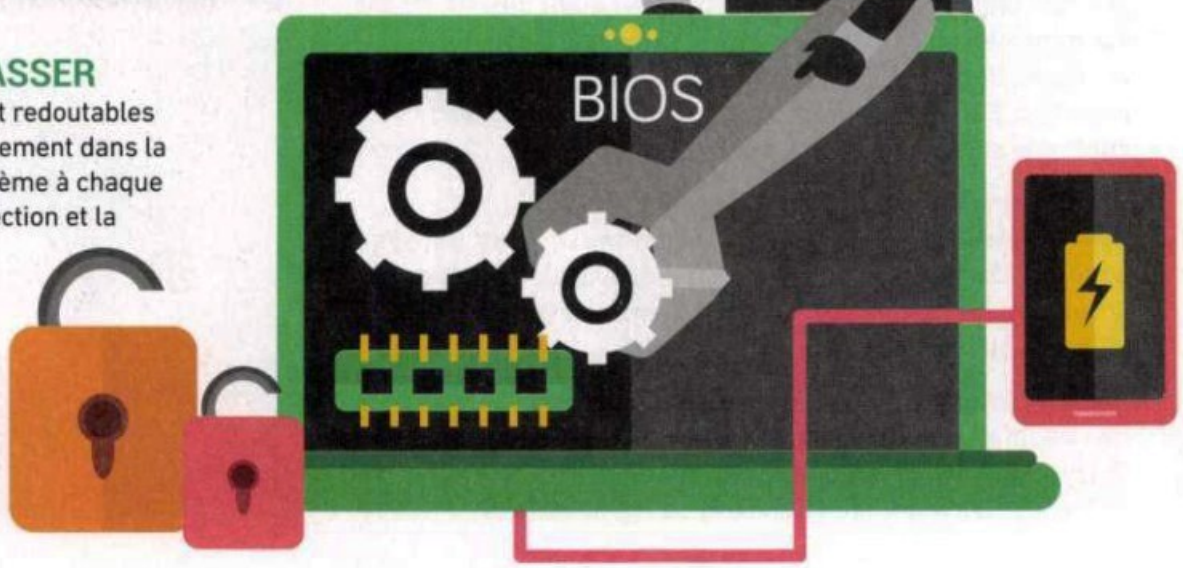
3 QUESTIONS SUR LES ATTAQUES DU FIRMWARE (BIOS/UEFI)

Au démarrage, un Bios corruptible

① ATTAQUES DU FIRMWARE : QU'EST-CE QUE C'EST ?

Le firmware de votre ordinateur (BIOS ou UEFI) est le premier élément à se lancer au démarrage. Il initialise vos composants matériels (processeur, RAM, périphériques) avant de passer le relais au système d'exploitation (Windows, Linux, macOS, etc.). Si des cybercriminels parviennent à manipuler ce niveau bas, ils peuvent ensuite installer des logiciels malveillants qui se lanceront avant même l'OS et contourneront la plupart des protections (antivirus, pare-feu, etc.). Au niveau du BIOS/UEFI, l'attaquant peut potentiellement accéder à toutes les ressources matérielles, voler des informations sensibles ou installer des backdoors.





DIFFICILE DE S'EN DÉBARRASSER

De telles attaques sont particulièrement redoutables car elles peuvent persister (loger directement dans la puce du BIOS/UEFI) et réinfecter le système à chaque démarrage, rendant très difficile la détection et la neutralisation. Même si vous reformatez ou réinstallez Windows, un firmware compromis peut réinjecter le malware dans l'OS. Les antivirus et autres solutions de sécurité de l'OS sont rarement capables de scanner ou nettoyer directement le firmware.

2 COMMENT FONT LES PIRATES ?

Voici les principaux vecteurs d'attaque :

a# Clés USB infectées
Lorsqu'un ordinateur démarre, le BIOS/UEFI peut charger certains fichiers depuis un périphérique USB pour booter un système, mettre à jour le firmware ou exécuter des utilitaires de diagnostic. Si la fonctionnalité de boot USB est autorisée (et mal sécurisée), un attaquant peut utiliser une clé USB modifiée pour injecter du code malveillant dans la mémoire du BIOS/UEFI.

AU DÉMARRAGE, VOTRE BIOS PEUT CHARGER UN PROGRAMME MALVEILLANT VENANT D'UN PÉRIPHÉRIQUE EXTERNE... ALORS MÊME QUE VOTRE ANTIVIRUS N'EST PAS ENCORE ACTIF.

Par exemple, le malware Mebromi ciblait le BIOS Award/Phoenix. Dans certains scénarios, si la mise à jour était lancée depuis une clé USB malveillante, Mebromi réécrivait une portion du BIOS pour y insérer son code.

b# Exploitation de failles logicielles
Un malware déjà présent sur le PC (via une infection traditionnelle) peut escalader ses privilèges en profitant d'une faille dans les pilotes ou les outils de mise à jour fournis par le constructeur. Il peut alors écrire directement dans la mémoire flash du BIOS/UEFI ou exécuter des commandes spécifiques (grâce à un pilote vulnérable) qui contournent les protections logicielles.
Le rootkit LoJax (attribué au groupe APT28/Fancy Bear) exploitait ainsi des vulnérabilités logicielles pour injecter un composant malveillant dans la partition EFI, lui permettant de se réinstaller à chaque redémarrage. Son objectif : assurer un contrôle continu de la machine pour espionner, voler des données ou déployer d'autres malwares.

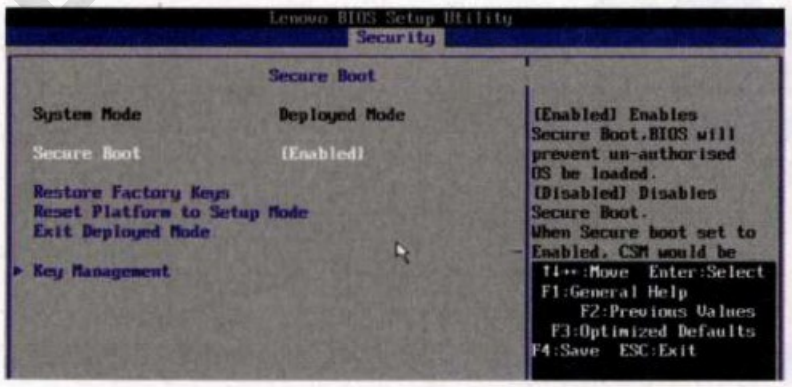
c# Mises à jour malveillantes
Les fabricants de cartes mères ou de PC proposent régulièrement des firmwares officiels (fichiers ".bin", ".rom", etc.) à installer via un utilitaire. Dans un scénario d'usurpation, le pirate se fait passer pour la marque (ou compromet le serveur de mise à jour) pour fournir un fichier modifié.

d# Exploits zero-day
Certaines failles UEFI/BIOS ne sont pas encore découvertes par les équipes de sécurité ("zero-day"). Les APT (Advanced Persistent Threats) peuvent en bénéficier. Ils modifient la séquence de boot ou désactivent des protections comme le Secure Boot, sans laisser de traces facilement détectables.

3 COMMENT SE PROTÉGER ?

a# Mettre à jour le BIOS/UEFI
Les fabricants de cartes mères ou de PC publient parfois des correctifs de sécurité et des mises à jour pour le BIOS/UEFI. Rester sur une version obsolète expose à des vulnérabilités connues.

b# Activer le Secure Boot (si disponible)
Le Secure Boot, disponible sur les systèmes UEFI récents, vérifie la signature des composants logiciels qui se lancent au démarrage. Ainsi, un malware modifiant l'EFI ou le bootloader sans signature valide sera bloqué.
Pour accéder au BIOS/UEFI, il faut généralement appuyer sur Suppr, F2 ou Esc au démarrage. Recherchez l'option **Secure Boot** ou (**Démarrage sécurisé**). Activez **Enabled** si elle est désactivée. Enregistrer les modifications et redémarrer.



c# Désactiver les maj automatiques depuis des sources non vérifiées
Des marques proposent parfois la mise à jour automatique du BIOS via Internet. Or, si cette fonctionnalité est mal sécurisée (ou si l'outil utilise un protocole obsolète), un attaquant pourrait injecter un firmware falsifié. Dans le BIOS/UEFI, cherchez une option du type **Internet BIOS Update** ou **Network BIOS Flash**. Désactivez cette option si vous ne faites pas confiance à la méthode de téléchargement. Préférez toujours un téléchargement manuel via le site officiel.

d# Ne pas brancher de clés USB "douteuses" au démarrage
Certaines attaques exploitent le fait que le BIOS/UEFI peut lire les informations sur les clés USB connectées (bootloader, fichiers EFI...). Des attaquants peuvent profiter d'une faille pour injecter du code malveillant dans le firmware. Désactivez également le **Boot from USB** dans le BIOS si vous n'en avez pas besoin.

e# Surveiller les signes d'une compromission
Un firmware compromis peut manifester des symptômes inhabituels comme la réinitialisation subite des paramètres BIOS. Mais c'est loin d'être toujours le cas. Certains fabricants proposent des utilitaires dédiés aux scans de bas niveau pour vérifier l'intégrité du BIOS (ex. HP Sure Start, Lenovo ThinkShield, etc.). Réalisez ces contrôles si vous soupçonnez une compromission.

SÉLECTION

LES MEILLEURES PLATEFORMES POUR SE FORMER

Le hacking éthique attire autant les curieux que les experts en quête de défis techniques. Et bonne nouvelle : Internet regorge de ressources gratuites pour s'initier ou se perfectionner dans ce domaine.

HACK THE BOX > L'ARÈNE DES HACKERS MODERNES

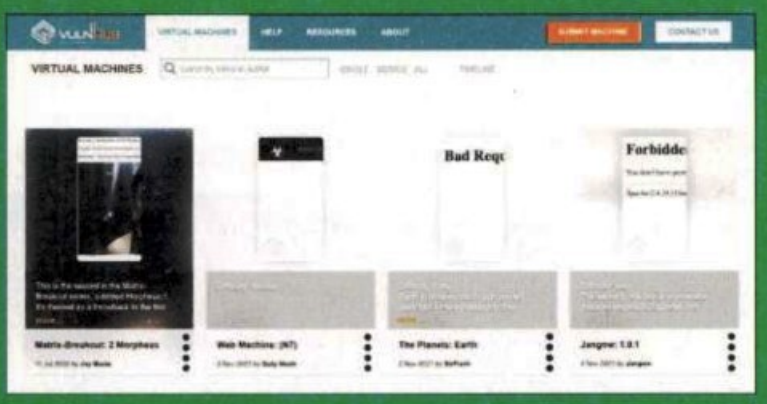
Hack The Box est un incontournable pour quiconque souhaite explorer le hacking éthique de manière interactive et ludique. La plateforme se présente comme une arène où chaque utilisateur peut tester ses compétences sur des machines virtuelles pleines de vulnérabilités à exploiter. Le concept ? Vous apprenez en « jouant », dans un environnement totalement sécurisé.

L'expérience démarre dès l'inscription : vous devrez résoudre un premier challenge pour décrocher votre invitation. Une fois à l'intérieur, les possibilités s'ouvrent à vous : défis de sécurité réseau, cryptographie, exploitation web, reverse engineering, et bien plus. Les débutants pourront s'appuyer sur la communauté mondiale pour progresser, tandis que les experts trouveront des machines redoutables à leur hauteur.

En revanche, il faut noter que l'interface et les exercices sont uniquement en anglais. Mais pour ceux qui n'ont pas peur de retrousser leurs manches, Hack The Box est une référence incontournable.

Lien : www.hackthebox.com

VULNHUB > LE LABORATOIRE HORS LIGNE



Si vous préférez travailler hors ligne, VulnHub est fait pour vous. Cette plateforme propose une bibliothèque de machines virtuelles prêtes à être téléchargées et utilisées dans un environnement local. Le principe est simple : chaque machine est un casse-tête à résoudre, avec des scénarios réalistes permettant de simuler des attaques ou des audits de sécurité.

Ce qui distingue VulnHub, c'est sa simplicité d'accès. Pas d'inscription requise, tout est gratuit et téléchargeable en quelques clics. Une fois une machine en main, vous pouvez l'importer dans VirtualBox ou VMware pour commencer votre exploration.

Certains critiques lui reprocheront son manque d'interactivité par rapport à des plateformes comme Hack The Box. Mais VulnHub reste un excellent outil pour développer ses compétences techniques en toute autonomie. Téléchargez vos premières machines.

Lien : www.vulnhub.com

TRYHACKME > APPRENEZ EN DOUCEUR

Parmi les plateformes de hacking éthique, TryHackMe se démarque par son accessibilité et sa pédagogie. Idéal pour les débutants, ce site propose des exercices guidés dans des environnements cloud. Pas besoin de compétences préalables ou de configuration complexe : tout est clé en main.
TryHackMe propose des salles thématiques, chacune recréant un scénario réaliste. Que vous souhaitiez apprendre les bases du hacking ou vous préparer à des certifications comme CEH ou CompTIA, tout est prévu. Une communauté dynamique permet également d'échanger et de progresser ensemble. Seul bémol, certaines salles avancées nécessitent un abonnement, mais le contenu gratuit est déjà impressionnant.

Lien : tryhackme.com

HACK THIS SITE

> LA VIEILLE ÉCOLE TOUJOURS EN FORME

Hack This Site est une véritable institution dans l'univers du hacking éthique. Lancé dans les années 2000, ce site propose une expérience éducative complète avec des missions interactives. Sécurité web, programmation, cryptographie, chaque domaine y est exploré à travers des défis conçus pour vous faire réfléchir.
Ce qui distingue Hack This Site, c'est son ambiance old school et sa communauté accueillante. Les forums sont remplis de passionnés prêts à partager astuces et conseils. C'est une excellente porte d'entrée pour les débutants, bien que l'interface puisse paraître un peu datée.

Lien : www.hackthissite.org

CYBRARY

> LA PLATEFORME ACADÉMIQUE

Enfin, Cybrary s'impose comme une ressource incontournable pour ceux qui recherchent une approche plus académique. Ici, pas de machines à pirater, mais une collection impressionnante de

cours en ligne couvrant tous les aspects de la cybersécurité et du hacking éthique. Vidéos, guides pratiques et parcours certifiants sont au rendez-vous.
Là encore, la barrière de la langue peut freiner certains utilisateurs, car le contenu est principalement en anglais. Mais pour ceux qui souhaitent se former aux certifications reconnues, Cybrary est un choix solide.

Lien : www.cybrary.it/free-content

ET LES RESSOURCES FRANCOPHONES ?

Le hacking éthique a ses adeptes francophones, et plusieurs plateformes méritent une mention spéciale. **Le Blog du Hacker (www.leblogduhacker.fr)**, par exemple, est une mine d'or pour les débutants. Tutoriels vidéo, conseils sur les outils à utiliser, ou encore stratégies pour détecter des vulnérabilités, tout y est présenté avec pédagogie.

50h de cours gratuits pour se

De son côté, **Jedha (www.jedha.co/julie)** propose une initiation gratuite au hacking éthique dans le cadre d'une formation plus large en cybersécurité. Des modules gratuits permettent de découvrir les bases tout en explorant des aspects concrets comme l'audit de sécurité.

DÉCRYPTAGE

RÉSEAUX MESH : CRÉEZ VOTRE RÉSEAU INTERNET CHIFFRÉ

Les réseaux mesh (ou « réseaux maillés ») sont des réseaux qui vous permettent d'accéder au Web ou d'échanger des données de façon chiffrée et en utilisant d'autres ordinateurs connectés comme relais. Rapide et sécurisé pour l'échange de fichiers. Mais il s'agit aussi d'une alternative aux VPN ou aux réseaux anonymes comme TOR ou I2P.

Pas envie de payer un VPN et Tor vous inquiète ? Il existe un autre chemin pour échanger anonymement et accéder au Web de façon sécurisée : les réseaux mesh. Ces réseaux interconnectés passent par les ordinateurs des différents membres, qui servent de relais. Un réseau mesh est un réseau dans lequel chaque nœud (ou « point d'accès ») est capable de communiquer directement avec d'autres nœuds, sans passer obligatoirement par un routeur centralisé. De nombreuses solutions payantes existent (comme Meshnet pour les particuliers chez NordVPN). Mais, heureusement, vous pouvez aussi adopter des outils gratuits performants comme Tailscale et Zerotier. Vous trouverez plus loin un guide complet pour configurer Tailscale.

« UN VPN COMMERCIAL COMME NORDVPN PROPOSE PAR EXEMPLE SA SOLUTION MESHNET CLÉ EN MAIN. L'OBJECTIF : VOUS PERMETTRE D'UTILISER DES PASSERELLES ANONYMISÉES AUX QUATRE COINS DU MONDE SANS ÊTRE ESTAMPILLÉ « SERVEUR NORDVPN » ET DE CRÉER VOTRE PROPRE RÉSEAU D'ÉCHANGES DIRECTS. MAIS DES SOLUTIONS GRATUITES EXISTENT AUSSI, COMME TAILSCALE (LIRE PLUS LOIN) OU ZEROTIER.

MESH FERMÉ OU OUVERT

À domicile, un réseau mesh vous permet de connecter plusieurs appareils sans passer par votre box. Vous créez ainsi un Intranet fermé et sécurisé, stable et rapide. Mais vous pouvez aussi vous connecter à des ordinateurs distants. Ici, vos données passeront bien par votre box FAI. Mais elles seront chiffrées avant d'être envoyées vers votre relais mesh situé chez le voisin ou à l'autre bout du monde.

Dans un réseau classique, la box ou un serveur distant joue le rôle du « maître d'orchestre » : tous les appareils doivent transiter par lui pour accéder à Internet ou échanger des données en local. Avec un réseau mesh comprenant plusieurs appareils, la structure est décentralisée : si un nœud est hors service, les autres peuvent continuer de communiquer en empruntant d'autres chemins. Car chaque nœud est interconnecté à plusieurs autres, créant de multiples routes possibles. Si un nœud est congestionné ou tombe en panne, les données sont automatiquement redirigées vers un autre. Et l'on peut facilement ajouter ou retirer des nœuds pour agrandir ou réduire la taille du réseau.

> Un réseau résilient et anonymisé, local ou mondial.

UN RÉSEAU MESH PEUT-IL REMPLACER MON FAI ?

Non. Pour bénéficier de toutes les fonctionnalités d'un réseau mesh, qu'il soit Wi-Fi ou virtuel, la plupart des utilisateurs gardent une box ou un routeur relié à un FAI. Si vous montez un réseau mesh purement local (en Wi-Fi ou via câbles Ethernet) pour relier des appareils au sein d'un même bâtiment, vous pouvez vous passer d'une connexion Internet. Ce réseau fonctionnera en vase clos, idéal pour partager des fichiers localement ou faire du streaming entre deux machines. Mais sans FAI, pas d'accès à des services extérieurs (mail, web, cloud, etc.).

À QUOI ÇA SERT ? 5 EXEMPLES D'USAGES

1) COUVRIR DE GRANDES SURFACES

Vous avez des problèmes de couverture Wi-Fi dans certaines pièces de votre maison ? Au lieu d'acheter un unique routeur ultra-puissant (et souvent onéreux), vous pouvez placer plusieurs petits nœuds maillés pour couvrir uniformément chaque recoin.

2) SÉCURISER LE TRAVAIL COLLABORATIF

En entreprise et même à domicile, vous pouvez créer un réseau mesh qui sera déconnecté de l'Internet public. Vous pouvez échanger des données entre vous sans qu'un tiers extérieur ne puisse accéder à votre réseau par une porte dérobée.

3) AMÉLIORER LA FIABILITÉ ET LA RÉSILIENCE

Grâce aux liaisons multiples entre nœuds, si l'un d'entre eux est en panne ou trop sollicité, le trafic peut être redirigé vers un chemin secondaire, sans coupure de service. C'est ce qui rend un réseau mesh particulièrement intéressant pour des environnements critiques (home cinéma, gaming en ligne, surveillance vidéo, IoT, etc.). Plus un réseau mesh intègre d'appareils connectés aux quatre coins du monde, plus la chance de trouver un « chemin » est grande.

4) FACILITER LA COLLABORATION À DISTANCE

Pour ceux qui cherchent à relier différents appareils sur un réseau chiffré et décentralisé — que ce soit pour le télétravail ou pour partager des fichiers en toute sécurité — un réseau mesh virtuel peut constituer une solution souple et sécurisée.

5) CHANGER D'ADRESSE IP

En combinant les atouts d'un réseau mesh virtuel (connexion chiffrée, peer-to-peer, topologie flexible) avec la notion de « nœud de sortie », vous pouvez créer un « VPN maison » sur mesure. Cette passerelle distante

vous permettra de faire transiter tout votre trafic Internet à travers un point unique possédant une autre adresse IP. **Lire page 40**.

TUTO

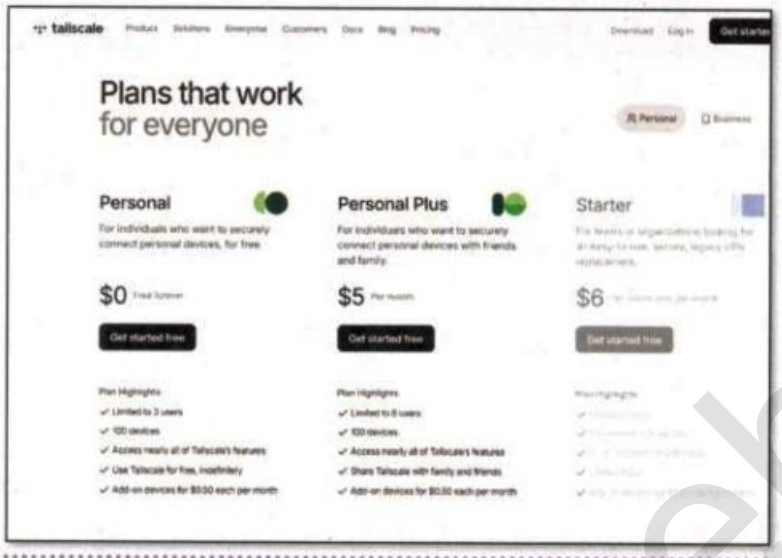
CONFIGUREZ VOTRE MESH GRATUIT AVEC TAILSCALE

PRATIQUE

Tailscale offre une version gratuite pour un usage personnel limité. Nous verrons ici comment créer votre compte puis votre premier réseau mesh en connectant deux de vos appareils.

01› ACCÈS GRATUIT

Allez sur **Tailscale.com**, puis **Pricing** et cliquez sur l'onglet **Personal**. Créer un compte Tailscale. Vous aurez accès à la version gratuite (limitée à 3 utilisateurs par compte) mais qui vous donne accès à la majeure partie des fonctionnalités. Cliquez sur **Get started free**.



02› CRÉER SON COMPTE

Créez maintenant votre compte Tailscale. Vous êtes obligé de passer par un provider (compte Google, Microsoft, etc.). Préférez Github ou OIDC si vous possédez de tels comptes. Choisissez quand l'interface vous le demandera **Personal use** puis cliquez sur **Download Tailscale for Windows** (ou tout autre système d'exploitation de votre choix).

03› INSTALLATION

Une fois téléchargé, lancez l'exécutable et installez Tailscale sur votre appareil. Il sera disponible via son icône à 9 points dans votre centre de notification de la barre des tâches, tout en bas à droite de votre écran. Faites un clic droit puis choisissez **Log In**.

04› SE CONNECTER

Vous basculez alors sur l'identification via votre navigateur Internet. Renseignez votre compte. Vous êtes sur le point de connecter l'appareil sur lequel vous avez installé Tailscale à son réseau Mesh. Sous **Device details**, vous pouvez vérifiez ces infos ainsi que la clé publique qui vous est attribuée. Cliquez sur **Connect**.

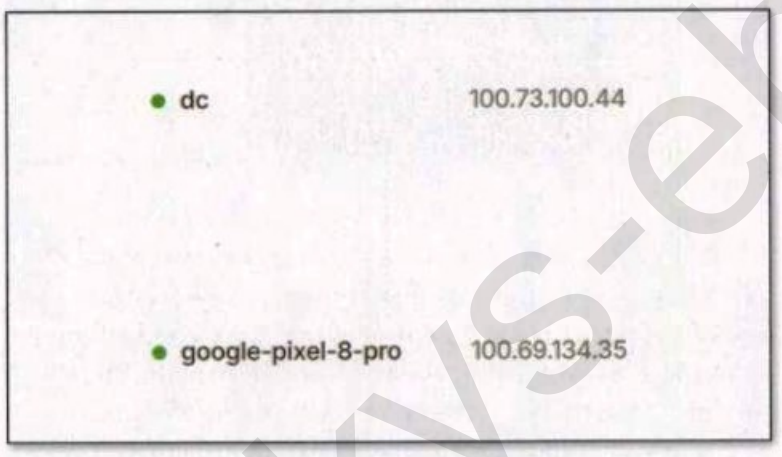
05› AJOUTER UN APPAREIL

Le nom de votre PC apparait maintenant sur votre console Tailscale disponible en ligne. Vous pouvez répéter l'opération avec le même compte mail sur

plusieurs autres appareils (PC, mobile, serveurs, etc.) pour créer votre Mesh local. Ici, nous avons connecté notre smartphone Android à notre compte.

06› MESH ET IP PRIVÉES

Tous les appareils appartenant à votre réseau mesh Tailscale disposent désormais d'une adresse



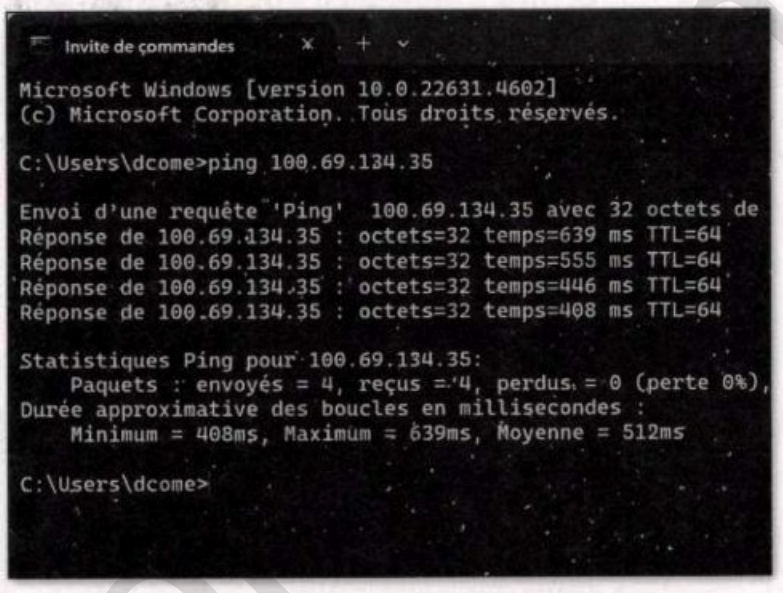
IP privée de la forme 100.x.y.z. Si vos appareils sont connectés à Tailscale, ils peuvent communiquer entre-eux, en local ou à distance via un accès Internet.

À SAVOIR

Lorsque vous activez un réseau mesh, vos données sont chiffrées avant de quitter votre appareil (PC, mobile, ...). Chez Tailscale par exemple, c'est le célèbre protocole Wireguard qui est utilisé. Si vos données transitent vers l'extérieur (Internet), elles passent par votre FAI (box ou données mobiles). Mais ce dernier ne voit qu'un flux chiffré, sans accéder au contenu réel (sites visités, documents, etc.). Votre routeur/box n'a qu'un rôle de « passerelle ». Cependant, une information importante lui demeure connue : votre adresse IP publique.

07› VÉRIFIER LA CONNEXION

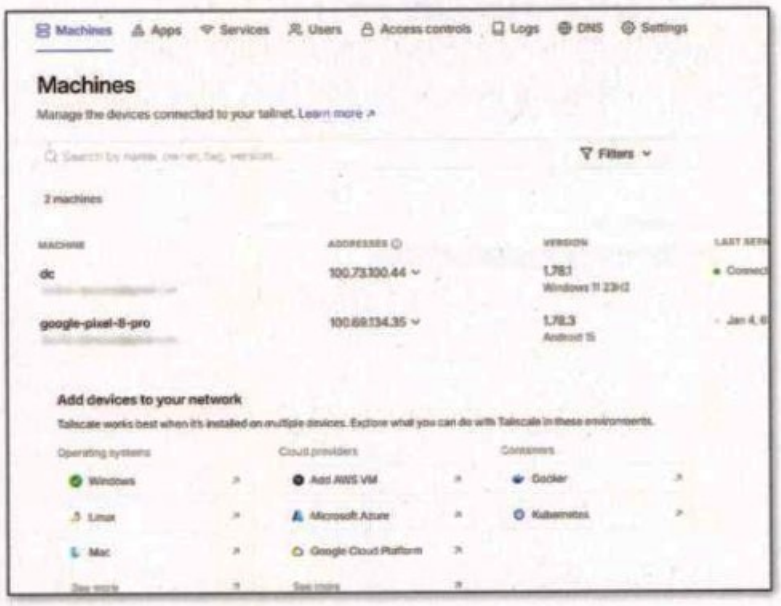
Vérifiez cette connexion en envoyant un ping depuis votre PC au second appareil. Ici, depuis l'invite de



commande Windows, exécutez **ping 100.x.y.z** (l'IP correspondant à votre second appareil, ici notre smartphone Android). Vous vérifierez que les résultats sont concluants. Revenez sur votre console Tailscale et passez à l'étape suivante en cliquant sur **Success, it works !**

08› CONSOLE D'ADMINISTRATION

Vous revenez sur la console d'administration de votre compte. Vous pouvez notamment voir les appareils enregistrés et s'ils sont bien connectés. Mais c'est



surtout ici que vous pourrez activer les fonctionnalités avancées telles que l'accès à distance ou la redirection de trafic. Vous pouvez aussi autoriser ou bloquer certains appareils et configurer des « routes » particulières pour partager un répertoire sur un NAS ou accéder à un serveur local.

TUTO

TAILSCALE TAILDROP : LE PARTAGE DE FICHIERS NATIF

PRATIQUE

Taildrop est une fonctionnalité native de Tailscale permettant de s'envoyer des fichiers entre appareils connectés au même compte Tailscale. C'est simple, tout est déjà chiffré, et cela évite de configurer des partages de dossiers.

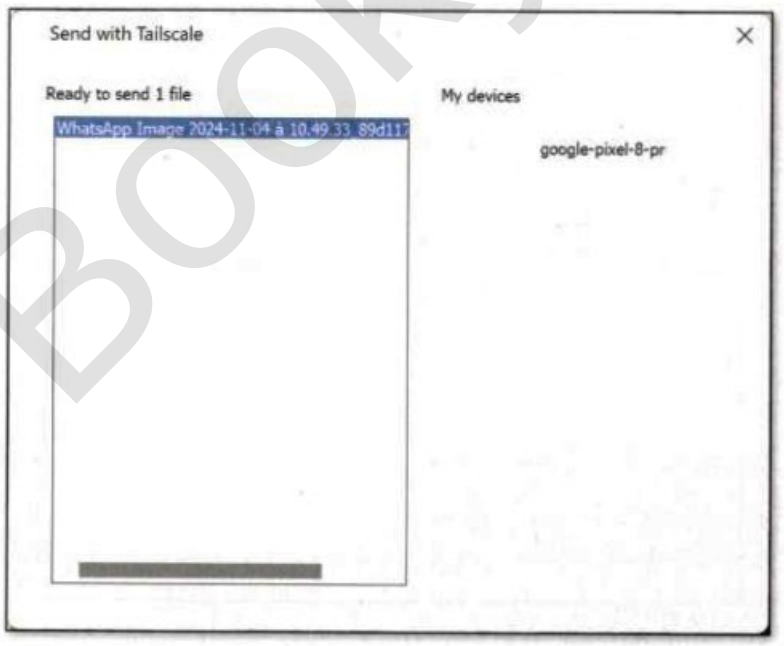
01› ACTIVER TAILDROP

Assurez-vous d'utiliser une version récente de Tailscale (≥ 1.20) et que Taildrop est activé dans les paramètres de votre compte (**Settings > Tailnet Settings > General > Send Files**). En principe, c'est le cas par

défaut. À exception des accès à un NAS, le partage entre appareils ne nécessite pas d'autres configurations.

02› TRANSFÉRER UN FICHIER DEPUIS UN PC

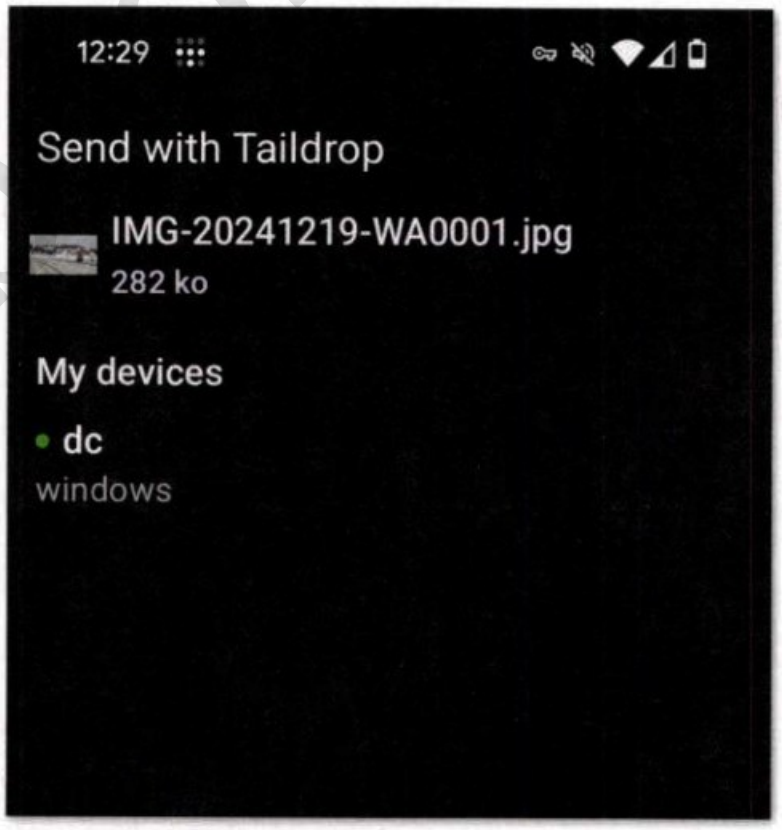
Envoyez un fichier à d'autres appareils de votre compte en cliquant avec le bouton droit de la souris



sur le fichier cible et en choisissant l'option **Send with Tailscale** dans le menu déroulant. Dans la nouvelle fenêtre, sélectionnez le fichier puis l'appareil connecté sur lequel envoyer le fichier. C'est parti !

03› TRANSFÉRER UN FICHIER DEPUIS UN MOBILE

Ouvrez votre fichier puis utilisez l'icône Partager. Sélectionnez dans la liste l'application Tailscale. Les autres appareils connectés à votre mesh apparaissent. Sélectionnez celui de votre choix, c'est parti !



OÙ TROUVER LES FICHIERS REÇUS ?

Selon votre appareil et votre OS, les chemins sont différents. Sur PC, ce sera dans votre dossier **Téléchargements**. Sur Android par exemple, vous recevrez une notification et le fichier sera placé dans votre dossier **Files** (si pas de surcouche logicielle). Pour vérifier les chemins d'accès, visitez sur **Docs > How-to Guides** sur votre plateforme Tailscales et sélectionnez **Access & Share Services > Use Taildrop**.

LES AUTRES SOLUTIONS DE PARTAGE

Avec Tailscale, tous vos appareils se trouvent sur un réseau privé virtuel sécurisé et peuvent communiquer directement. Que vous souhaitiez simplement échanger un fichier avec Taildrop ou monter un partage SMB/NFS complet, les possibilités sont multiples :

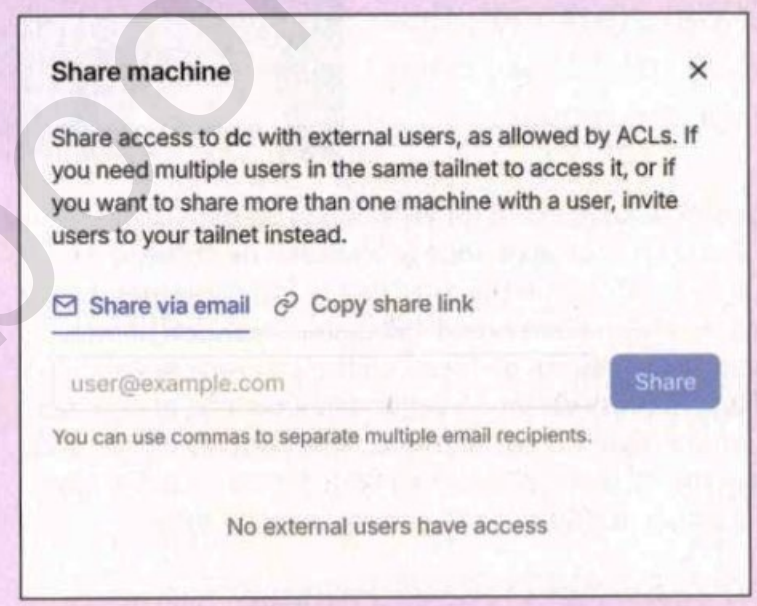
1) Taildrop : pour les transferts rapides de fichiers (lire ci-contre).

2) Protocole réseau standard (SMB, NFS, SFTP...) : pour créer des partages permanents.

3) Serveur multimédia : Utilisez par exemple Plex, Jellyfin ou Emby sur l'une des machines connectées à Tailscale. Depuis un autre appareil Tailscale, entrez l'adresse Tailscale du serveur (par exemple 100.x.x.x:32400 pour Plex). Vous pouvez alors streamer vidéo/musique comme si vous étiez sur le même LAN.

4) Accès distant (RDP, VNC, SSH) : avec Tailscale, vous pouvez utiliser le remote desktop (RDP) ou VNC sur une machine distante via son IP Tailscale, sans exposer de port sur Internet.
Exemple RDP Windows : mstsc /v:100.x.x.x (ou l'adresse MagicDNS si activée).
Exemple VNC : connectez-vous à 100.x.x.x:5900 (le port VNC).

5) Device Sharing : vous permet de partager temporairement ou durablement l'accès à l'un de vos appareils Tailscale à quelqu'un d'autre (un collaborateur, un ami, un client), même si cette personne fait partie d'un autre compte Tailscale. À partir de votre tableau de bord Tailscale, sélectionnez l'appareil à partager. Cliquez sur **Share this device** et renseignez l'adresse mail de la personne avec qui vous souhaitez partager. Cette personne recevra une invitation par e-mail pour accepter l'accès à votre appareil. Votre ami ou collègue voit votre appareil dans son interface Tailscale comme s'il en faisait partie. Il peut ainsi s'y connecter selon les ACL que vous aurez définies (ou en mode par défaut, s'il n'y a pas de restrictions particulières).



tailscale

À SAVOIR

Par défaut, chaque appareil de votre réseau Tailscale peut communiquer avec tous les autres. Vous pouvez définir des règles pour limiter la façon dont les appareils peuvent communiquer entre eux. Dans le tableau de bord Tailscale, ouvrez la section **Access Controls**. Modifiez ou créez des règles pour autoriser/limiter l'accès à certains ports ou protocoles.

TRANSFORMEZ TAILSCALE EN VPN GRATUIT

Avec la fonctionnalité Exit node, vous pouvez accéder au Web en utilisant un appareil distant connecté au votre via un tunnel chiffré. Mais Tailscale ne propose pas de liste de nœuds accessibles à travers le monde. Ce sera à vous de les créer ou de les trouver.

Pourquoi souscrire à un VPN quand on peut utiliser Tailscale !? Un exit node (ou « nœud de sortie ») vous permet de faire transiter tout le trafic Internet d'un appareil via un autre nœud Tailscale. Cela vous permet d'accéder à Internet de façon chiffrée comme si vos échanges provenaient de cet appareil distant, et non pas de votre propre PC par exemple. Utile pour conserver son anonymat et aussi accéder au Web depuis un autre pays en changeant d'adresse IP, comme avec un VPN.

EXIT NODE AVEC SES APPAREILS

Sur la machine que vous souhaitez transformer en exit node (par exemple votre PC à la maison), exécutez la commande **tailscale up --advertise-exit-node** ou passez par l'icône Tailscale dans votre barre des tâches.

Rendez-vous sur le tableau de bord Tailscale pour autoriser l'exit node. Sur l'autre machine (par exemple, votre smartphone Android), activez l'exit node en cochant la case correspondante dans l'application Tailscale (rubrique **Settings > Exit Node**). Résultat : tout le trafic Internet du smartphone sera chiffré et redirigé vers la connexion Internet de votre PC, où qu'il se trouve.

ET COMMENT TROUVER UN EXIT NODE EXTÉRIEUR ?

Pour l'instant, Tailscale ne propose pas de liste publique de « nœuds ouverts » auxquels chacun pourrait se connecter. Le fonctionnement de Tailscale repose généralement sur votre propre réseau (votre organisation, votre groupe de travail, vos amis) ou sur des nœuds qui vous appartiennent (comme un VPS, un Raspberry Pi, etc.). Si vous cherchez un « nœud extérieur » pour faire transiter votre trafic ou tester des connexions, il existe plusieurs options :

1) Créer votre propre nœud sur le Cloud
Vous pouvez choisir un fournisseur de Cloud (AWS, etc.) et localiser le serveur dans le pays de votre choix. Vous pourrez alors configurer ce serveur distant comme votre Exit node et profitez de sa géolocalisation ainsi que de ces fonctions avancées d'obfuscations si vous y souscrivez. Inconvénient : vous avez les frais d'hébergement et la maintenance de cette instance.

2) Rejoindre un autre réseau Tailscale
Si un collègue ou un ami possède déjà son propre réseau Tailscale avec d'autres nœuds (par exemple des serveurs distants, des PC de test, etc.), il peut vous inviter en tant qu'utilisateur sur ce réseau. Une fois que vous aurez accepté cette invitation, tous les nœuds (ou seulement ceux autorisés par les ACL) vous seront accessibles.

WHATSAPP : EMPÊCHEZ LE TÉLÉCHARGEMENT AUTOMATIQUE DES PHOTOS

PRATIQUE

Protégez la confidentialité de votre galerie photos en désactivant le téléchargement automatique des images (et autres médias) sur WhatsApp.

INFOS [Whatsapp]
Où le trouver ? [Whatsapp.com]
Difficulté : ☠☠☠

01› RÉGLAGES

Accédez aux **Paramètres** de WhatsApp puis allez sur **Stockage et données**. Sous **Téléch. Auto. des médias**, vous accédez aux réglages pour le téléchargement en données mobiles ou en Wi-Fi.

02› DÉSACTIVER

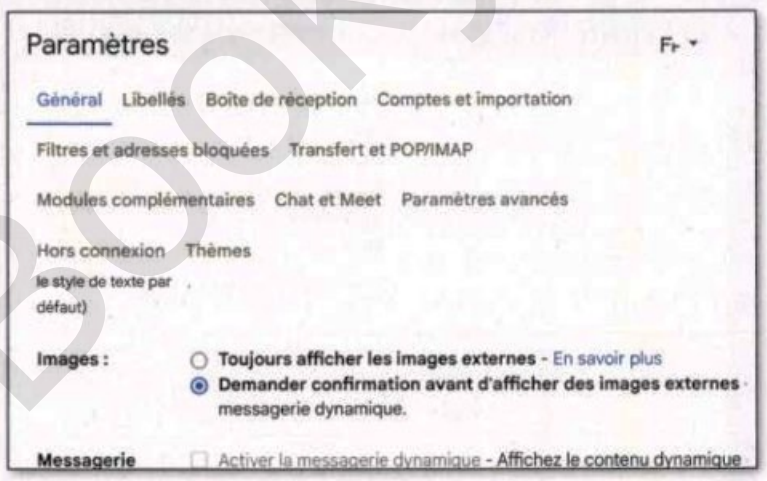
En données mobiles et en Wi-Fi, décochez la case **Photos** (et éventuellement **Vidéos, Audio, Documents**). En itinérance : en général, il est recommandé de tout décocher pour éviter des frais supplémentaires.

GMAIL : DÉSACTIVEZ LES IMAGES POUR ÉVITER LE PISTAGE

PRATIQUE

De nombreux outils marketing insèrent un « pixel de suivi » dans les images des emails. Lorsqu'un destinataire ouvre l'email, ce petit fichier envoie des informations comme votre adresse IP, l'heure d'ouverture ou votre type de navigateur.

Gmail
Où le trouver ? [mail.google.com]
Difficulté : ☠☠☠



01› MASQUER PAR DÉFAUT

Accédez à vos **Paramètres** Gmail (Web) puis sur **Voir tous les paramètres.** Dans l'onglet **Général**, faites défiler jusqu'à la section **Images**. Sélectionnez **Demander confirmation avant d'afficher les images externes** puis sur **Enregistrez les modifications.**

02› AFFICHER QUAND MÊME

Ainsi, vous aurez un aperçu du mail sans charger automatiquement les images. Si vous faites confiance à l'expéditeur, vous pourrez cliquer pour afficher les images de manière ponctuelle (**Afficher les images ci-dessous**) ou permanente (**Toujours afficher les images de...**).

NOUVEAUTÉ TOR

TESTEZ LES ONIONS ÉPHÉMÈRES

Comment fonctionnent les adresses .onions éphémères sur Tor ? Et comment en créer une pour l'un de vos « hidden services » sur le dark web ?

Les services .onion classiques (aussi appelés "Hidden Services") sont habituellement configurés de manière permanente. Plus que de simples sites Web, ces services .onions sont de véritables applications en ligne, développées dans une version 100% Tor (comme ProtonMail, SecureDrop, Riseup, Ahmia ou certaines marketplaces). Ce sont des endroits stratégiques qui interagissent avec leurs visiteurs. Les serveurs conservent leurs clés et leur configuration, rendant le service accessible sur la durée. Or, pour un usage ponctuel ou sensible (partage temporaire d'un fichier, test rapide d'une appli), on peut souhaiter qu'aucune trace persistante ne demeure.

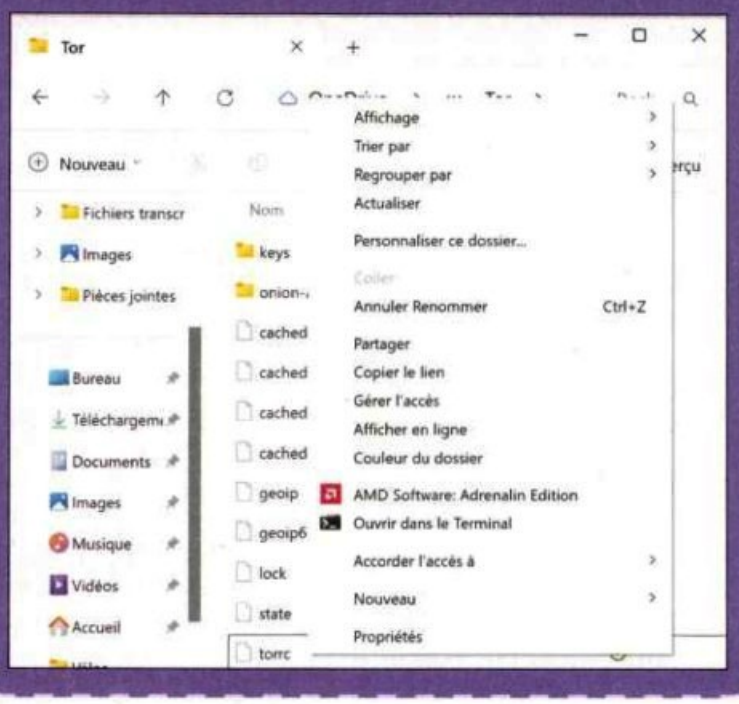
> Des applications qui disparaissent une fois leur mission achevée.

DESTRUCTION APRÈS USAGE

Les "services onion éphémères", présentés récemment par Tor Project, utilisent la même infrastructure cryptographique que les services .onion standards (cryptographie en oignon, répertoires de service, etc.). Mais la différence est qu'ils ne stockent pas durablement les clés de chiffrement et la configuration. Ces clés sont générées en mémoire et détruites à la fermeture de la session ou après un délai donné. Une nouvelle fonction encore en expérimentation, mais que vous pouvez tester avec l'astuce ci-dessous !
Cela peut vous permettre de créer un point d'accès confidentiel pour du support technique, sans laisser d'empreinte à long terme ou d'héberger brièvement un outil de collaboration (chat, wiki) sans devoir sécuriser un serveur web permanent. Bien sûr, cela sera aussi très apprécié par tous ceux qui veulent partager des fichiers ou des informations hypersensibles, tout en s'assurant de réduire les possibilités de réexposition ultérieure.

COMMENT LES UTILISER ?

Dans le répertoire de Tor Browser sur votre PC, trouvez **torrc** en passant par **Browser > TorBrowser > Data > Tor**. Faites une copie de Torrc puis passez en mode édition. Vous activerez la nouvelle fonctionnalité en ajoutant la ligne suivante : **HiddenServiceEnableEphemeral 1**. Enregistrez et replacez ce fichier à sa racine.
Redémarrez ensuite le daemon Tor pour générer un nouveau service onion temporaire. Gardez précieusement l'adresse .onion communiquée dans les logs, car elle disparaîtra ensuite.



TOP 3 OUTILS POUR SUPPRIMER LES TRACES DE VOS FICHIERS MULTIMÉDIA

SÉLECTION

Dans cet article, nous vous présentons trois outils – tous gratuits – pour limiter ou effacer les traces contenues dans vos photos et vos vidéos.

MAT2 (METADATA ANONYMISATION TOOLKIT) : L'ANONYMISEUR « TOUT EN UN »

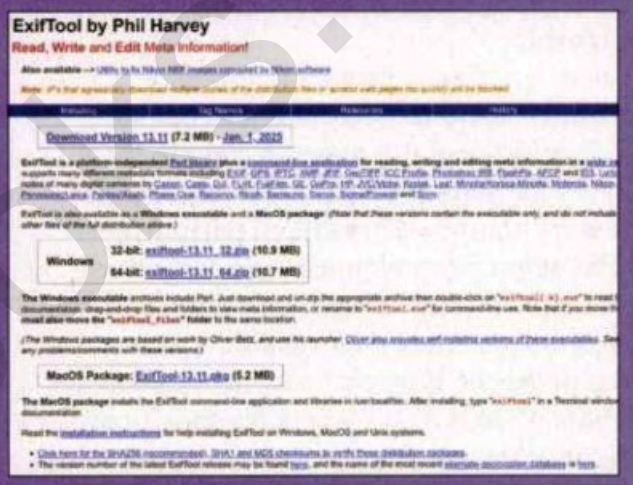
MAT2 est une boîte à outils libre spécialement conçue pour anonymiser divers formats (images, PDF, audio, vidéo...). Très simple d'utilisation sur

Linux (une interface graphique est disponible) et fonctionnel aussi sur d'autres systèmes via des conteneurs ou émulation. Installez MAT2 (directement depuis les dépôts officiels de plusieurs distributions Linux ou via Flatpak). Glissez-déposez vos fichiers dans l'interface pour lancer l'anonymisation. MAT2 crée des copies nettoyées, en supprimant les informations sensibles (balises EXIF, métadonnées PDF, etc.).

Lien : https://0xacab.org/jvoisin/mat2

EXIFTOOL : NETTOYER LES MÉTADONNÉES DE VOS PHOTOS

Cet utilitaire en ligne de commande permet de lire, d'éditer et de supprimer les métadonnées (EXIF) contenues dans les images (format JPEG, PNG...), mais aussi dans d'autres types de fichiers. Gère un grand nombre de formats et offre des commandes très précises, idéales pour automatiser le nettoyage de gros volumes de photos. Sous Windows, après avoir



télécharger l'utilitaire, il faudra passer par l'invite de commandes et exécuter : **exiftool -all= Chemin/vers/fichier.jpg**

Cette commande efface toutes les métadonnées EXIF.

Lien : exiftool.org

SHUTTER ENCODER : RÉENCODER ET PURGER LES MÉTADONNÉES DE VOS VIDÉOS

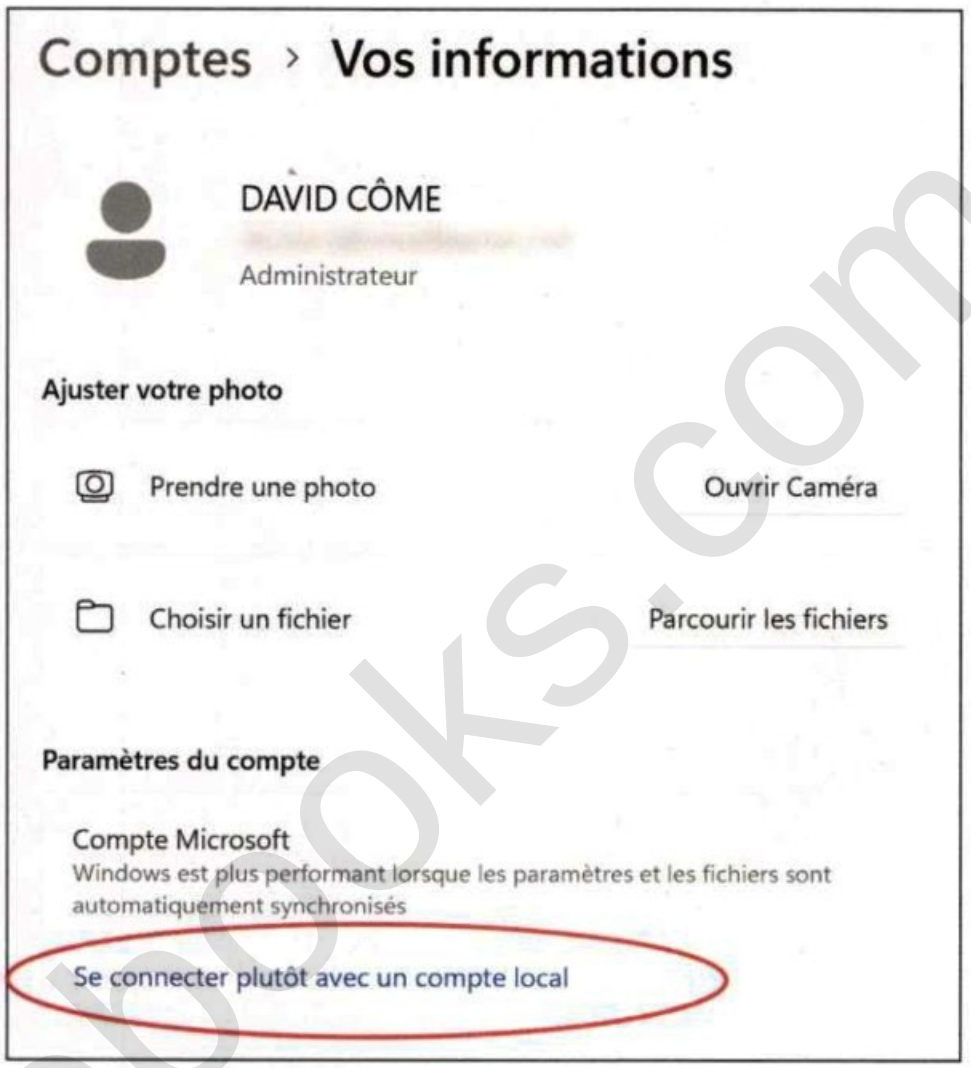
Ce logiciel gratuit et en français permet de convertir de nombreux formats vidéo et audio. Durant la conversion, Shutter Encoder supprime la plupart des métadonnées, réduisant ainsi votre empreinte numérique tout en optimisant la taille du fichier. Dans les options avancées du logiciel, activez l'option pour effacer ou limiter les métadonnées et lancez l'encodage.

Lien : www.shutterencoder.com/fr/

Passer à un compte local

> Avec Windows

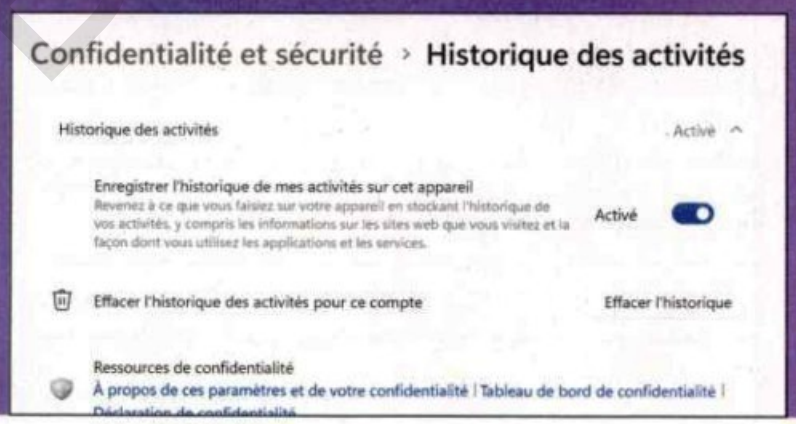
Lors de l'installation de Windows 10 ou 11, Microsoft propose (voire impose) de se connecter avec un compte en ligne. Cela synchronise vos paramètres, votre historique de navigation ou encore vos fichiers sur OneDrive. Si vous préférez conserver davantage de contrôle sur vos données, l'utilisation d'un compte local limite la dépendance à l'écosystème Microsoft.
Passez par **Paramètres > Comptes > Vos informations**. Sélectionnez l'option **Se connecter plutôt avec un compte local**. Suivez l'assistant et entrez le mot de passe de votre compte Microsoft (si déjà connecté). Définissez un nom d'utilisateur local et, si vous le souhaitez, un mot de passe local. Déconnectez-vous pour appliquer les changements. Une fois reconnecté, vous ne dépendez plus d'un compte Microsoft pour ouvrir votre session.



Désactiver l'Historique d'activité

> Avec Windows 11

Windows 10 introduisait la fonction "Timeline" qui enregistrait vos activités (documents ouverts, sites visités, etc.) pour vous permettre de revenir en arrière dans le temps. Sur Windows 11, cet historique existe toujours, sous d'autres formes (Activités récentes). Si vous ne souhaitez pas partager en ligne ces informations, désactivez-le. Dans **Paramètres > Confidentialité et sécurité > Historique d'activité**, décochez **Enregistrer l'historique de mes activités sur cet appareil**. Cela empêche Windows de conserver en local l'historique de vos activités. Pour effacer l'historique existant, cliquez sur **Effacer l'historique** en dessous.



Stripping des paramètres de suivi dans les URL

> Avec Firefox

Introduite courant 2023, cette fonction supprime automatiquement les paramètres de tracking dans les URL (comme utm_source, utm_campaign, etc.), empêchant ainsi les sites et annonceurs de collecter des informations liées à votre navigation. Pour vérifier (ou activer) cette fonctionnalité, ouvrez un nouvel onglet et tapez **about:config**, puis validez l'avertissement. Dans la barre de recherche, saisissez **Privacy.query_stripping.enabled** (ou similaire, selon la version). Assurez-vous que la valeur est sur **true**. Fermez l'onglet et testez en cliquant sur des liens issus de newsletters ou de réseaux sociaux : l'URL devrait être nettoyée de ses paramètres de suivi.

PIRATE INFORMATIQUE

JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON MARCHAND DE JOURNAUX

Direct éditeurs

DÉCRYPTAGE

EMPREINTE DIGITALE : VENDRE SON ÂME À GOOGLE ?

Comment fonctionne le déverrouillage par empreinte digitale sur nos appareils Android ? Est-ce une solution sécurisée ? Qui peut y avoir accès ou la récupérer à notre insu ?

Si votre téléphone est équipé d'un lecteur d'empreinte digitale, sur l'écran ou à l'arrière de votre smartphone, vous pouvez l'utiliser pour déverrouiller votre appareil, certaines applications ou autoriser des paiements en ligne. Ce système de déverrouillage est plus rapide et pratique que le renseignement d'un code. Attention cependant, contrairement à l'intuition, la protection par empreinte digitale est considérée, à raison, comme moins sécurisée que le verrouillage par code. Des techniques simples existent pour copier votre empreinte digitale ! Comme dans un mauvais film, il suffit de vous tendre un verre et de le récupérer pour avoir une chance de la reproduire.

Sur Android, la protection de nos empreintes est gérée par Google. Bonne nouvelle ?

PRATIQUE ET INTÉGRÉ

Tous les smartphones Android disposant de cette fonction s'appuient sur des matériels et capteurs différents, choisis par chaque fabricant. Mais la plupart utilisent ensuite le système logiciel intégré par Android (et donc par Google) pour gérer la reconnaissance et les autorisations. Sur Android 15, vous pouvez ajouter jusqu'à cinq empreintes par appareil, utile pour enregistrer plusieurs doigts, mais aussi pour autoriser l'accès à plusieurs personnes d'une même famille par exemple.

ENVOYÉE À GOOGLE ?

Google affirme que les données liées à nos empreintes digitales sont stockées de façon sécurisée sur notre appareil et jamais partagées avec Google. Ni même avec le fabricant de notre smartphone ou avec d'autres applis installées sur notre téléphone. Lorsque Google ou un autre service veut vérifier la validité d'une empreinte, ces derniers reçoivent simplement une notification de votre appareil indiquant si l'empreinte digitale est validée ou non. Il n'y a pas d'envoi et de vérification des données biométriques dans le cloud, tout reste dans le téléphone sauf le message « Valide / Non valide ».

Mais si un fabricant de smartphones utilisant la technologie Google enfreignait ces règles de base et parvenait à enregistrer vos empreintes

COMMENT FONT LES PIRATES POUR REPRODUIRE UNE EMPREINTE DIGITALE ?

Comme vous l'avez deviné, le plus simple est de récupérer un objet sur lequel vous avez apposé vos doigts. Ou de prendre une photo haute définition de votre main, cela peut suffire. Un logiciel de retouche photo est nécessaire pour nettoyer l'image et optimiser les détails de la zone ciblée. Il faut ensuite imprimer l'empreinte, le plus courant étant de le faire sur une feuille d'acétate (quelques dizaines de centimes). Le pirate déposera enfin un peu de colle à bois sur l'impression, puis retirera cette pellicule de colle une fois séchée. On se retrouve alors avec une fausse peau, prête à l'emploi, avec les empreintes. Cette technique fonctionne avec les capteurs capacitifs (lire ci-dessous), mais se heurte à la finesse d'analyse des nouveaux capteurs à ultra-sons.

Ces derniers sont beaucoup plus fiables puisque l'empreinte est analysée en 3D. En plus, le système peut être capable de détecter les flux de sang qui circulent au même moment dans les veines. Mais les capteurs bas et moyens de gamme, même à ultra-sons, fonctionnent sur des probabilités « faibles ». Pour faire vite et ne pas frustrer l'utilisateur, les capteurs doivent donner une réponse rapide et dans des conditions variées. Du coup, il validera une empreinte s'il la juge « suffisamment ressemblante pour être, statistiquement, celle de l'utilisateur ». Voilà qui ne nous rassure pas. Des moulages en silicone 3D et même l'usage d'encres conductrices sont déjà sur le marché pour tenter d'abuser de cette faiblesse.

TROIS TYPES DE CAPTEURS

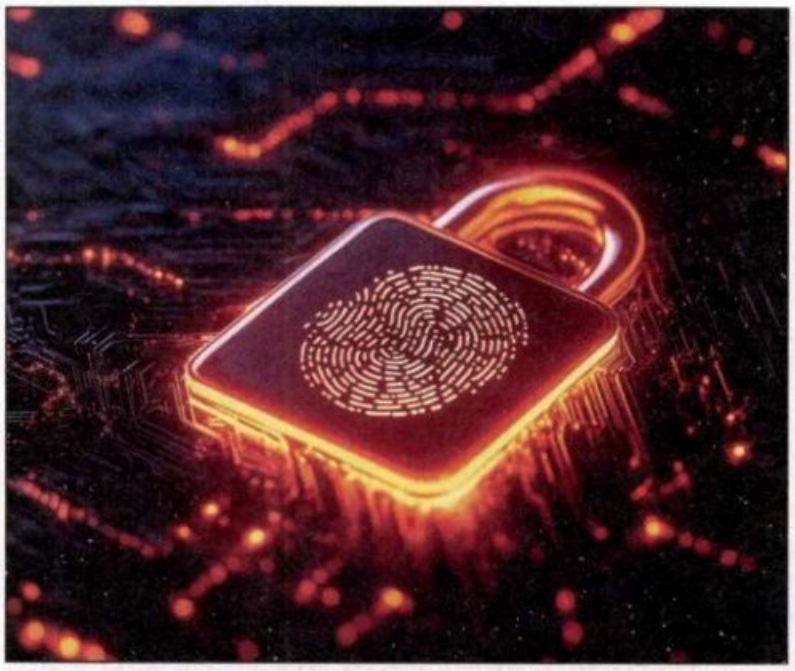
Il existe aujourd'hui trois principaux types de capteurs utilisés sur nos smartphones et tablettes :

- Capteurs optiques : Les capteurs optiques utilisent une lumière pour capturer une image visuelle de l'empreinte digitale. Lorsqu'un doigt est placé sur le capteur, une caméra ou un capteur d'image enregistre l'empreinte en utilisant la réflexion de la lumière. Bien que cette technologie soit éprouvée et couramment utilisée, elle est la plus vulnérable à certaines méthodes de contournement, comme l'utilisation de fausses empreintes.

- Capteurs capacitifs : Les capteurs capacitifs mesurent les différences de capacité électrique causées par les crêtes et les vallées de l'empreinte digitale. En détectant ces variations, ils créent une image détaillée de l'empreinte. Cette méthode offre une précision élevée et est moins susceptible d'être trompée par de fausses empreintes, car elle nécessite un contact avec la peau conductrice (mais certains matériaux posés sur le doigt d'un escroc peuvent le permettre).

- Capteurs ultrasoniques : Les capteurs ultrasoniques émettent des ondes sonores à haute fréquence pour pénétrer la couche externe de la peau et capturer une

image tridimensionnelle de l'empreinte digitale. Cette technologie permet une lecture précise même en présence de contaminants tels que la saleté ou l'huile, et offre une sécurité accrue en raison de la profondeur des informations capturées.



EN RESTANT SUR LE SYSTÈME INTÉGRÉ PAR ANDROID, VOS EMPREINTES RESTENT EN LOCAL, CHIFFRÉES DANS UN ESPACE NON CONNECTÉ DE LA MÉMOIRE DE VOTRE APPAREIL. ELLES SONT CENSÉES Y ÊTRE INACCESSIBLES. MAIS ATTENTIONS AUX APPLICATIONS OU AUX FABRICANTS QUI UTILISENT LEUR PROPRE SYSTÈME DE SAUVEGARDE ET DE VALIDATION.

et à se les envoyer ? Google indique que son service doit être exécuté dans un environnement d'exécution sécurisé appelé « Trusted Exécution Environnement » et que tous les matériels concernés doivent être protégés par une règle SELinux qui rend théoriquement impossible une exfiltration des données.

STOCKÉE EN LOCAL ET CHIFFRÉE

La mémoire de l'appareil où est stocké ce type de données doit être inaccessible à un tiers, à Google comme au fabricant de smartphones. Ces informations sont notamment chiffrées (le système de clés est couplé à votre empreinte) et ne doivent pas pouvoir être extraites, même après le root de l'appareil. Enfin, elles doivent aussi pouvoir être supprimées définitivement à la demande de l'utilisateur, sans possibilité de restauration. Mais attention, si vous passez par d'autres applications vous demandant de faire une capture de vos empreintes, vous devez vous assurer d'utiliser les outils intégrés d'Android et jamais un autre capteur du téléphone (photo, lumière). De la même manière, vérifiez toujours que le fabricant de votre smartphone ou tablette ne passe pas par une solution propriétaire de son cru qui serait beaucoup moins exigeante en termes de sécurité et de protection des données. Car un mot de passe corrompu, cela se change. Une empreinte volée, non, elle restera un sésame vous identifiant toute votre vie.

FORCE BRUTE : UNE MÉTHODE DE PROS

Les chercheurs de Tencent Labs et de l'université de Zhejiang ont révélé une vulnérabilité critique dans l'authentification par empreinte digitale des smartphones Android, nommée "BrutePrint". En résumé, l'idée est de soumettre des centaines voire des milliers d'empreintes au capteur jusqu'à ce que l'une d'entre-elles « matche » avec celle du propriétaire. Si tous les humains possèdent des empreintes digitales uniques, les capteurs, eux, ne fonctionnent que sous forme de probabilités peu strictes. Il suffit de trouver une empreinte qui « ressemble suffisamment » à celle d'un utilisateur pour tromper la machine.

BASES D'EMPREINTES EN LIBRE ACCÈS

Mais, normalement, une attaque en force brute (répéter une tentative d'identification des centaines de fois jusqu'à trouver la bonne) bloque nos appareils. C'est là que BluePrint exploite une faille Android pour contourner cette mesure de sécurité et la neutraliser. Cependant, les pirates ou un service d'enquête doivent avoir le smartphone cible entre leurs mains et un équipement minimal pour lancer cette attaque. Quant aux bases de milliers d'empreintes digitales permettant de tenter ce type piratage, il est facile de les acheter... plus ou moins légalement.

> Un mot de passe volé, cela se change. Une empreinte, elle, vous identifiera toute votre vie.

CRÉER, AJOUTER OU SUPPRIMER DES EMPREINTES

PRATIQUE

Changer de doigts, autoriser une autre personne à accéder à votre appareil ou simplement supprimer les autorisations déjà enregistrées : tout savoir en pratique.

01› DÉVERROUILLAGE

Sur votre smartphone, allez dans **Paramètres > Sécurité et confidentialité > Déverrouillage de l'appareil**. Appuyez ensuite sur **Déverrouillage par empreinte digitale et reconnaissance faciale**. Saisissez le code de déverrouillage de votre téléphone pour accéder à cet espace sécurisé. Allez dans **Déverrouillage par empreinte digitale**.

02› AJOUT OU SUPPRESSION

Dans cet espace, vous accédez aux empreintes éventuellement enregistrées ou vous pouvez en créer une nouvelle en appuyant sur **+ Ajouter une empreinte**. Vous avez la possibilité de créer jusqu'à cinq empreintes différentes, qui seront toutes reconnues par votre appareil. Pour en supprimer une, il vous suffit de sélectionner la corbeille en face de celle que vous ciblez.

03› LECTURE ET ENREGISTREMENT

Avec **Ajouter une empreinte**, le processus d'enregistrement de votre empreinte commence. Vous devrez tapoter plusieurs fois le capteur puis varier les angles d'apposition (droite, gauche) en suivant les demandes de votre smartphone. Une fois ce processus achevé avec succès, votre empreinte est sauvegardée dans la liste des empreintes reconnues.

04› RENOMMER

Vous pouvez renommer chaque empreinte (pratique pour les membres d'une même famille utilisant l'appareil) en appuyant simplement sur le nom par défaut de l'empreinte enregistrée (**Doigt1**, **Doigt2**, ...) puis en modifiant son intitulé. Validez par **OK**.

VOTRE WI-FI EST-IL PIRATÉ ?

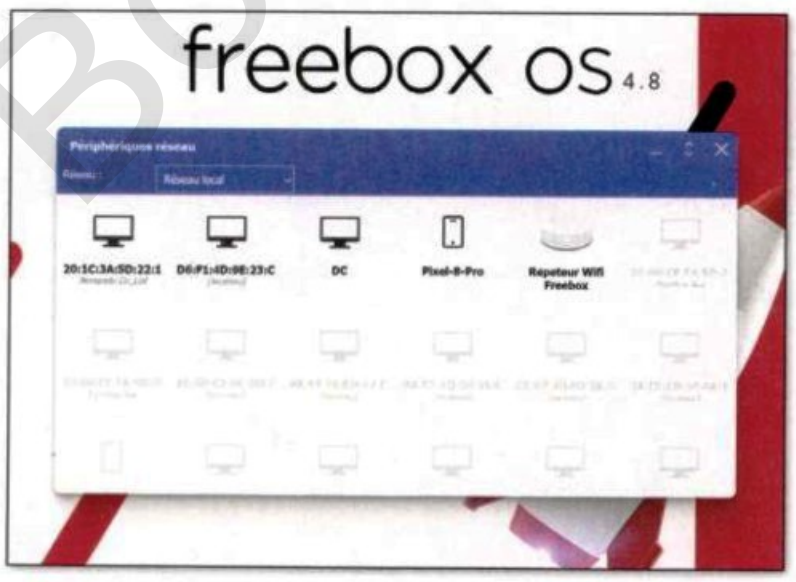
Contrôlez la liste des appareils connectés pour vérifier si un intrus (ordinateur, smartphone ou autre) ne squatterait pas votre bande passante.

01› INTERFACE D'ADMINISTRATION

Accédez à l'interface d'administration du routeur : sur une box internet (Livebox, Freebox, Bbox...), ouvrez votre navigateur et tapez l'adresse de l'interface (par exemple http://192.168.1.1 ou http://192.168.0.1 selon votre fournisseur). Connectez-vous avec vos identifiants (vérifiez l'étiquette collée sous votre box ou consultez le manuel).

02› REPÉREZ

Trouvez la rubrique **Périphériques réseau**, **Appareils connectés**, **Réseau local** ou **LAN**. Le libellé peut varier, mais vous y verrez la liste des équipements actuellement reliés en WiFi et/ou en Ethernet. Chaque appareil apparaît généralement sous forme d'adresse MAC (ex. "00:1A:2B:3C:4D:5E") et parfois avec un nom d'hôte ("PC-de-Jean", "iPhone-de-Marie", etc.).



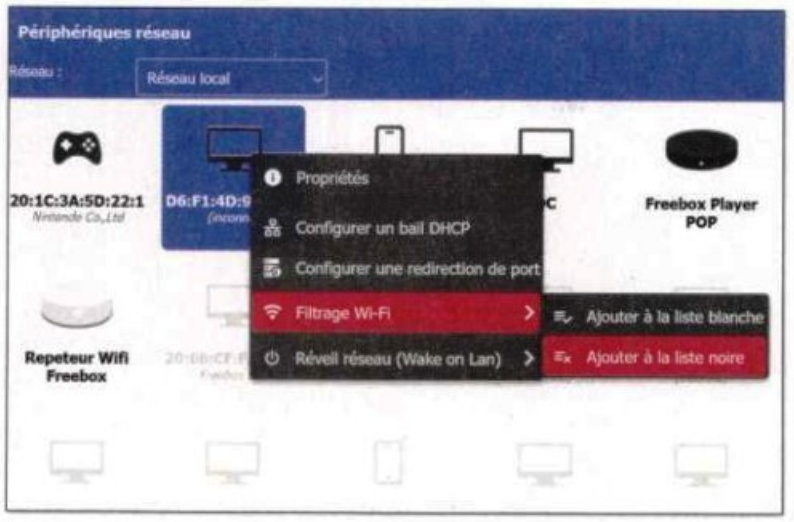
03› AU CAS OÙ

Si vous voyez une adresse MAC ou un nom inconnu, vérifiez d'abord que ce n'est pas un de vos

objets connectés (smart TV, console, ampoule connectée, etc.). En cas de doute, prenez note de l'adresse MAC suspecte.

04› BLOQUEZ ET BLACKLISTEZ

Éventuellement, bloquez l'appareil : la plupart des routeurs/boxs proposent une option "Block / Bloquer" ou "Filter MAC addresses" (filtrage d'adresses MAC). Si vous êtes certain qu'il s'agit d'un intrus, ajoutez son adresse MAC à la liste noire pour l'empêcher de se reconnecter.

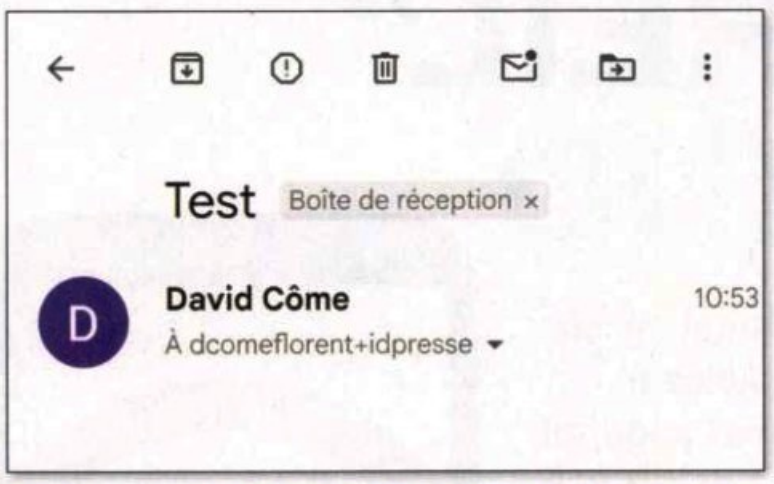


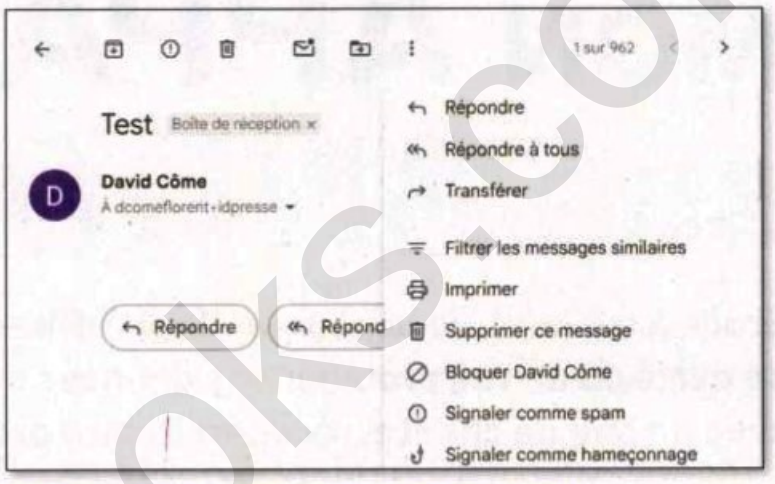
GMAIL : CONNAISSEZ-VOUS CETTE ASTUCE AVEC « + » ?

PRATIQUE

Créez des alias malins sur Gmail avec cette astuce : Gmail ignore tout ce qui suit un signe « + » dans la partie avant le @. Par exemple, les adresses suivantes renvoient toutes au même compte Gmail : monadresse@gmail.com ou monadresse+newsletter@gmail.com.

Gmail
Où le trouver ? **[mail.google.com]**
Difficulté : ☠☠☠





01› CRÉATION D'ALIAS À LA VOLÉE

Lorsque vous vous inscrivez sur un nouveau site, vous pouvez utiliser **monadresse+nomdusite@gmail.com** comme alias. De cette façon, vous pouvez créer autant d'adresses mails personnalisées en fonction des sites où vous vous inscrivez.

02› DÉTECTION DE SPAM

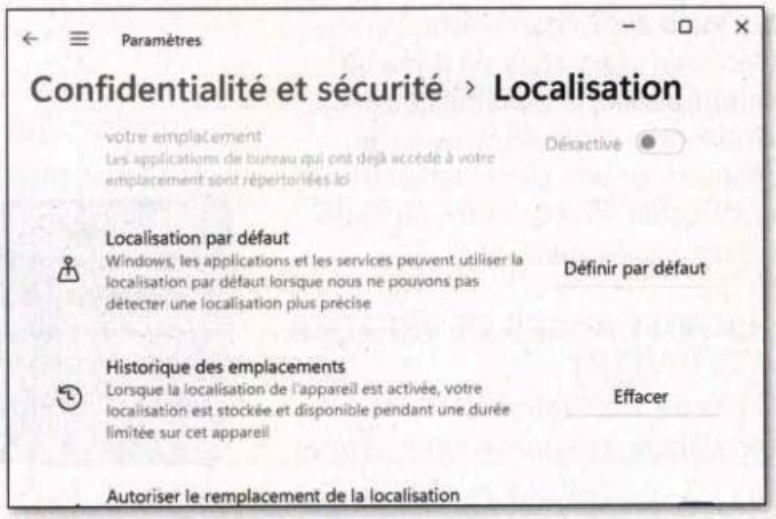
Si vous remarquez que **monadresse+newsletter@gmail.com** reçoit soudainement des mails de spam, vous identifierez tout de suite l'origine (ou la fuite) et pourrez filtrer ou bloquer rapidement les messages.

GÉREZ LA GÉOLOCALISATION SUR WINDOWS

PRATIQUE

Si les services de localisation vous offrent des suggestions de lieu ou de météo plus précises, ils peuvent aussi être utilisés pour suivre vos déplacements.

Windows
Difficulté : ☠☠☠



01› RÉGLAGE

Allez dans les **Paramètres** puis sur **Confidentialité** (ou **Confidentialité et sécurité**) et recherchez l'onglet **Localisation** (ou **Géolocalisation**). Basculez sur **Désactivé** si vous ne voulez pas que Windows détermine votre position.

02› HISTORIQUE

Vous pouvez conserver la géolocalisation activée, mais ne l'autoriser que pour certaines applications (en gérant les autorisations pour chaque appli). Effacez l'historique de localisation plus bas dans la même page en cliquant sur **Effacer** l'historique.

TUTO

ACTIVEZ "LOCALISER MON APPAREIL" SUR ANDROID

Grâce à cet outil, vous pouvez réagir efficacement en cas de perte ou de vol, protéger vos données sensibles et, avec un peu de chance, récupérer votre précieux appareil.

La fonction "Localiser mon appareil" (ou Find My Device, en anglais) est un outil proposé par Google pour localiser, verrouiller ou effacer à distance un smartphone Android perdu ou volé. Si cette fonctionnalité est souvent sous-estimée, elle constitue pourtant l'un des dispositifs de sécurité les plus importants pour protéger vos données personnelles.

RETROUVER SON SMARTPHONE PERDU

Que vous ayez égaré votre téléphone chez vous ou dans un endroit public, la possibilité de le faire sonner à distance ou de le localiser sur une carte est un atout inestimable pour remettre la main dessus rapidement.

LIMITER L'ACCÈS ET EFFACER LE CONTENU

En cas de vol, l'option de verrouillage à distance vous permet d'empêcher l'accès non autorisé à vos informations personnelles (photos, contacts, messages, applications bancaires, etc.). Vous pouvez également définir un message sur l'écran de verrouillage ou un numéro à contacter. Si vous n'avez vraiment plus d'espoir de récupérer votre smartphone, il reste la possibilité de le réinitialiser à distance. Ainsi, vos données confidentielles (comptes, identifiants, fichiers) ne tomberont pas entre de mauvaises mains.

À SAVOIR

"Localiser mon appareil" repose sur la capacité de l'appareil à communiquer sa position aux serveurs Google. Cela nécessite, au minimum, que le téléphone soit allumé et dispose encore d'une connexion Internet (Wi-Fi ou données mobiles). Si vous effectuez une demande de localisation ou d'effacement, ces instructions resteront en "attente" jusqu'à sa prochaine mise sous tension et reconnexion à Internet.

COMMENT ÇA MARCHE ?

"Localiser mon appareil" utilise plusieurs sources pour localiser un téléphone : le GPS avec une précision de quelques mètres (mais consomme de la batterie) ; le Wi-Fi, moins précis que le GPS mais utile dans les environnements urbains denses ; la cellule téléphonique (triangulation du signal), encore moins précise mais opérationnelle même en zone sans Wi-Fi

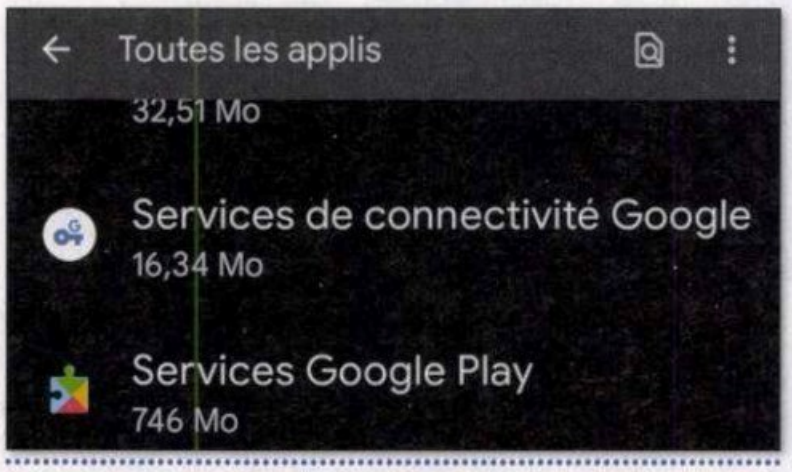
CONFIGUREZ "LOCALISER MON APPAREIL"

PRATIQUE

Le site ou l'application mobile "Localiser mon appareil" se connecte à votre compte Google pour afficher la position en temps réel de votre smartphone. Vous seul avez accès à cette fonctionnalité.

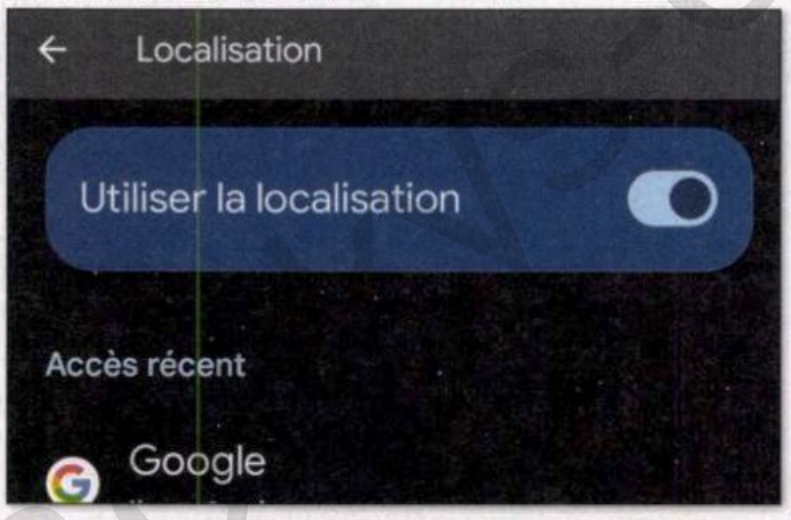
01› VÉRIFIER LA COMPATIBILITÉ

Ouvrez **Paramètres > Applications**. Vérifiez que **Services Google Play** est présent et à jour.



02› ACTIVER LA LOCALISATION ET LE WI-FI

Toujours dans **Paramètres**, recherchez la section **Localisation** et assurez-vous qu'elle est activée. Activez également le Wi-Fi (même si vous n'êtes pas connecté à un réseau), car Android utilise les bornes Wi-Fi environnantes pour trianguler la position.

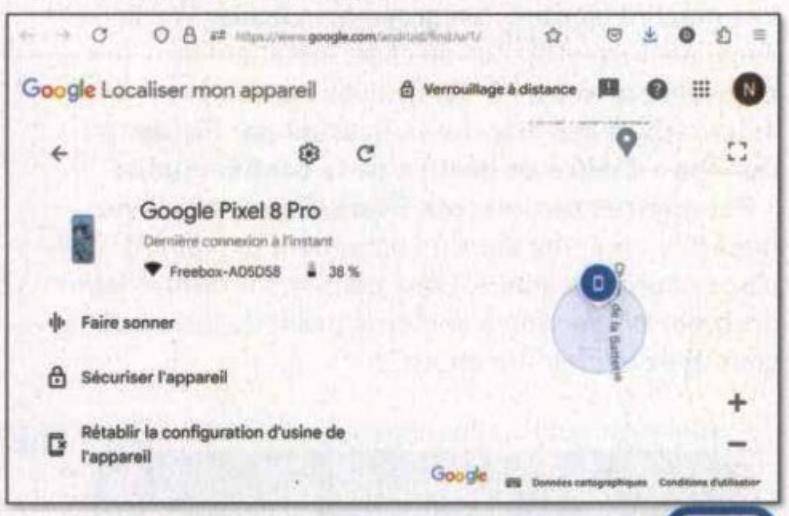


03› ACCÉDER À "LOCALISER MON APPAREIL"

Depuis **Paramètres**, recherchez **Sécurité & confidentialité**. Sélectionnez **Localisateurs d'appareils**. Activez la fonction.

04› TESTER LA CONFIGURATION

Ouvrez un navigateur web sur un autre appareil. Connectez-vous à **google.com/android/find** avec le même compte Google que celui configuré sur votre téléphone. Votre téléphone doit apparaître sur la carte avec un point de localisation plus ou moins précis.



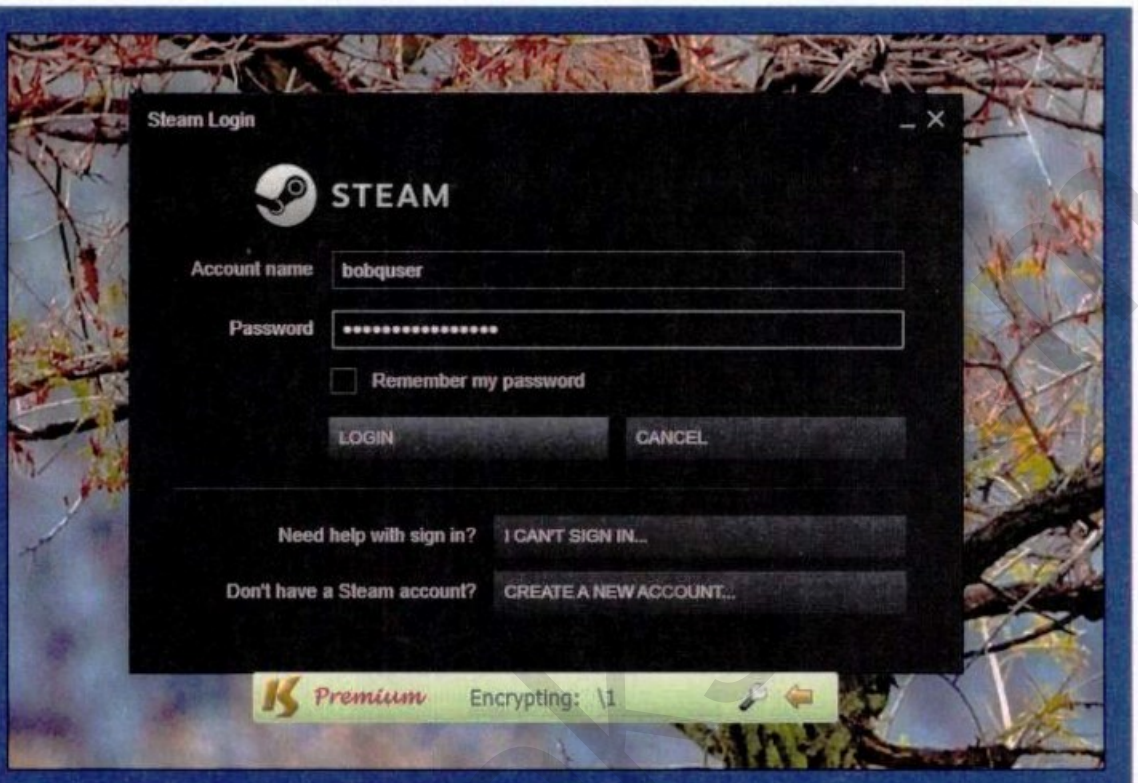
QUELLES ACTIONS POSSIBLE EN CAS DE PERTE ?

Depuis l'interface de Find My Device, cliquez sur l'option **Sécuriser l'appareil** ou **Verrouillage à distance**. Choisissez un mot de passe temporaire ou verrouillez l'écran avec votre code habituel. Vous pouvez aussi afficher un message ou un numéro de contact sur l'écran, invitant la personne qui trouve l'appareil à vous appeler. Vous pouvez enfin cliquer sur **Faire sonner** pour déclencher une sonnerie, même s'il est en mode vibreur ou silencieux.

EFFACER LES DONNÉES

Si le vol est avéré ou si l'appareil est définitivement perdu, sélectionnez **Rétablir la configuration d'usine de l'appareil**. Toutes les données (photos, contacts, applications, etc.) seront supprimées. Attention : Une fois l'effacement effectué, il n'est plus possible de localiser ou de retrouver l'appareil via Find My Device. Cette action est irréversible.

Qui surveille mon clavier ?
> AVEC KEYSCRAMBLER PERSONAL



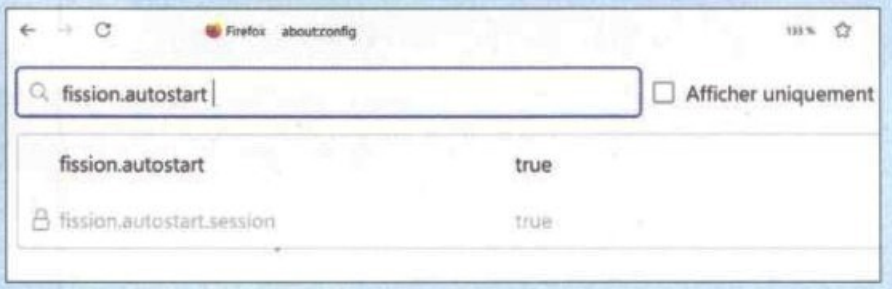
La version gratuite de KeyScrambler chiffre les frappes du clavier en temps réel, empêchant les keyloggers de les intercepter quand vous écrivez via un navigateur Web ou une application en ligne. C'est un outil très efficace pour protéger les données de connexion et autres informations sensibles. Léger et discret, il est peu gourmand en ressources et est compatible avec tous les navigateurs courants.

Lien : www.qfxsoftware.com

Macros malveillantes dans les documents > AVEC OFFICE

Les macros (scripts) intégrées à un fichier Word/Excel peuvent exécuter du code, installant un malware sur votre PC. Désactivez l'exécution automatique des macros en passant par **Fichier > Options > Centre de gestion de la confidentialité > Paramètres des macros (Word/Excel)**. N'activez jamais les macros dans un document provenant d'une source inconnue. Sans oublier d'analyser les documents avec votre antivirus avant de les ouvrir, si vous avez le moindre doute.

Contrer les attaques de type Spectre
> AVEC FIREFOX

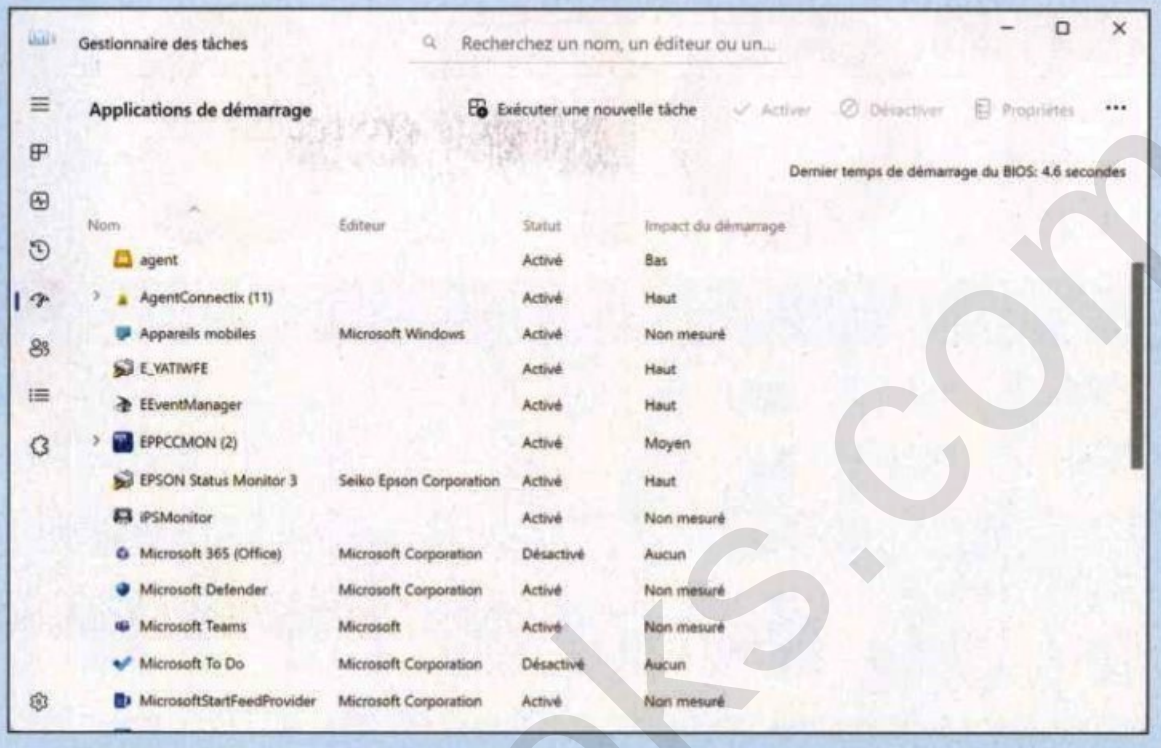


La **Site Isolation** (arrivant progressivement depuis 2023 et jusqu'à cette année) place chaque site Web dans un "processus isolé", réduisant les risques de fuites de données entre onglets, même en cas de failles comme Spectre ou Meltdown.

Vérifiez (ou activez) la disponibilité de cette fonction sur votre navigateur. Tapez **about:config** dans la barre d'adresses. Recherchez **fission.autostart** (le nom du paramètre correspondant à la Site Isolation, aussi appelée "Fission"). Passez la valeur à **true** si elle ne l'est pas déjà. Redémarrez Firefox pour appliquer la modification. Ouvrez plusieurs sites dans différents onglets et vérifiez dans le Gestionnaire de tâches de Firefox (tapez **about:performance**) que chaque domaine utilise un processus distinct.

Désactiver le démarrage automatique des programmes inutiles

> Avec Windows

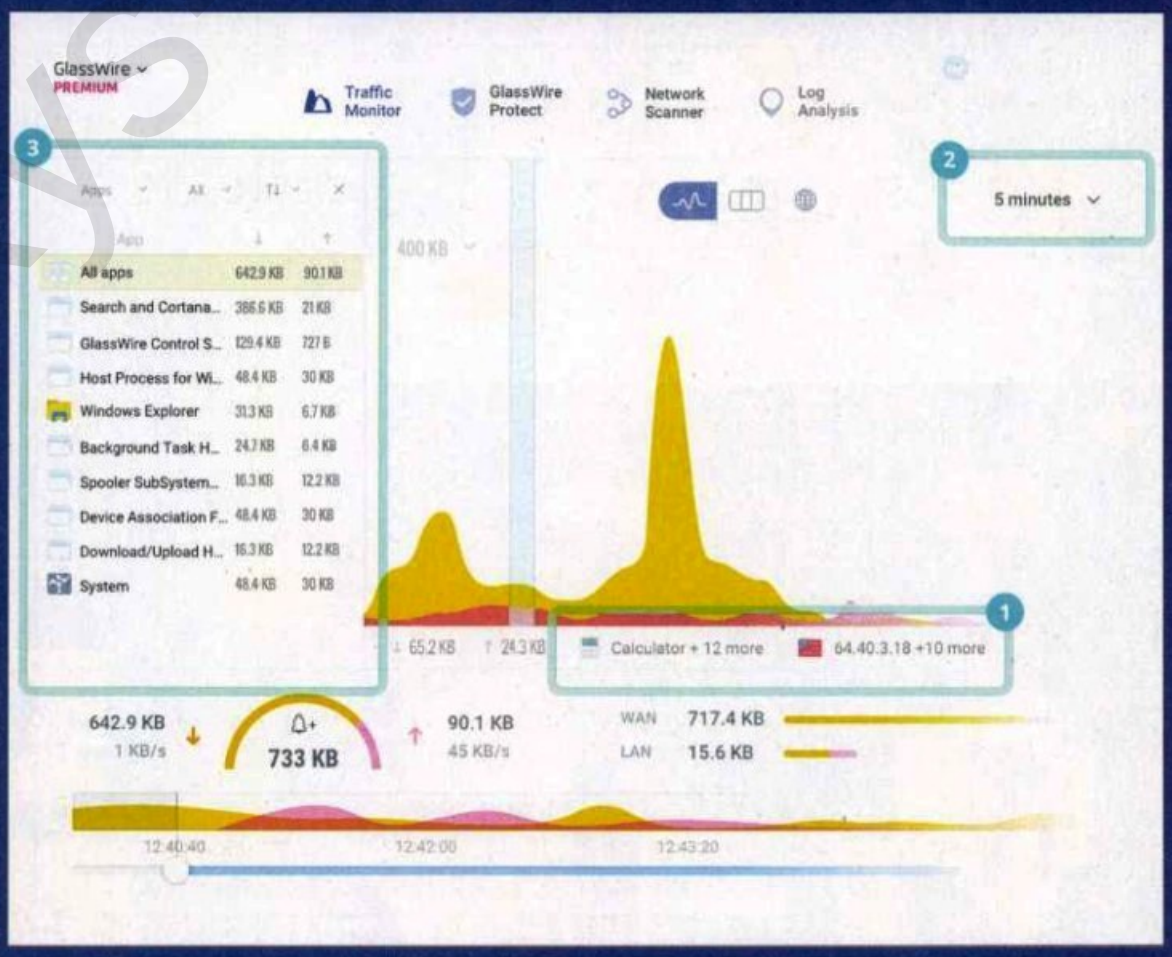


Beaucoup de malwares se lancent au démarrage de Windows. Limiter les programmes au strict nécessaire améliore sécurité et performances. Cliquez droit sur la barre des tâches puis sur **Gestionnaire des tâches**. Dans l'onglet **Démarrage** (icone en forme de compteur de vitesse à gauche), repérez les programmes indiqués comme **Activé**. Sélectionnez ceux que vous ne voulez pas lancer et cliquez sur **Désactiver**. Redémarrez votre PC.

Vérifier les connexions réseau > Avec GlassWire Free

Des programmes malveillants ou des trojans peuvent envoyer des données à l'extérieur de votre appareil sans que vous ne le sacjiez. GlassWire vous permet de visualiser et contrôler le trafic entrant/sortant et de repérer les anomalies. Téléchargez GlassWire Free sur le site officiel puis lancez-le. Surveillez le tableau de bord pour voir quelles applications consomment de la bande passante. Bloquez les connexions suspectes à l'aide du pare-feu intégré. Configurez enfin des alertes pour être prévenu si un nouveau programme se connecte.

Lien :
www.glasswire.com



SÉLECTION

TOP 8

SERVICES DE CLOUD GRATUITS

Retrouvez vos fichiers et documents sur tous vos écrans grâce au stockage en ligne. Solutions de sauvegarde automatique, de partage ou de travail collaboratif : des services de cloud vous proposent gratuitement des offres généreuses, simples d'accès, sécurisées et disposant même pour certains d'outils en ligne pour tout faire sans logiciel. Suivez le guide.

Le stockage dans le cloud est devenu indispensable pour les particuliers et les professionnels, que ce soit pour sauvegarder des fichiers, travailler en ligne et collaborer sur des projets ou synchroniser des fichiers entre différents appareils. Mais tous les services de cloud gratuit ne se valent pas, surtout quand on regarde de près les capacités de stockage, la rapidité de transfert et la sécurité des données. Voici un tour d'horizon des meilleurs services gratuits disponibles, en fonction de leurs forces et faiblesses pour des usages concrets. Certains vous correspondront mieux que d'autres... mais n'oubliez pas que vous pouvez aussi en utiliser plusieurs !

85 GO GRATUITS !

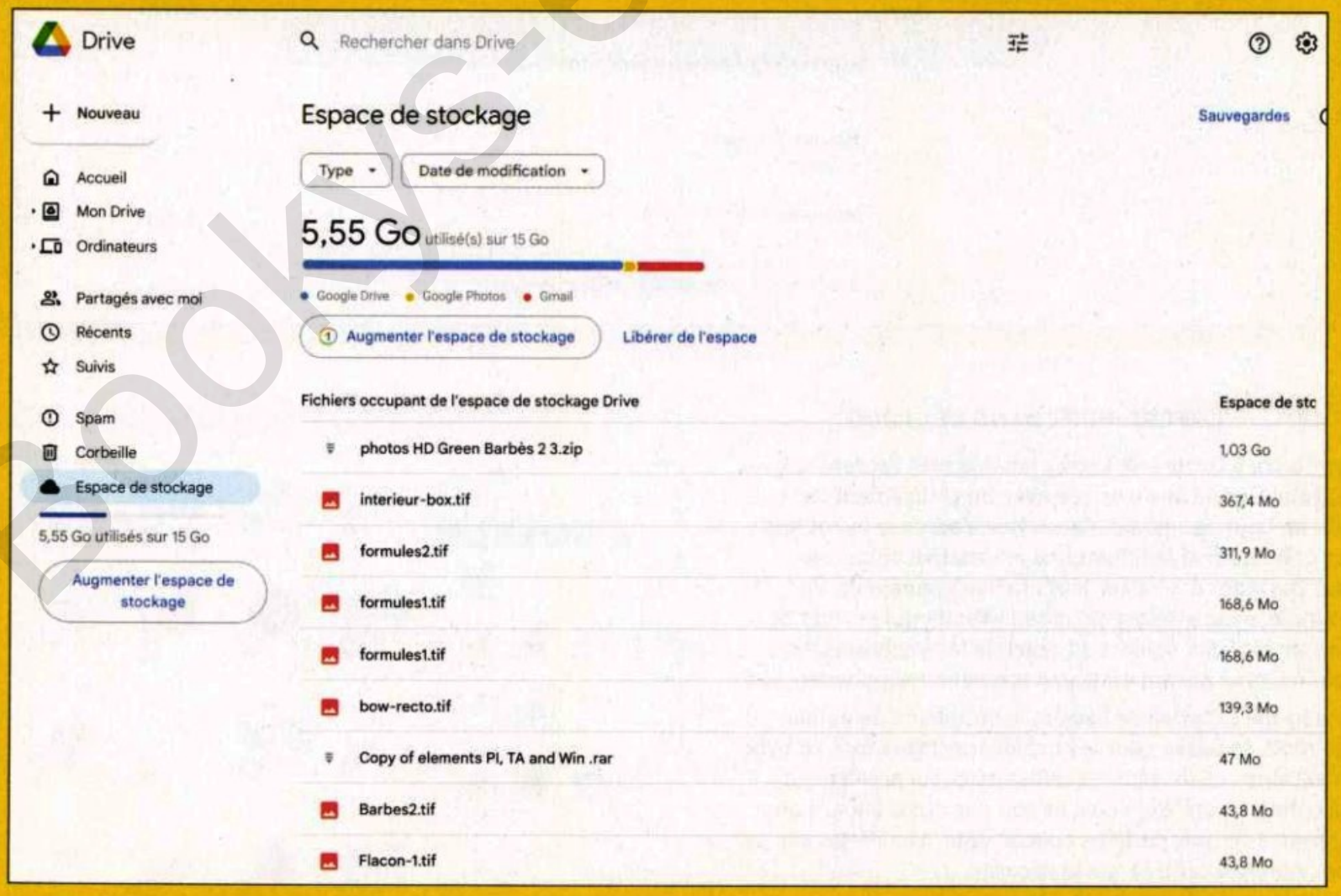
Un pour la sauvegarde de vos docs pros, un autre pour le stockage de vos photos ou musique, un troisième pour accéder à vos films et séries où vous le souhaitez, un dernier pour protéger vos données et documents les plus sensibles ! Au total, si on additionne les huit services que nous vous présentons, cela représente quand même quelques 85 Go gratuits. De quoi satisfaire la plupart de vos besoins.

Google Drive > Complet et intégration des services Google

Avec 15 Go de stockage gratuit, Google Drive reste un incontournable, surtout si vous utilisez déjà des services Google comme Gmail ou Google Photos. En offrant une intégration native avec Google Docs, Sheets et Slides, Google Drive se distingue pour le travail collaboratif. Par exemple, si vous travaillez en équipe sur un document, chaque personne peut apporter ses modifications en temps réel, ce qui en fait un outil idéal pour les étudiants ou les professionnels gérant des projets partagés.

Sur le plan de la compatibilité, Google Drive est disponible sur PC, Mac, Android, et iOS, garantissant un accès fluide entre vos appareils. Le chiffrement des données SSL/TLS assure la sécurité de vos fichiers lors de leur transfert, un atout pour ceux qui stockent des documents sensibles. Cependant, si vos besoins en espace sont élevés, les 15 Go peuvent vite se remplir, notamment si vous synchronisez des photos via Google Photos.

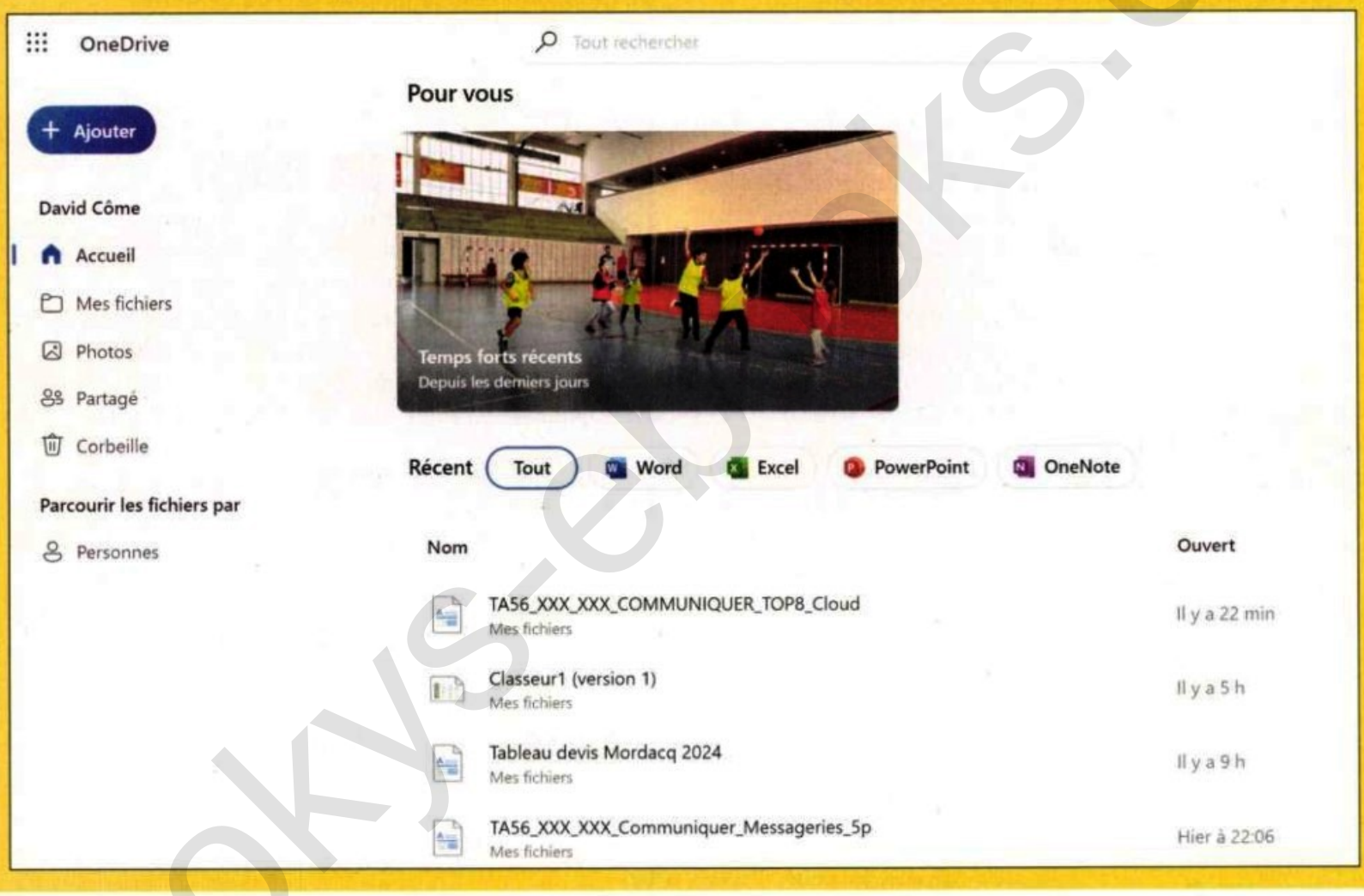
Lien : https://drive.google.com/



Microsoft OneDrive > IDÉAL POUR LES UTILISATEURS WINDOWS

Pour ceux qui utilisent Windows au quotidien, OneDrive offre un stockage gratuit de 5 Go et une intégration étroite avec le système d'exploitation. Vous pouvez sauvegarder automatiquement vos documents et photos dans le cloud, et accéder facilement aux fichiers depuis n'importe quel appareil connecté, qu'il s'agisse d'un PC, d'un smartphone ou d'une tablette. La synchronisation se fait en arrière-plan, et grâce à sa compatibilité avec les applications Microsoft Office, OneDrive facilite le travail collaboratif sur des documents Word, Excel et PowerPoint. Les données sont sécurisées lors du transfert, bien que certaines options de chiffrement avancé ne soient disponibles que pour les utilisateurs payants. Un bon choix pour ceux qui utilisent beaucoup les outils Office et souhaitent une intégration transparente avec leur PC.

Lien : https://onedrive.live.com



Sync > COFFRE-FORT DANS LE CLOUD

Sync offre 5 Go de stockage gratuit et met l'accent sur la protection de la vie privée avec un chiffrement de bout en bout par défaut. Ce service s'adresse avant tout aux utilisateurs cherchant une alternative sécurisée pour partager et stocker leurs fichiers sensibles. Par exemple, Sync propose un mode «Vault» qui permet de stocker certains fichiers à l'écart de la synchronisation automatique, offrant ainsi une protection supplémentaire.

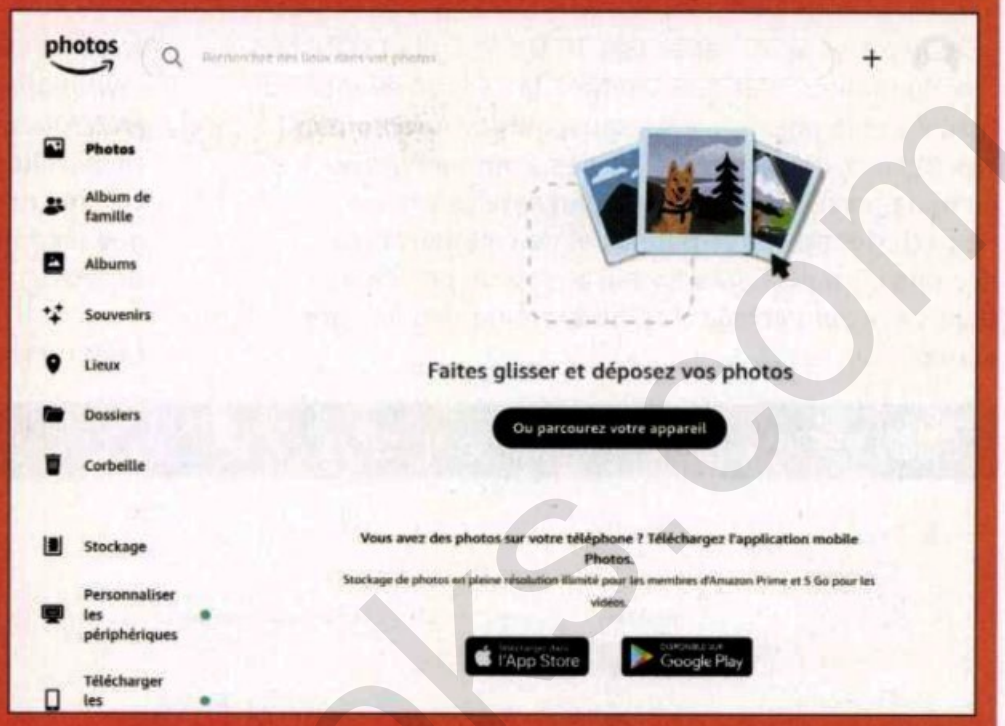
Le partage sécurisé de liens et la possibilité de définir des mots de passe pour les fichiers partagés font de Sync un excellent choix pour les utilisateurs qui privilégient la confidentialité. Bien qu'il ne soit pas aussi intégré aux systèmes comme certains concurrents, il se démarque par son approche centrée sur la sécurité.

Lien : www.sync.com

Amazon Drive > Un cloud intégré pour les clients Amazon

Amazon Drive propose 5 Go de stockage gratuit, particulièrement avantageux pour les abonnés Amazon Prime. Ce service est idéal pour les utilisateurs qui souhaitent principalement sauvegarder des photos, bien que les fichiers soient également pris en charge.
Disponible sur Android, iOS, et via le navigateur pour une synchronisation entre tous les appareils, Amazon Drive est une bonne option pour les amateurs de photographie. Cependant, pour les autres types de fichiers, les 5 Go gratuits peuvent rapidement devenir insuffisants.

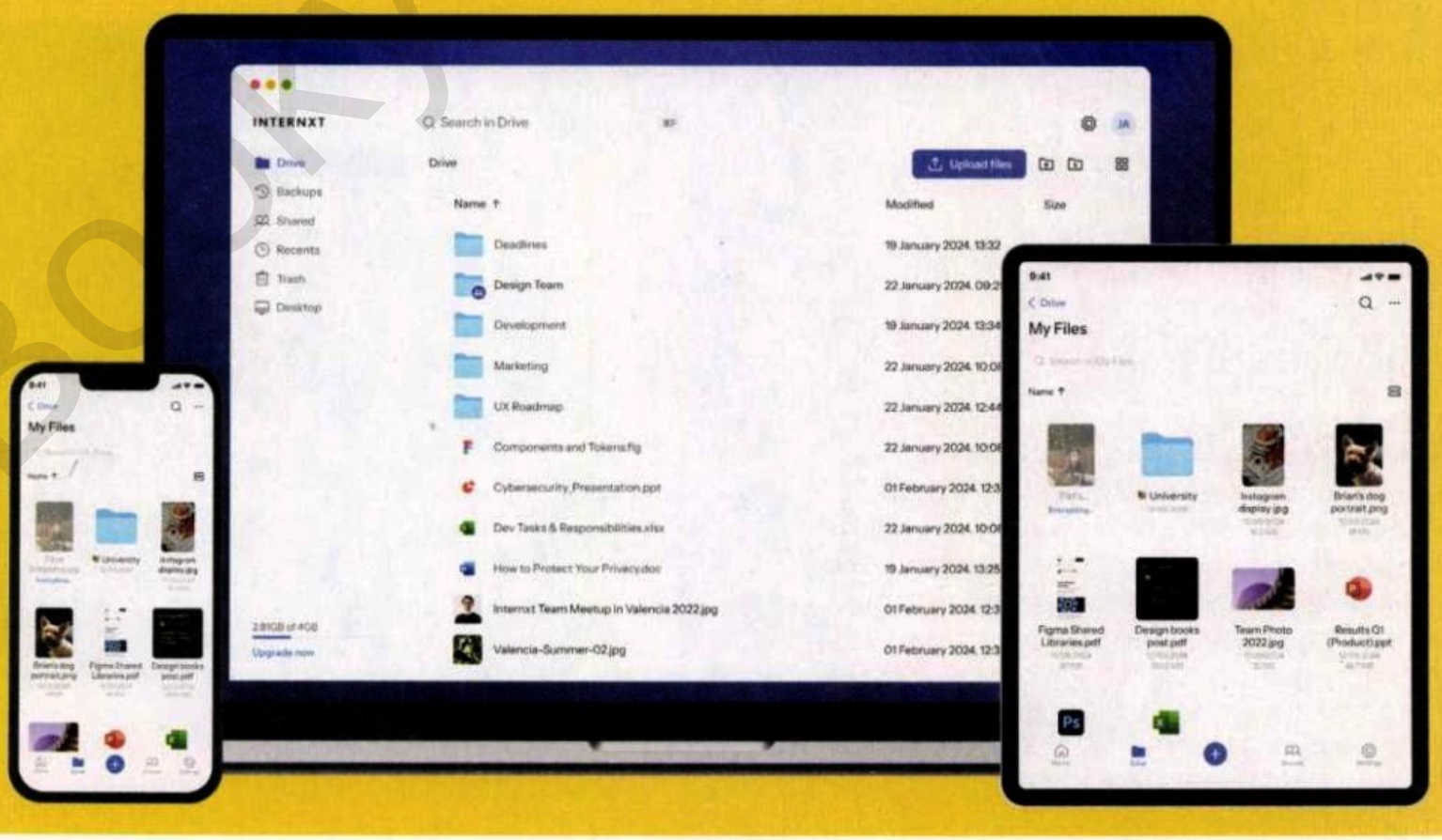
Lien : www.amazon.com/clouddrive



Internxt > Une option éthique et sécurisée

Internxt propose 10 Go de stockage gratuit et se distingue par son engagement en faveur de la confidentialité des utilisateurs et de l'éthique numérique. Ce service utilise un chiffrement de bout en bout et une architecture décentralisée, ce qui signifie que les fichiers sont répartis et stockés sur plusieurs serveurs sécurisés.
Internxt est particulièrement recommandé pour les utilisateurs soucieux de la sécurité et de la confidentialité de leurs données. Bien qu'encore relativement nouveau, il gagne en popularité grâce à sa transparence en matière de protection des données. Les fonctionnalités de base sont accessibles depuis tous les appareils, même si l'interface pourrait être améliorée pour les utilisateurs moins techniques.

Lien : https://internxt.com/

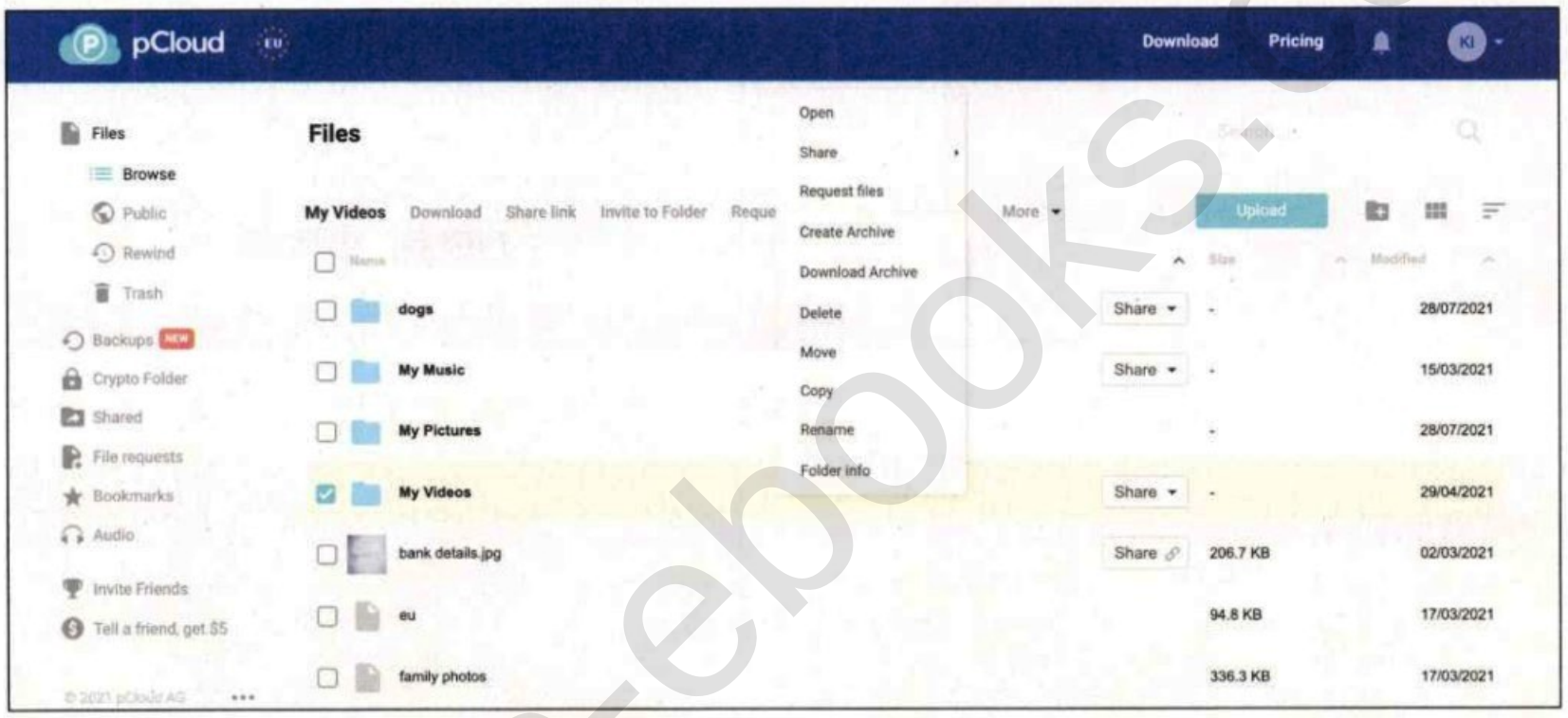


pCloud > Alternative pratique pour les gros fichiers

pCloud propose un espace de 10 Go gratuit et offre des fonctionnalités pratiques comme la gestion avancée de fichiers et la possibilité de sauvegarder directement des fichiers de services externes, comme Facebook ou Instagram. La plateforme permet également de partager des liens publics et de collaborer sur des dossiers partagés, ce qui en fait un bon choix pour ceux qui partagent régulièrement des fichiers volumineux.

Avec un stockage qui peut être étendu via des invitations ou des actions spécifiques, pCloud est idéal pour les indépendants ou les freelances qui recherchent un cloud souple et sans contrainte de volume de fichier pour les sauvegardes. À noter que les fonctionnalités de chiffrement avancé sont proposées sous forme d'option payante.

Lien : www.pcloud.com



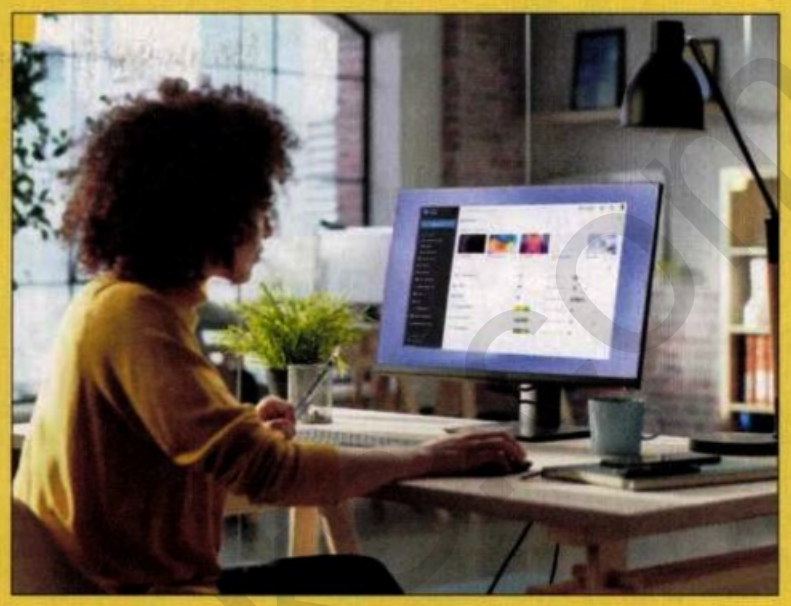
MEGA > Stockage généreux et sécurisé

MEGA propose l'un des plus grands espaces de stockage gratuit du marché avec 20 Go offerts. Ce service néo-zélandais est reconnu pour sa sécurité avancée, avec un chiffrement de bout en bout pour toutes les données. MEGA s'adresse particulièrement aux utilisateurs soucieux de la confidentialité, offrant des fonctionnalités comme le partage de fichiers sécurisé avec des clés de chiffrement.

Bien que MEGA soit accessible depuis n'importe quel appareil via un navigateur, l'expérience est souvent meilleure sur les applications dédiées (disponibles sur Windows, macOS, Android et iOS). Pour les utilisateurs qui manipulent de gros volumes de fichiers ou qui privilégient la sécurité, MEGA est une option solide, bien qu'il puisse être légèrement moins intuitif pour les nouveaux utilisateurs.

Lien : https://mega.nz

kDrive > Concurrent de Google... mais soucieux de votre vie privée



kDrive, développé par l'entreprise suisse Infomaniak, propose un espace de stockage gratuit de 15 Go. Ses centres de données sont situés en Suisse et disposent d'un chiffrement de pointe pour garantir la confidentialité des utilisateurs. Côté fonctionnalités, kDrive inclut une suite bureautique intégrée permettant d'éditer des documents, feuilles de calcul et présentations, offrant une alternative complète aux outils collaboratifs comme Google Workspace ou Microsoft Office. En outre, kDrive se distingue par sa fonctionnalité d'import automatique depuis d'autres services de cloud (comme Google Drive, Dropbox et OneDrive), facilitant la migration des utilisateurs vers leur plateforme.
Avec sa compatibilité multi-plateformes (PC, Mac, iOS, Android) et ses options de partage de fichiers avec contrôle d'accès (mots de passe), kDrive se présente comme une solution puissante, sécurisée et respectueuse de la vie privée.

Lien : www.infomaniak.com

OFFRES DE CLOUD GRATUIT : NOTRE COMPARATIF

Service	Capacité de stockage gratuit	Vitesse de transfert	Compatibilité	Sécurisation des données	Outils de collaboration	Où le trouver ?
Google Drive	**15 Go**	Excellente	PC, Mac, Android, iOS	Chiffrement SSL/TLS	Google Docs, Sheets, Slides	**https://drive.google.com**
OneDrive	**5 Go**	Très bonne (Windows)	PC, Mac, Android, iOS	SSL, chiffrement au repos	Word, Excel, PowerPoint	**https://onedrive.live.com**
MEGA	**20 Go**	Variable	PC, Mac, Android, iOS	Chiffrement bout en bout	Partage sécurisé	**https://mega.nz**
pCloud	**10 Go**	Bonne	PC, Mac, Android, iOS	Chiffrement (payant)	Dossiers partagés	**www.pcloud.com**
Sync	**5 Go**	Bonne	PC, Mac, Android, iOS	Chiffrement bout en bout	Partage sécurisé	**www.sync.com**
Amazon Drive	**5 Go**	Variable	PC, Mac, Android, iOS	SSL	Sauvegarde photos (Prime)	**www.amazon.com/clouddrive**
Internxt	**10 Go**	Variable	PC, Mac, Android, iOS	Chiffrement décentralisé	Partage sécurisé	**https://internxt.com**
kDrive	**15 Go**	Excellente	PC, Mac, Android, iOS	Chiffrement avancé en Suisse	Suite bureautique	**www.infomaniak.com**

PILET

VOTRE MINI-ORDI À CLIPSER

LE PILET SE SITUE SUR UN CRÉNEAU HYBRIDE ENTRE LA CARTE DE DÉVELOPPEMENT « PUR ET DUR » (TYPE ARDUINO) ET LE NANO-ORDINATEUR POLYVALENT (TYPE RASPBERRY PI). CE MINI-ORDINATEUR MODULABLE EST CONÇU POUR FONCTIONNER EN « KITS ÉVOLUTIFS » ACCESSIBLES ET PARIE SUR UN DÉSIGN ACCROCHEUR.

Où le trouver ? soulscircuit.com

Le Pilet est un micro-contrôleur hybride embarquant un environnement de développement intuitif, une connectique modulaire et un mini-système d'exploitation baptisé « SoulOS », propre à SoulsCircuit. L'objectif : permettre à quiconque – du bricoleur en herbe au développeur chevronné – de donner vie à des projets électroniques et informatiques sans se ruiner en temps ou en argent. Il offre suffisamment de puissance pour faire tourner des applications basiques (domotique, robotique, scripts Python) et même certaines applications web légères. En revanche, ce n'est pas un monstre de puissance pour de la reconnaissance d'image ou du data processing avancé.

Initialement présenté comme un concept lors d'un hackathon en 2023, Le Pilet a su séduire par sa simplicité d'usage et sa compacité. Après deux ans de développement et de retours communautaires, SoulsCircuit commercialise cette année sa carte et ses premiers packs.

MODULES À CLIPSER

L'une des forces de SoulsCircuit réside dans son approche : Le Pilet se conçoit comme une base principale, qui peut accueillir différents modules d'extension. À la manière des solutions Raspberry Pi, la carte principale embarque l'essentiel (processeur, mémoire, stockage,

POUR LES DÉVELOPPEURS

Grâce à l'IDE (environnement de développement) fourni par SoulsCircuit, qui repose sur une interface web accessible depuis n'importe quel navigateur, il est possible de déployer rapidement des scripts en Python, en C ou même en Rust. Cette plateforme SoulOS est compatible avec la plupart des protocoles populaires (MQTT, HTTP, etc.). Les développeurs peuvent tester leurs codes directement depuis l'interface, et collecter des logs pour déboguer leurs programmes.

connectivité). Mais SoulsCircuit va plus loin en proposant des modules de connectique additionnels : un ensemble de ports (HDMI, Ethernet, USB 3.0, etc.) à clipser sur la tranche du Pilet grâce à un connecteur propriétaire. L'arrivée de module spécialisé est donc de la partie avec des caméras, capteurs de mouvement, émetteurs Zigbee ou LoRa, ampli audio, carte GPS... Tout un écosystème conçu pour les makers et développeurs IoT.

UN DESIGN RÉTRO ET ACCROCHEUR

De la même manière, cette approche « tout-en-un » disponible par défaut (ce qui rebutera certains puristes du DIY) concerne aussi le design : des boîtiers modulaires (3D imprimés ou en aluminium) s'assemblent facilement et protègent le cœur du Pilet, tout en assurant un look futuriste.

PRIX

Au moment où nous écrivions ces lignes, SoulsCircuit n'avait pas encore annoncé ses tarifs définitifs. Voici les gammes de prix auxquelles s'attendre :

- **Le Pilet Standard** (carte seule avec processeur ARM double-cœur, 512 Mo de RAM, 4 Go eMMC) : **entre 40 € et 50 €.**
- **Pack "Starter"** (carte + coque de base + alimentation USB-C) : **autour de 55 € à 65 €.**
- **Le Pilet Pro** (carte seule avec 1 Go de RAM, stockage eMMC de 8 Go, batterie interne) : **entre 60 € et 80 €.**
- **Pack "Pro"** (carte + coque premium + modules de connectique HDMI/USB 3.0) : **environ 100 €**
- **Modules et accessoires :**
  > Modules de connectique additionnels (USB 3.0, HDMI, Ethernet, etc.) : **10 € à 20 € par module.**
  > Modules spécialisés (caméras, GPS, Zigbee, LoRa, ampli audio, etc.) : **à partir de 20 €**
  > Covers et coques : **de 5 € à 25 €**

Le design fait partie intégrante de la démarche de SoulsCircuit : grâce à ses coques interchangeables et à sa connectique latérale, Le Pilet se permet d'afficher des lignes minimalistes et des LED discrètes qui indiquent l'état du système. Les coloris disponibles (noir mat, argent, ou encore la version « Cyber Green ») témoignent de la volonté de proposer un objet techniquement avancé et agréable à l'œil.
Pour s'inspirer, SoulsCircuit a notamment étudié la façon dont certains projets comme les Framework Laptop ou le nouveau mini-ordinateur modulable basé sur le Raspberry Pi 5 intègrent des accessoires. Le résultat se veut plus simple, plus intuitif et visuellement attrayant, afin de séduire un large éventail d'utilisateurs, des geeks férus d'électronique jusqu'aux semi-professionnels.

UNE COMMUNAUTÉ EN DEVENIR ?

Similaire à l'esprit d'un Raspberry Pi ou d'un Arduino, Le Pilet dispose d'une communauté en pleine expansion sur le forum officiel. Les ressources pédagogiques se multiplient, et on trouve déjà des didacticiels pour programmer des robots rouleaux, des stations météo ou encore des jeux rétro.

LA CONCEPTION MODULAIRE DES COQUES PERMET L'AJOUT DE DIVERS COMPOSANTS, TELS QU'UN CLAVIER, UNE MANETTE DE JEU OU UNE TABLETTE. SOULSCIRCUIT INDIQUE QUE LES UTILISATEURS POURRONT CRÉER ET DE PERSONNALISER LEURS PROPRES MODULES EN IMPRESSION 3D.

CARACTÉRISTIQUES

- Dimensions : 70 × 45 × 12 mm.
- Processeur : ARM Cortex-A53 double-cœur, 1 GHz.
- RAM : 512 Mo de LPDDR4 sur la version standard, 1 Go sur la version Pro.
- Stockage : 4 Go de mémoire eMMC + slot microSD (jusqu'à 128 Go).
- Connectivité : Wi-Fi 5 (802.11ac), Bluetooth 5.0, USB-C (alimentation et transferts de données).
- Modularité : 20 broches GPIO + connecteurs propriétaires pour modules externes.
- Système d'exploitation : SoulOS
- Batterie : optionnelle (Li-ion), à brancher sous forme de module additionnel.

FACE À LA CONCURRENCE

Le Pilet se situe à mi-chemin entre un microcontrôleur simple (type Arduino) et un micro-ordinateur complet (type Raspberry Pi). Contrairement à un Arduino Uno, il dispose d'un vrai système d'exploitation et d'une connectivité Wi-Fi/Bluetooth intégrée, ce qui le rend plus autonome et plus polyvalent. En revanche, par rapport à un Raspberry Pi Zero ou 4, il est moins puissant en termes de CPU et de RAM, même si son format et sa consommation énergétique sont plus avantageux.

SÉLECTION

TOP 15 Logiciels & services GRATUITS

TOP5 ANTI-ROOTKITS

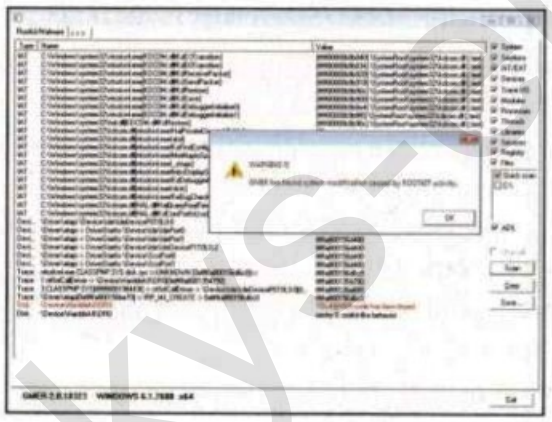
SOPHOS SCAN & CLEAN

> GÉNÉRALISTE

Cet outil gratuit de Sophos est conçu pour détecter et supprimer de nombreux malwares cachés dont les rootkits. Avec un scan rapide et léger, il est idéal pour les systèmes personnels. Si son efficacité contre les menaces courantes est indéniable, il est moins spécialisé que des solutions plus complètes.

Lien : www.sophos.com

GMER > L'EXPERT INTIMIDANT



GMER est un outil spécialisé qui excelle dans la détection des rootkits systémiques. Bien qu'il soit très technique, son aptitude à identifier des anomalies subtiles en fait un incontournable pour les experts en cybersécurité. Seul bémol : il nécessite une certaine courbe d'apprentissage.

Lien : www.gmer.net

MALWAREBYTES ANTI-ROOTKIT

> LE BON COMPROMIS

Intégré désormais à la solution Malwarebytes Free, le scan anti-rootkit (**Sécurité >** activez l'option **Analyser les rootkits)** combine robustesse et précision. Il propose des scans détaillés pour retirer les menaces les plus complexes. Sa richesse fonctionnelle peut intimider les novices.

Lien : www.malwarebytes.com

AVAST FREE ANTIVIRUS

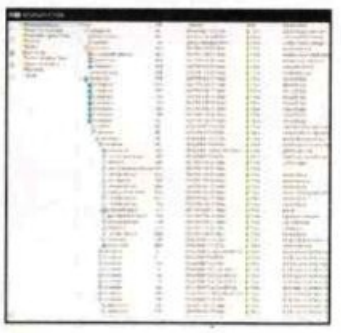
> INTÉGRÉ ET TEMPS RÉEL

Plus qu'un simple antivirus, Avast inclut lui aussi un scanner anti-rootkit dans sa version gratuite. Polyvalent, il offre une protection en temps réel et des options de nettoyage automatisées. Sa limite ? Des fonctions avancées réservées à la version payante.

Lien : www.avast.com

ESET SYSINSPECTOR

> NIVEAU AVANCÉ



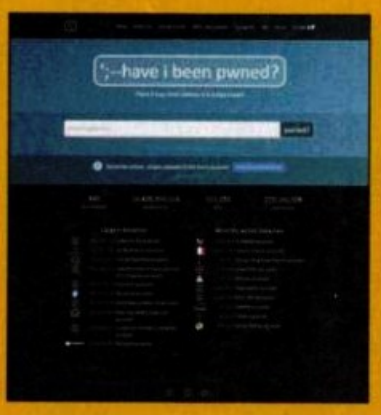
Plus qu'un scanner anti-rootkit, cet outil analyse en profondeur les processus, les services et les fichiers du système pour repérer des anomalies. Idéal pour les utilisateurs avancés, il demande une certaine expertise pour interpréter les résultats.

Lien : www.eset.com/int/support/sysinspector

TOP5 VOS DONNÉES ONT-ELLES FUITÉ ?

HAVE I BEEN PWNED

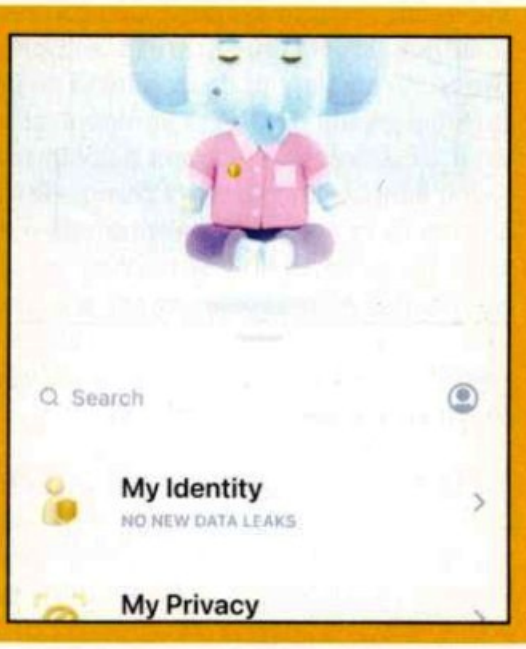
> LE PLUS CONNU



Ce service populaire est une référence pour vérifier si vos données personnelles ont été compromises dans des fuites connues. En saisissant votre email ou votre numéro de téléphone, vous obtenez un rapport détaillé des violations associées.

Lien : haveibeenpwned.com

JUMBO PRIVACY



Toujours disponible, Jumbo scanne vos comptes et vous alerte sur les failles potentielles puis vous guide pour ajuster vos paramètres. Très accessible, certaines fonctionnalités avancées nécessitent un abonnement premium.

Lien : www.jumboprivacy.com

TOP5 TROUVER DES IMAGES LIBRES DE DROITS

PIXABAY > Le plus connu

Pixabay offre plus de 2,6 millions d'images et vidéos libres de droits, incluant des photos, illustrations, vidéos et musiques. Les fichiers sont disponibles en plusieurs résolutions, et l'interface conviviale facilite la recherche par mots-clés et filtres.

Lien : pixabay.com/fr/

UNSPLASH > Pour les exigeants

Réputé pour sa collection de photos artistiques et de haute qualité, avec plus de 3 millions d'images disponibles. Les fichiers sont en haute résolution, et la recherche est facilitée par des collections thématiques.

Lien : unsplash.com

OPENVERSE > Métamoteur

Openverse, anciennement CC Search, est un moteur de recherche dédié aux contenus libres de droits, incluant des images et des vidéos. Il permet de filtrer les résultats par type de licence et source.

Lien : wordpress.org/openverse

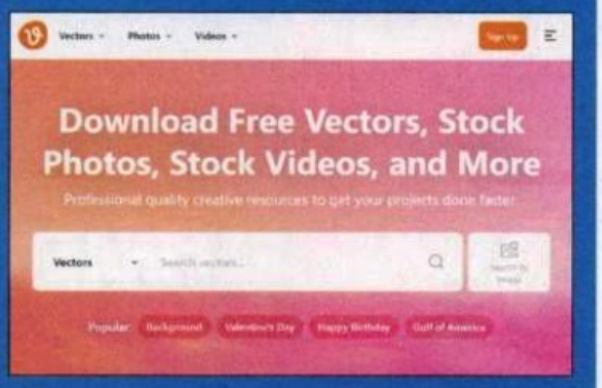
PEXELS > L'alternative

Pexels propose une vaste collection de photos et vidéos gratuites de haute qualité. Les fichiers sont téléchargeables en différentes résolutions. Points forts : contenu moderne et tendance. Limites : moins d'illustrations vectorielles disponibles.

Lien : www.pexels.com/fr-fr/

VECTEEZY > On veut du vecteur !

Vecteezy offre une vaste collection d'illustrations vectorielles gratuites, parfaites pour le design graphique. Les fichiers sont disponibles en formats AI, EPS et SVG, avec des outils de recherche par catégorie et style.



Lien :www.vecteezy.com

FIREFOXMONITOR

Firefox Monitor vous permet de vérifier si vos comptes en ligne ont été compromis lors de fuites de données. Facile à utiliser, il propose des recommandations concrètes pour renforcer vos mots de passe.

Lien : monitor.mozilla.org

SOCIAL ANALYZER

Social Analyzer est un outil open-source qui scanne vos comptes pour repérer les informations accessibles au public. Conçu pour les utilisateurs techniques, il offre une analyse détaillée, mais son utilisation peut paraître complexe pour les novices.

Lien : github.com/qeeqbox/social-analyzer

DEHASHED

DeHashed est un moteur de recherche qui vous permet de vérifier si vos informations personnelles sont exposées. En plus des emails, il couvre les noms d'utilisateur, les adresses IP et bien plus. La version gratuite offre des recherches de base utiles.

Lien : www.dehashed.com

 # Casser les codes et décrypter l'info #

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON SOUS PLI DISCRET

OFFRE ABONNEMENT

1 AN POUR 19,90 € (au lieu de ~~23,60 €~~)

2 ANS POUR 35,40 € (au lieu de ~~47,20 €~~)

- LIVRÉ CHEZ VOUS !
- PRATIQUE & ÉCONOMIQUE !

LES GUIDES du HACKER et du PIRATE

- > Logiciels et applications exclusifs
- > Tutoriels et astuces clairs
- > Dossiers pratiques complets pour débutants et experts
- > Sélection et test de matériels
- > L'actu et les nouveautés !

RÉDUCTION JUSQU'À -25%

À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À RENVOYER SOUS ENVELOPPE AFFRANCHIE À :
BII - SERVICE ABONNEMENT - 15, RUE DE MERY - 60420 MÉNÉVILLERS

☐ **Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 19,90 €**
☐ **Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 35,40 €**

☐ OUI, JE M'ABONNE :

Nom .....
Prénom .....
Adresse .....
.....
Code Postal .....
Ville .....
E-Mail .....

Signature obligatoire :

☐ Je joins mon règlement par chèque à l'ordre de ID PRESSE (France uniquement)

Offre valable en France métropolitaine uniquement.

POUR NOUS CONTACTER :
abonnement.bii@gmail.com

Offre valable jusqu'au 31 décembre 2025. Les délais d'acheminement de La Poste varient selon les régions et pays. Conformément à la loi Informatique et Libertés du 6/1/1978, vous disposez d'un droit d'accès et de rectification quant aux informations vous concernant, que vous pouvez exercer librement auprès de ID PRESSE – 1104, CHEMIN

LES AVANTAGES :

- > **Jusqu'à -25 % sur le prix en kiosques**
- > **Ne manquez aucun numéro**
- > **Ne soyez plus une victime**
- > **Vos magazines livrés chez vous gratuitement**

LES DOSSIERS DU Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ D'ASTUCES

100% Windows

Actuellement #Guide pratique

TOUT FAIRE AVEC L'IA

MESH

GMAIL

GÉOLOCALISATION

TOR

Wi-Fi

WHATSAPP

BIOS

ESPIONS

ANTIVOL

PIRATE
INFORMATIQUE

IDPRESSE id presse

L 12730 - 63 - F: 5,90 € - RD

BELUX 6,80€ - CH 9,50CHF - PORT-CONT 6,90€ - DOM 6,70€ - NCAL 1050XPF - POL 880XPF - MAR 66MAD - TUN 12TND - CAN 10,50$CAD