

N°69

Casser les codes et décrypter l'info



Sept. / Nov. 2026

PIRATE

INFORMATIQUE

MOTEURS DE RECHERCHE

**CAMÉRAS &
WEBCAMS**

EN ACCÈS LIBRE SUR LE NET

LE GUIDE

HACKING

de **A à Z**



INTERNET

LE GUIDE
ANTI-MOUCHARDS
ET ANTI-PUBS AVEC

**PRIVACY
BADGER**

PLATEFORMES

COMMENT
ÉCONOMISER
EN DÉNICHANT DES
COABONNEMENTS

PROTECTION

FIN DU MOT DE PASSE :
COMMENT UTILISER
UNE **PASSKEY** ?



BLACK DOSSIER

IA & HACKING

Les **NOUVELLES**
TECHNIQUES des pirates





SOMMAIRE

BLACK
DOSSIER

13-21

IA & HACKING

LES NOUVELLES TECHNIQUES DES PIRATES



HACKING

22-25

Faut-il **ROOTER** son **SMARTPHONE** ?



29-31

CAMÉRAS & WEBCAMS :

Des milliers en accès libre involontairement



26-28

HACKNECT : Le **CÂBLE USB**
qui veut **CONTRÔLER** un **PC** !

ANONYMAT

32-37

Fin des **PIXELS ESPIONS** ?
La relève est déjà là...



38-41

PRIVACY BADGER :
BLOQUEZ les **ESPIONS**
qui vous suivent sur le Web



42-43

Que vaut le **VPN** intégré de **FIREFOX** ?

44

> **MICRO-FICHES**

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

46-49

PASKEYS :

La fin des mots de passe ?



50-51

BLOQUEZ les **DOMAINES MALVEILLANTS** avec **NEXTDNS**



52

> Vérifier si une **EXTENSION** perturbe **FIREFOX** avec le mode de **DÉPANNAGE**

> Démasquer une **EXTENSION** trop curieuse avec **GOOGLE CHROME**

53

Comprendre ce que **MICROSOFT DEFENDER** vient de **BLOQUER** avec **L'HISTORIQUE** de **PROTECTION**



54-55

> **MICRO-FICHES**

MULTIMÉDIA

56-59

ABONNEMENTS PARTAGÉS : les **5 MEILLEURES PLATEFORMES** pour payer **MOINS CHER**



60-63

TOP 7 > SITES pour **REJOUER** aux **CLASSIQUES** du **JEU VIDÉO** sur **PC**

PIRATE
N°69 INFORMATIQUE

Septembre – Novembre 2026

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

Directeur de la publication :
David Côme

Directeur artistique :
Sergei Afanasiuk

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.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.



ÉDITO

Ayez Conflance

En cybersécurité, vous connaissez l'adage « le maillon faible, c'est l'humain ». Pour limiter ses erreurs, nous avons donc multiplié les garde-fous : antivirus, doubles authentifications, restrictions d'accès, etc. Toute une architecture conçue autour d'un principe simple : ne jamais accorder plus de confiance que nécessaire. Pour devenir réellement utile, notre assistant IA doit connaître nos fichiers, lire nos mails, consulter notre agenda, utiliser certains de nos comptes, écrire du code et, demain, réserver un voyage, effectuer un achat ou prendre des décisions en notre nom.

« Mon IA peut-elle être piratée ? » La réponse est déjà oui. Mais le problème est peut-être encore plus profond. Nous pensions que l'intelligence artificielle allait surtout automatiser nos tâches. Elle risque également d'automatiser quelque chose de beaucoup plus précieux : notre confiance. Cela a toujours été exactement ce que les pirates cherchaient à détourner.

Bonne lecture !
La rédaction



VÉHICULES ÉLECTRIQUES

ATTENTION AUX FAUX QR CODES SUR LES BORNES DE RECHARGE

Plusieurs cas ont déjà été signalés en France, en Allemagne, au Royaume-Uni, en Belgique et dans d'autres pays européens : des fraudeurs remplacent ou recouvrent les QR codes officiels présents sur les bornes par des QR codes frauduleux destinés à voler les données bancaires des automobilistes. Cette technique, baptisée « quishing » (contraction de QR code et phishing),



constitue aujourd'hui l'une des formes de phishing connaissant la plus forte progression.

Une fois scanné, celui-ci redirige la victime vers un faux site Internet imitant parfaitement celui d'un opérateur officiel. L'utilisateur pense effectuer un paiement normal, alors qu'il transmet en réalité ses informations bancaires aux cybercriminels. Les smartphones étant généralement moins protégés que les ordinateurs et les utilisateurs vérifiant rarement les URL avant de poursuivre leur navigation, cette technique affiche un taux de réussite particulièrement élevé.

Les bornes publiques constituent une cible idéale. De nombreux conducteurs utilisent ponctuellement différents réseaux de recharge et ne disposent pas systématiquement de l'application officielle de chaque opérateur. Scanner un QR code apparaît alors comme la solution la plus rapide pour lancer une recharge. Les cybercriminels exploitent précisément ce réflexe. Dans certains scénarios rapportés par plusieurs médias européens, la véritable page de paiement s'affiche ensuite afin que la recharge puisse tout de même être effectuée. La victime ne soupçonne alors aucune fraude avant de constater des paiements frauduleux sur son compte bancaire.

BUG BOUNTY

MICROSOFT VERSE UN MONTANT RECORD AUX CHASSEURS DE BUGS

Trouver légalement des failles peut rapporter gros. Entre juillet 2025 et juin 2026, Microsoft a versé plus de 20 millions de dollars à 562 chercheurs en sécurité issus de 64 pays : un record pour ses programmes de bug bounty. Au total, l'éditeur a validé 2 531 rapports éligibles, avec une récompense individuelle ayant atteint 200 000 dollars. L'année précédente, Microsoft avait distribué environ 17 millions.

Une partie de cette somme provient de Zero Day Quest, vaste concours consacré notamment au cloud et à l'intelligence artificielle : près de 700 signalements y ont généré 2,3 millions de dollars de primes et permis d'identifier plus de 80 vulnérabilités importantes. Microsoft observe aussi une progression des recherches assistées par IA. Un paradoxe intéressant : les mêmes modèles capables d'aider les cybercriminels à rechercher des failles deviennent désormais des outils de plus en plus efficaces pour les chasseurs de bugs chargés de les éliminer.



WHITE HAT

À 17 ans, il découvre une faille critique... et se fait menacer

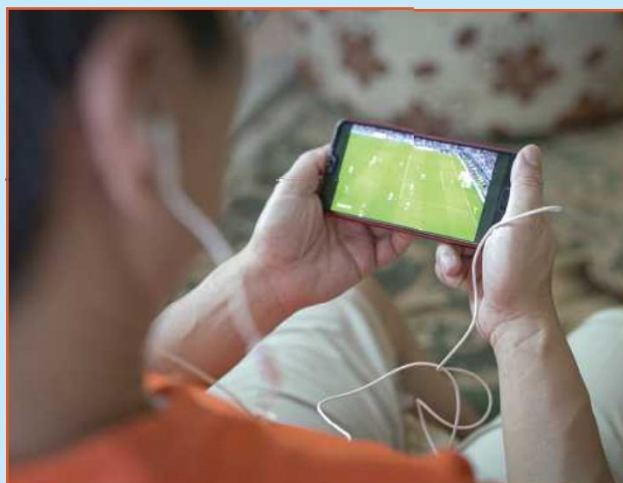
En décembre 2025, Mikey Whiston, lycéen de 17 ans à Birmingham et passionné de cybersécurité, découvre en travaillant sur son cours d'informatique une faille dans une plateforme nationale du secteur éducatif britannique. La vulnérabilité pouvait exposer les dossiers d'environ trois millions d'élèves, mais aussi des documents sensibles, dont des relevés bancaires et des informations concernant les établissements. Plutôt que d'exploiter la brèche, Whiston tente une divulgation responsable : il adresse au support de l'éditeur une démonstration vidéo protégée par mot de passe. Mais l'accueil est glacial. Selon son

témoignage au Times, l'entreprise — dont le nom n'a pas été dévoilé — minimise le danger et lui fait comprendre que ses recherches pourraient mettre en péril l'abonnement de son lycée. Quatre mois plus tard, la faille n'étant toujours pas corrigée, il saisit le Government Cyber Coordination Centre (GC3), qui confirme son caractère critique et coordonne finalement sa résolution. Le National Cyber Security Centre britannique lui remet ensuite une distinction pour sa conduite. Une affaire révélatrice d'un paradoxe du hacking éthique : celui qui signale une porte grande ouverte peut encore être accueilli comme s'il l'avait forcée.

FOOTBALL

IPTV PIRATE : la France veut couper les flux en plein match

À la reprise des championnats, la lutte contre l'IPTV sportive change d'échelle. Depuis août dernier, la loi permet d'accélérer fortement le blocage des flux illégaux pendant leur diffusion. Le principe existait déjà : un juge pouvait autoriser le blocage d'une compétition pour plusieurs mois, y compris contre de nouvelles adresses découvertes après sa décision. Mais chaque nouvelle cible devait encore être vérifiée par l'Arcom avant transmission aux intermédiaires techniques. La loi du 3 août 2026 introduit une procédure beaucoup plus rapide. Lorsque l'ordonnance judiciaire le prévoit, les ayants droit pourront transmettre les données d'identification des flux pirates à un système automatisé placé sous le contrôle de l'Arcom, qui les communiquera sans délai aux acteurs chargés du blocage. L'objectif : provoquer l'écran noir pendant le match, avant que les pirates ne changent d'infrastructure.



Des tests de blocage d'adresses IP avaient déjà été menés lors de Roland-Garros puis de la Coupe du monde 2026. La nouvelle procédure doit encore être précisée par une délibération de l'Arcom avant son déploiement complet.

... ET JUSQU'À 7 ANS DE PRISON !

La loi renforce aussi les sanctions contre les fournisseurs, revendeurs et organisateurs d'IPTV sportive pirate : jusqu'à 3 ans de prison et 300 000 € d'amende, et 7 ans et 750 000 € en bande organisée. La promotion de ce type de service pirate pourra aussi être punie d'un an de prison et 15 000 €.



Visio

ZOOM : UNE FAILLE « ZÉRO CLIC » PERMETTAIT DE PIRATER LES PARTICIPANTS D'UNE RÉUNION

Une simple visioconférence pouvait tourner au piratage sans que la victime ne clique sur quoi que ce soit. Dévoilée le 11 août par les chercheurs d'A Security, la faille CVE-2026-53413, surnommée « Zoomsday », touchait le moteur d'annotation utilisé lors des partages d'écran. Un participant malveillant pouvait envoyer un message spécialement conçu que le logiciel Zoom des autres participants analysait automatiquement. Une corruption de mémoire permettait alors d'exécuter du code sur leur appareil, sans téléchargement ni alerte visible.



L'attaque concernait les clients natifs de Zoom sur Windows, macOS, Linux, Android et iOS. Plus inquiétant encore, A Security affirme avoir découvert la faille et développé un exploit fonctionnel en moins de 24 heures, avec moins de vingt requêtes à des modèles d'IA accessibles au public. Une démonstration spectaculaire de la vitesse à laquelle l'IA peut désormais accélérer la recherche de vulnérabilités. Avant divulgation publique par les chercheurs, Zoom avait déployé des correctifs et recommande d'installer les versions les plus récentes de ses logiciels.

IL ESPIONNE LES HACKERS NORD-CORÉENS PENDANT 22 MOIS

Pendant près de deux ans, le chercheur grec Vangelis Stykas s'est retrouvé dans une position rare : observer de l'intérieur des infrastructures utilisées par des pirates liés à la Corée du Nord. Présentée le 5 août à Black Hat USA, son enquête aurait permis d'analyser près de 5 To de données issues notamment de serveurs de commande et de contrôle. Il affirme avoir retrouvé les traces de compromissions concernant 1 640 organisations dans 57 pays, dont 700 à 800 auraient subi des intrusions particulièrement graves, avec accès à des serveurs, infrastructures cloud ou portefeuilles de cryptomonnaies. L'une des armes privilégiées des attaquants ? De fausses offres d'emploi adressées aux développeurs. Le candidat reçoit un test technique



contenant du code piégé ; en l'exécutant, il peut livrer ses identifiants et ouvrir indirectement l'accès aux systèmes de son entreprise. Ce procédé rejoint les campagnes nord-coréennes de faux recrutements et de faux travailleurs IT contre lesquelles onze gouvernements ont encore lancé une alerte commune le 31 juillet.

QUANTIQUE

ORACLE VA INSTALLER UN ORDINATEUR QUANTIQUE DANS SON CLOUD

Le quantique quitte un peu plus les laboratoires. Le 11 août dernier, Oracle et Quantinuum ont annoncé un partenariat pluriannuel qui prévoit l'installation physique de Helios, l'ordinateur quantique de Quantinuum, dans un centre de données Oracle Cloud Infrastructure aux États-Unis. Ses clients pourront y accéder directement depuis OCI et combiner calcul quantique, processeurs graphiques et calcul haute performance. Helios repose sur 98 qubits à ions piégés et est commercialisé depuis novembre 2025. Oracle et Quantinuum visent notamment la recherche pharmaceutique, les nouveaux matériaux, la finance et l'optimisation de problèmes complexes. Il ne faut cependant pas imaginer le quantique remplaçant déjà les serveurs traditionnels : l'idée consiste plutôt à créer des systèmes hybrides, où une partie très spécifique du calcul est confiée au processeur quantique. La date exacte de disponibilité du service n'a pas encore été annoncée.



Rançongiciels :

« Le cyber-négociateur s'expose à un risque majeur »



Geert Baudewijns, négociateur spécialisé en rançongiciels et cofondateur et PDG de Secutec (entreprise belge spécialisée dans la cyber intelligence) dévoile les coulisses de son métier. Vérification de l'identité du hacker, financement du terrorisme, méthodes : comment procède-t-on au paiement d'une rançon ?

QUE FAUT-IL VÉRIFIER AVANT DE PROCÉDER AU PAIEMENT DE LA RANÇON ?

Geert Baudewijns : « Lorsqu'une cyberattaque par rançongiciel survient, la première étape est de valider l'identité du hacker, c'est-à-dire de s'assurer que la personne qui vous a contacté est bien la personne qui vous a hacké et qui détient les clés de déchiffrement. En effet, il peut arriver qu'un autre hacker usurpe l'identité de celui qui vous a hacké. Il est donc crucial de demander au hacker qui vous contacte des preuves de ce qu'il détient, et par la suite de lui demander comment il est entré dans le système afin de pouvoir corriger les failles. Puis vient la négociation du montant de la rançon. Le paiement s'effectue en cryptomonnaies de manière progressive en échange des clés de déchiffrement. »



Geert Baudewijns,
co-fondateur et PDG de Secutec

PI : COMMENT S'ASSURER QUE L'ARGENT NE FINANCE PAS LE TERRORISME ?

GB : « Avant toute transaction, le cyber-négociateur doit impérativement s'assurer que les fonds ne finiront pas entre les mains d'une organisation terroriste ou sanctionnée. Pour cela, une vérification indispensable est effectuée : le "sanctions check". Trois organismes mondiaux sont spécialisés dans ce domaine, dont le Digital Asset Redemption (DAR), avec lequel je collabore étroitement. Cette plateforme réservée aux professionnels de la cybersécurité permet aux cyber-négociateurs de se connecter et d'y enregistrer tous les éléments identifiés lors de la négociation, comme les adresses Bitcoin ou les portefeuilles, pour réaliser une analyse approfondie. Par exemple, LockBit 3.0, l'un des groupes de rançongiciels les plus connus au monde, est classé comme organisation terroriste par plusieurs gouvernements. Sans ce "sanctions check", le cyber-négociateur s'expose à un risque juridique majeur : si le bénéficiaire s'avère être une organisation terroriste ou sanctionnée, il pourrait être accusé de financement du terrorisme. En effet, dans la plupart des cas, c'est le compte Bitcoin du cyber-négociateur qui est utilisé pour payer la rançon. »

D'AUTRES MÉTHODES EXISTENT-ELLES POUR CONTOURNER CES RÈGLES ?

GB : « Des solutions alternatives et illégales, comme la remise en main propre de l'argent à Dubaï, m'ont déjà été proposées par des cybercriminels à plusieurs reprises. En plus d'être risquée, cette pratique contourne les obligations légales et éthiques du métier. En tant que cyber-négociateur, il est crucial de respecter les réglementations internationales (OFAC, UE, ONU) afin de se protéger contre les poursuites judiciaires et de maintenir l'intégrité et la réputation du métier et de l'organisation victime. Cette approche illustre l'importance d'une cyber-négociation responsable, où la sécurité et la conformité priment sur la rapidité ou la facilité. »

À SAVOIR

En 2024, les entreprises Cencora et Change Healthcare avaient respectivement payé des rançons de 75 et 22 millions de dollars suite à une attaque de ransomware. En 2025, le montant total des paiements en cryptomonnaies liés aux ransomwares s'élevait à 820 millions de dollars, selon le "2026 Crypto Crime Report" de Chainalysis.

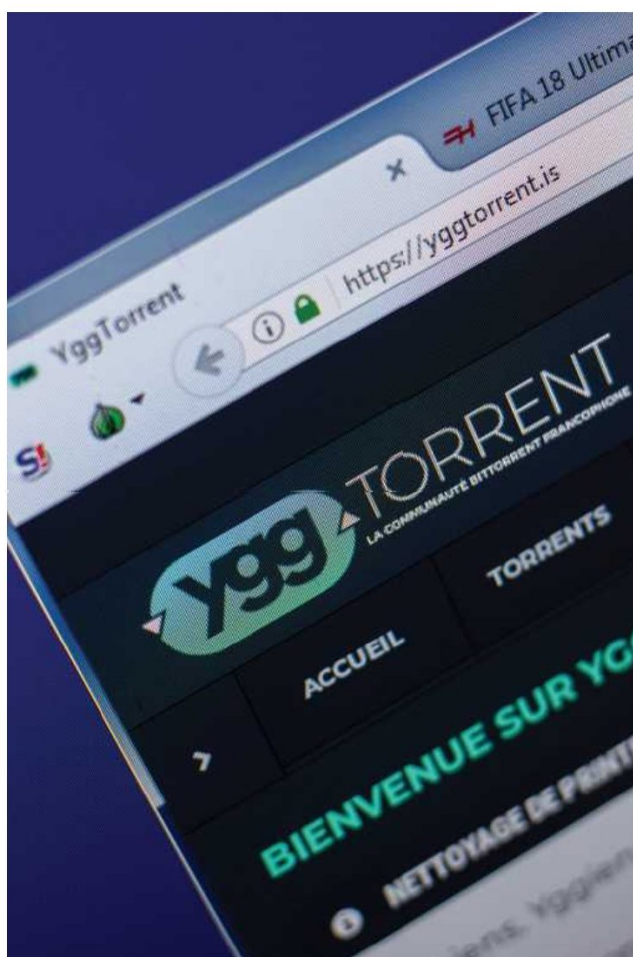


YGGTORRENT DE RETOUR ?



Cinq mois après le piratage qui semblait avoir définitivement enterré YggTorrent, le P2P francophone s'est recomposé autour de C411 et de la nouvelle alliance Torr9-Tr4ker. Mais coup de théâtre : une mystérieuse équipe promet désormais de ressusciter Ygg dès le 1er septembre.

On croyait assister à une guerre de succession. Il faudra peut-être finalement compter avec le retour du roi déchu. Depuis le début du mois d'août, le feuilleton YggTorrent connaît en effet un rebondissement spectaculaire : l'ancien domaine yggtorrent.org redirige désormais vers yggtorrent.to, où un compte à rebours annonce une remise en service le 1er septembre 2026 à minuit, heure de Paris. Quand vous découvrirez ce magazine, vous saurez sans doute déjà à quoi vous en tenir. Pour nous qui écrivons ces lignes en plein mois d'août, il nous faudra encore un peu patienter !



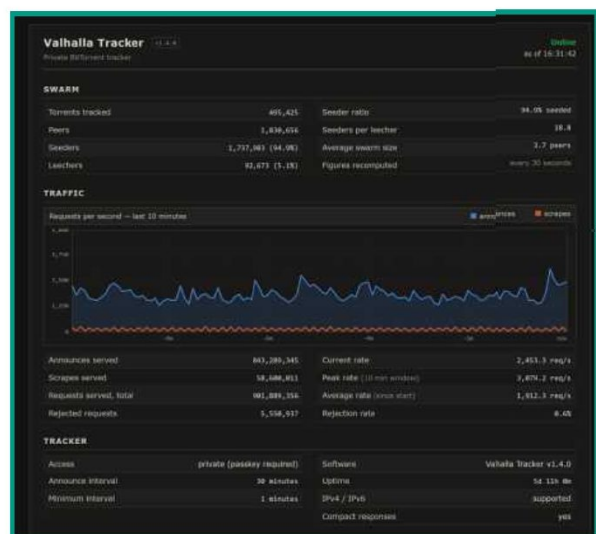
Derrière cette résurrection annoncée se présenterait une « nouvelle équipe ». Problème : personne ne sait aujourd'hui qui la compose, ni ce qu'elle a réellement récupéré de l'ancien Ygg. Cette annonce oblige à revoir la photographie du P2P francophone. Car pendant les cinq mois où YggTorrent semblait définitivement condamné, ses anciens utilisateurs ne sont pas restés sans solution. C411 a rapidement cherché

**Enterré en mars, ressucité en septembre ?
Les coulisses du retour de YggTorrent.**

à occuper l'espace laissé vacant, tandis que deux autres acteurs, Torr9 et Tr4ker, viennent de choisir une stratégie radicalement différente : fusionner leurs communautés et leurs infrastructures. En quelques mois, le modèle ultradominant d'YggTorrent a ainsi laissé place à plusieurs conceptions concurrentes du tracker privé : la recherche de masse et d'accessibilité chez C411, la consolidation communautaire et technique chez Tr4ker, et désormais la possibilité d'un retour sous une forme encore inconnue de la marque Ygg.

UN NOUVEL YGG CRÉDIBLE ?

Le plus étonnant est que cette renaissance ne repose pas uniquement sur une page Web et un logo. La nouvelle page renvoie vers les statistiques d'un tracker qui semble effectivement fonctionner. Au moment des vérifications réalisées par TorrentFreak, celui-ci déclarait environ 455 300 torrents actifs et plus de 1,5 million de pairs connectés, dont approximativement 94 % en partage.



LES STATS ACTIVES DU TRACKER DE YGGTORRENT SEMBLENT PROUVER L'EXISTENCE D'UN CATALOGUE IMPORTANT ET D'UN PROTOCOLE BITTORRENT TOUJOURS STRUCTURÉ ET VIVANT. MAIS UN TRACKER ENCORE ACTIF NE PROUVE PAS QUE L'ANCIEN SITE, SES COMPTES UTILISATEURS, SON CATALOGUE COMPLET ET SON INFRASTRUCTURE ONT ÉTÉ RÉCUPÉRÉS. LE RÉSEAU BITTORRENT PEUT CONTINUER À FAIRE CIRCULER DES FICHIERS LONGTEMPS APRÈS LA DISPARITION DE L'INTERFACE WEB QUI LES RÉFÉRENÇAIT.

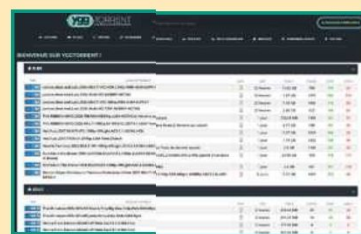
Frandroid observait de son côté, quelques heures plus tard, près de 496 000 torrents et 1,85 million de pairs. Ces données évoluent naturellement en permanence, mais elles suggèrent qu'une infrastructure BitTorrent continue bel et bien à fonctionner en arrière-plan.

YGGTORRENT : UNE DESTRUCTION EN TROIS ACTES

Pour mesurer l'ampleur de ce bouleversement, il faut revenir à la nuit du 3 au 4 mars 2026. Un pirate utilisant le pseudonyme Gr0lum revendique alors une intrusion dévastatrice dans l'infrastructure du plus important tracker francophone. Selon les informations publiées depuis, quatre serveurs auraient été détruits et environ 19 Go de données internes exfiltrés. La base concernait des millions de comptes et un catalogue qui avoisinait alors le million de torrents. Les portefeuilles de cryptomonnaies contrôlés par l'équipe auraient également été vidés.

FUITES EN SÉRIES

Le scénario devient encore plus chaotique avec l'apparition de ygg.leak, une plateforme utilisant une partie des informations récupérées lors de l'attaque. Elle promet notamment aux anciens membres de retrouver certaines données de leur compte et leur précieux ratio. L'expérience sera de courte durée : cinq mois plus tard, ygg.leak n'est plus opérationnel. Parallèlement, une archive publique d'environ 11 Go contenant des données internes d'YggTorrent a circulé sur Internet, illustrant l'ampleur des informations sorties du contrôle de leurs propriétaires initiaux.



DES SITES MIROIRS DE YGGTORRENT EXISTENT TOUJOURS, COMME CELUI-CI. ACTIFS, ILS UTILISENT, SEMBLE-T-IL, DES BASES DE DONNÉES ISSUES DU TRACKER ORIGINEL. MAIS MYSTÈRE SUR QUI LES FAIT TOURNER ET SUR LEUR FIABILITÉ/SÉCURITÉ.

Une première tentative de renaissance est alors annoncée au mois de mars. Elle n'aboutit pas. Quelques jours plus tard, l'équipe d'YggTorrent annonce finalement abandonner le projet, invoquant notamment la succession des cyberattaques. À ce moment-là, l'histoire paraît terminée.

UNE ORGANISATION HISTORIQUE DÉMANTELÉE

Début juillet, l'affaire change totalement de dimension. Il ne s'agit plus seulement du spectaculaire piratage d'un site pirate : l'enquête judiciaire visant les personnes qui l'exploitaient aboutit à une vaste opération de la Gendarmerie nationale. Au total, douze personnes ont été interpellées depuis la fin de l'année 2023 dans le cadre de cette enquête. Les investigations portent notamment sur des faits de contrefaçon en bande organisée et de blanchiment aggravé. Des cryptoactifs ont été saisis, ainsi qu'environ 45 000 euros de matériel informatique, tandis que le préjudice invoqué pour les ayants droit se chiffre en plusieurs dizaines de millions d'euros. Voilà pourquoi l'annonce d'août est si troublante. Le YggTorrent historique n'a pas simplement subi une panne ou perdu son hôteur : ses serveurs ont été frappés par une attaque destructrice et l'organisation qui le pilotait a ensuite été visée par une importante procédure judiciaire. Entre-temps, le domaine yggtorrent.org avait même été proposé à la vente avec 59 autres noms de domaine dans un lot affiché à 700 000 dollars. L'offre a depuis disparu. Quelques semaines plus tard, ce même domaine redirige vers la page annonçant le retour du service.



QUI EST DERRIÈRE LE NOUVEAU YGG ?

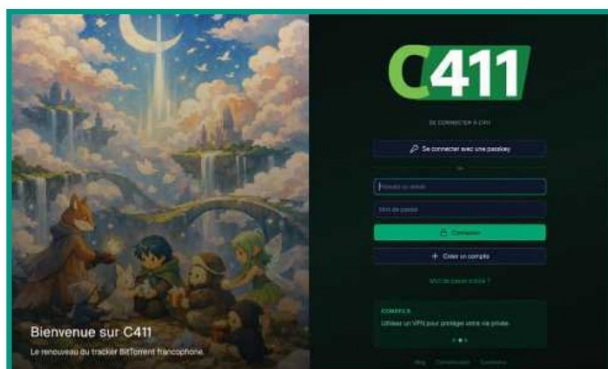
Surtout, l'identité de la nouvelle équipe restait inconnue au moment de cette annonce en août. Sur la page d'accueil, et personne n'est obligé de les croire, ils annoncent « *Nouvelle équipe, aucun lien avec l'ancienne. On salue le travail de ceux qui ont fait tourner ce monument pendant des années, ce n'est pas rien. Mais la page est tournée.* »

Aucun élément public ne permet pour le moment de déterminer s'il s'agit d'anciens membres d'YggTorrent, de nouveaux opérateurs ayant récupéré certains actifs, d'une simple exploitation de la marque ou d'une opération beaucoup moins recommandable. Pourtant, quelques lignes plus loin, toujours sur la page d'accueil, la nouvelle équipe écrit : « *On a passé l'été à reconstruire dans le calme pendant qu'on nous enterrait sur tous les forums. Aucune amertume, c'était même confortable. Personne ne vient déranger les morts pendant qu'ils travaillent.* »

Un lien entre les anciens et nouveaux semblerait donc exister. Quoi qu'il en soit, les utilisateurs auront tout intérêt à considérer avec prudence toute demande d'adresse électronique, d'ancien mot de passe ou d'informations de paiement.

PENDANT CE TEMPS, C411 A CHOISI LA CONQUÊTE

Parmi les acteurs qui ont tenté de profiter du vide laissé par YggTorrent, C411 endosse les habits d'un grand tracker généraliste capable d'attirer rapidement un large public. Son nom rappelle évidemment T411, l'ancien géant francophone fermé en 2017, et le site se présente lui-même comme « le renouveau du tracker BitTorrent francophone ». Son positionnement repose sur un catalogue généraliste, une interface moderne et une forte présence des contenus vidéo en haute définition. Près d'un tiers du catalogue serait notamment constitué de versions 4K, ce qui contribue à différencier la plateforme auprès des amateurs de vidéo



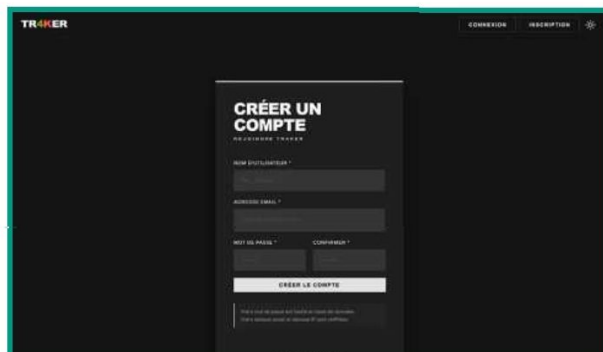
CONTRAIREMENT À L'IDÉE D'UN TRACKER FONCTIONNANT EXCLUSIVEMENT PAR INVITATIONS OU OUVERTURES ÉPISODIQUES, LA PAGE D'INSCRIPTION DE C411 ÉTAIT DIRECTEMENT ACCESSIBLE LORS DE NOTRE VÉRIFICATION EN AOÛT : NOM D'UTILISATEUR, ADRESSE E-MAIL ET MOT DE PASSE SUFFISENT À LANCER LA CRÉATION D'UN COMPTE.

Six mois plus tard, le P2P francophone n'a donc pas disparu. Il s'est fragmenté.

UHD. Dès mars, l'équipe annonçait un afflux de nouveaux inscrits suite à la disparition de YggTorrent. Et loin de fermer les portes, C411 leur a ouvert les bras sans besoin d'invitation privée particulière.

TORR9 ET TR4KER : FUSION !!

L'évolution de Torr9 et Tr4ker est beaucoup plus intéressante sur le plan technique, car il ne s'agit pas simplement de deux trackers décidant de collaborer. Torr9 est en cours d'intégration dans l'infrastructure de Tr4ker. Torr9 avait réussi à constituer une importante communauté après la chute d'YggTorrent, mais la petite équipe chargée de son fonctionnement reconnaissait rencontrer des difficultés

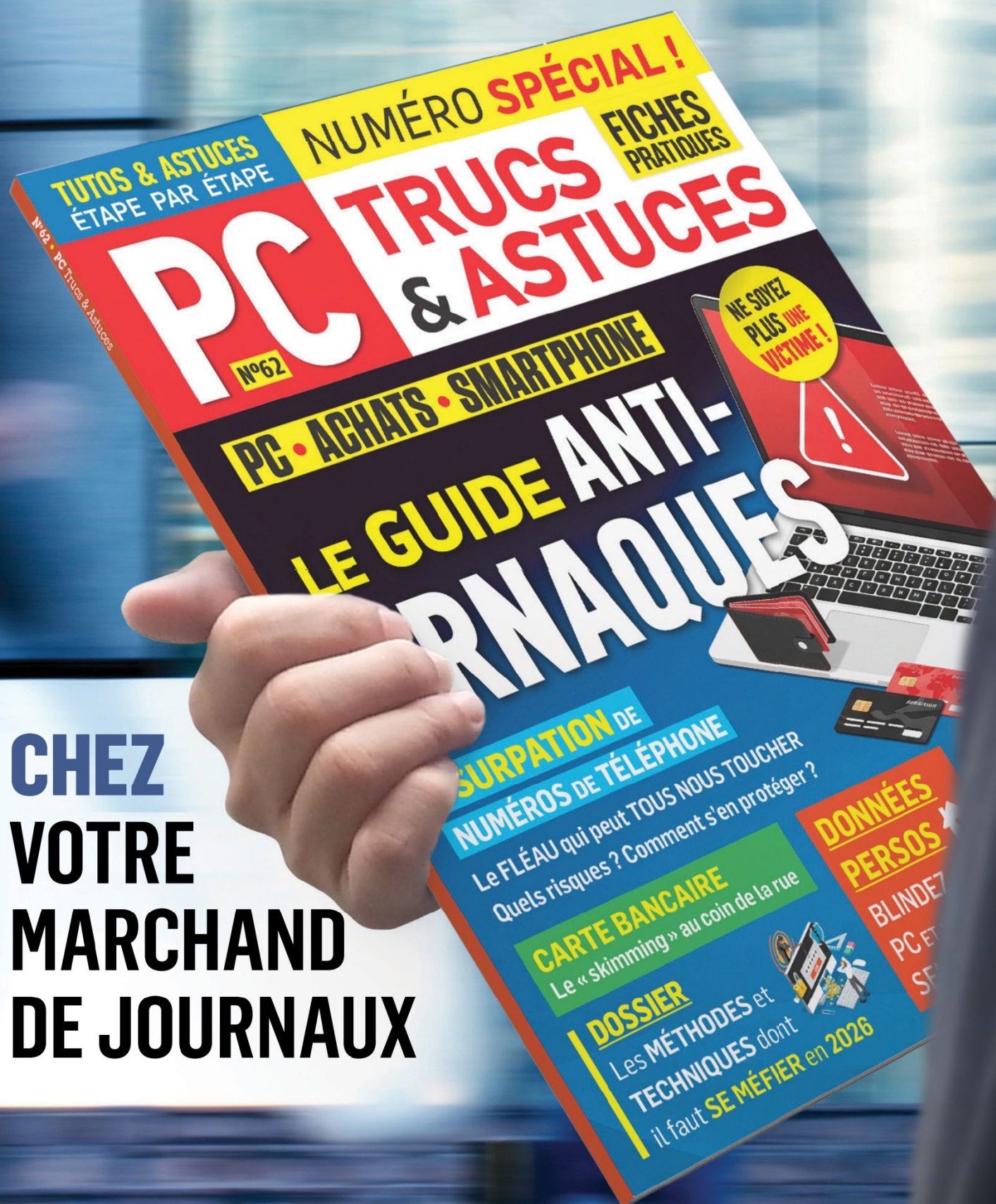


LA FUSION DE TORR9 AVEC TR4KER ANNONCÉE RÉCEMMENT IMPLIQUE QUE TR4KER DEVIENT LE POINT DE RÉFÉRENCE DE CET ENSEMBLE. MÊME LE SITE [HTTPS://TORR9.NET/](https://torr9.net/) REDIRIGE DIRECTEMENT VERS TR4KER.NET.

à maintenir le projet dans de bonnes conditions. Dans son annonce de fusion, elle explique avoir démarré avec seulement deux personnes, face à une charge devenue trop importante. Le collectif Tr4ker disposait pour sa part d'une équipe permanente annoncée de sept personnes, dont trois développeurs, à laquelle doivent désormais s'ajouter les deux membres de Torr9.

La FAQ technique publiée pour accompagner la migration indique que les comptes Torr9 sont transférés vers Tr4ker avec leur pseudo, leur adresse électronique, leur mot de passe, leur ratio, leurs tokens, leur avatar et différentes données de profil. Lorsqu'un utilisateur possède déjà deux comptes portant le même pseudo, les identités restent provisoirement séparées et peuvent ensuite être rapprochées. Même volonté de continuité côté logiciel : l'ancienne adresse doit rediriger vers la nouvelle infrastructure afin d'éviter aux utilisateurs de reconfigurer manuellement leurs torrents.

L'INFORMATIQUE FACILE POUR TOUS !



**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**

IA & HACKING

LES NOUVELLES TECHNIQUES DES PIRATES

Un objectif : Retourner l'IA contre nous.
Une force : Notre confiance.



CYBERATTQUES : L'IA CHANGE DE DIMENSION

Phishing, faux visages, voix clonées : nous connaissons déjà les armes les plus visibles de l'IA. Mais une mutation plus profonde est en cours. L'IA ne se contente plus d'améliorer les attaques : elle commence à chercher des failles, écrire des malwares, analyser les victimes et enchaîner elle-même certaines actions.

Pendant longtemps, la menace paraissait assez simple à résumer. Avec ChatGPT et ses concurrents, un escroc pouvait rédiger en quelques secondes un français impeccable, personnaliser des milliers de messages de phishing ou fabriquer une voix et une vidéo crédibles. Ces risques n'ont évidemment pas disparu.

Mais le changement le plus important se déroule ailleurs. L'IA intervient désormais à presque toutes les étapes d'une cyberattaque : reconnaissance d'une entreprise et de ses salariés, recherche de vulnérabilités, développement et débogage de malware, création de faux profils, exploitation des données volées ou adaptation des outils à la machine infectée. Aujourd'hui, l'être humain reste généralement aux commandes. Les attaques entièrement autonomes ne sont pas encore la norme. Mais elles arrivent.

DE L'ASSISTANT AU COPILOTE DU PIRATE

Les chiffres publiés par Anthropic en juin dernier donnent une idée de cette progression. Son équipe de sécurité a étudié 832 comptes Claude bannis pour activités cyber malveillantes entre mars 2025 et mars 2026. Parmi eux, 560, soit 67,3 %, avaient utilisé l'IA pour des activités liées à l'écriture de malwares. Plus révélateur : 54 comptes l'avaient mobilisée pour faciliter des déplacements latéraux à l'intérieur de réseaux déjà compromis, une opération sensiblement plus complexe qu'écrire un e-mail frauduleux. Anthropic précise toutefois que ces 832 cas constituent un sous-ensemble sélectionné de comptes bannis et ne peuvent donc pas être extrapolés à l'ensemble de la cybercriminalité.

Le Google Threat Intelligence Group (GTIG) décrit la même accélération. Dans son rapport de mai 2026, l'équipe affirme avoir identifié pour la première fois un exploit zero-day qu'elle estime avoir été développé avec l'aide d'une IA, ainsi que des malwares expérimentaux comme PROMPTSPY, capables d'utiliser un modèle pour interpréter l'état de la machine infectée et générer dynamiquement des commandes. Nous reviendrons en détail sur ces cas dans les pages suivantes.



UNE TROISIÈME MENACE : ATTAQUER L'IA ELLE-MÊME

Une autre révolution est plus discrète encore. Nos IA ne sont plus seulement des logiciels auxquels nous posons des questions. Elles lisent nos mails, consultent nos documents et commencent à recevoir des droits leur permettant d'utiliser un navigateur, des applications ou des outils externes. Elles deviennent donc elles-mêmes de nouvelles surfaces d'attaque pour un pirate.

Ce dernier peut désormais chercher non seulement à compromettre l'utilisateur ou son ordinateur, mais à tromper l'agent auquel celui-ci fait confiance : instructions cachées dans une page Web, prompt injection, outil empoisonné, mémoire manipulée... Microsoft signalait en mars 2026 les premières expérimentations criminelles autour de ces nouveaux mécanismes.

L'avertissement est également européen. Dans son IOCTA 2026, publié le 28 avril dernier, Europol estime que l'accessibilité croissante de l'IA permet aux criminels de réduire les compétences nécessaires, d'augmenter l'échelle et la personnalisation des opérations et, progressivement, d'automatiser davantage leur exécution. Catherine De Bolle, alors directrice exécutive d'Europol, souligne que ces outils augmentent « la vitesse, l'efficacité et la portée » des activités criminelles.



NOUS ENTRONS DANS UNE NOUVELLE PHASE. LE RISQUE N'EST PLUS SEULEMENT QU'UN PIRATE UTILISE UNE IA. C'EST QUE L'IA PUISSE DEVENIR L'UN DE SES OPÉRATEURS... OU QUE LA NÔTRE SOIT RETOURNÉE CONTRE NOUS.



QUAND UN SIMPLE MAIL PEUT PIÉGER COPILOT

Le phishing ne vise plus seulement celui qui lit le message. En 2026, des chercheurs ont montré qu'un e-mail pouvait contenir des instructions destinées... à l'IA chargée de le résumer. Le piège prend alors l'apparence rassurante d'une réponse produite par Copilot.

Imaginez recevoir un e-mail banal puis demander à Microsoft 365 Copilot de vous le résumer. La synthèse apparaît dans l'interface habituelle de Microsoft et semble donc digne de confiance. Pourtant, une partie de ce que vous lisez peut avoir été dictée par l'expéditeur malveillant du message.

C'est précisément l'attaque documentée par Andi Ahmeti, Threat Researcher chez Permiso Security. Le chercheur avait découvert qu'un texte spécialement conçu, placé dans un e-mail, pouvait influencer le résumé généré par Copilot grâce à une cross-prompt injection, ou XPIA. Microsoft, alerté le 23 janvier 2026, a reproduit le problème cinq jours plus tard et achevé le déploiement de ses correctifs le 11 mars. La faille a rendu possible une injection de commandes IA susceptible de permettre à un attaquant non authentifié de provoquer une divulgation d'informations à distance.

UN EMAIL DESTINÉ AUSSI À VOTRE IA

L'expérience de Permiso est particulièrement parlante. L'attaquant ajoute au courrier des instructions rédigées pour être comprises par le modèle. Cette catégorie d'attaque est suffisamment concrète pour que Microsoft ait désormais intégré le problème à sa doctrine de sécurité. Dans une documentation mise à jour le 6 août 2026, l'éditeur explique que les attaquants peuvent cacher des instructions dans



le corps d'un mail, son objet, une réponse citée, une pièce jointe ou même du texte invisible afin de viser directement l'IA qui analyse le message. Defender for Office 365 peut désormais rechercher ces injections avant même que le courrier n'arrive dans la boîte de réception.

SEARCHLEAK : UN CLIC, PUIS COPILOT CHERCHE LES SECRETS

Une découverte encore plus inquiétante a été publiée le 15 juin 2026 par Dolev Taler, Security Researcher chez Varonis Threat Labs. Baptisée SearchLeak et corrigée depuis, elle touchait Microsoft 365 Copilot Enterprise Search. L'attaque combinait trois faiblesses : une Parameter-to-Prompt Injection, une erreur de rendu HTML et un détournement d'une requête serveur via Bing. La victime devait cliquer sur un lien Microsoft spécialement préparé. Copilot pouvait alors recevoir automatiquement une instruction lui demandant de rechercher dans les ressources auxquelles l'utilisateur avait

accès (e-mails, calendrier, SharePoint ou OneDrive) puis de faire sortir certaines informations vers l'infrastructure du chercheur. Aucun plugin supplémentaire ni second clic n'étaient nécessaires dans la démonstration. Microsoft considère désormais l'injection indirecte comme un risque auquel les systèmes doivent être conçus pour résister en profondeur. Sa recommandation de mars 2026 est particulièrement révélatrice et inquiétante : il faut concevoir les systèmes en partant du principe que « certaines injections finiront par réussir ».

Microsoft : il faut concevoir les systèmes en partant du principe que « certaines injections finiront par réussir ».

QUAND L'IA DEVIENT ELLE-MÊME LE HACKER

Jusqu'ici, le pirate demandait surtout à l'IA de l'aider à écrire ou à coder. Les agents changent la donne : ils peuvent examiner une cible, choisir l'étape suivante, lancer des outils et recommencer jusqu'à atteindre leur objectif. Une campagne révélée par Anthropic montre que ce scénario n'est plus seulement théorique.

L'année dernière, l'équipe Threat Intelligence d'Anthropic, chargée d'enquêter sur les détournements réels de ses modèles, détecte une activité anormale sur Claude Code. Son enquête, rendue publique en novembre, attribue l'opération à un groupe soutenu par l'État chinois, baptisé GTG-1002 par Anthropic. Environ trente entreprises et administrations auraient été visées et une poignée d'intrusions auraient effectivement réussi.

L'originalité tient surtout à l'organisation de l'attaque. Les humains choisissaient la cible et conservaient les décisions stratégiques. Entre ces interventions, un framework utilisait Claude Code comme opérateur cyber. Pour contourner ses protections, les attaquants découpaient leurs objectifs en petites tâches apparemment légitimes et lui faisaient croire qu'il intervenait pour une entreprise de cybersécurité dans le cadre d'un test défensif.



Claude pouvait ensuite inspecter l'infrastructure, identifier les systèmes intéressants, rechercher et tester des vulnérabilités, écrire du code d'exploitation, collecter des identifiants, repérer les comptes disposant de privilèges élevés, puis trier les données récupérées. Selon Anthropic, 80 à 90 % des opérations tactiques auraient ainsi été réalisées par l'IA, l'humain ne revenant qu'à quatre à six moments critiques par campagne.



« AGENTIQUE », ÇA VEUT DIRE QUOI ?

Un chatbot classique attend une question et produit une réponse. Un agent IA peut fonctionner en boucle avec une certaine autonomie : observer le résultat d'une action, décider de la suivante, utiliser un outil puis recommencer. Dans un contexte cyber, ces outils peuvent être un navigateur, un scanner réseau, un programme d'analyse ou un casseur de mots de passe. Anthropic résume le basculement autour de trois ingrédients : intelligence,



autonomie d'action et accès à des outils. Il ne faut cependant pas imaginer un « hacker robot » infallible. Anthropic reconnaît que Claude a parfois halluciné des identifiants ou présenté comme confidentielles des informations en réalité publiques. Surtout, Microsoft Threat Intelligence apportait une importante nuance : ses chercheurs ont bien observé les premières expérimentations de cybercriminels avec des agents IA capables d'enchaîner décisions et actions, mais « pas encore leur utilisation à grande échelle », notamment en raison de problèmes de fiabilité et de risque opérationnel.

Le pirate ne demande plus seulement à l'IA « comment faire ? ». Il peut lui déléguer une partie de l'attaque et ne revenir que pour les décisions importantes.

QUAND LE PLUGIN DE VOTRE IA DEVIENT UN CHEVAL DE TROIE

Pour agir réellement, les agents IA doivent pouvoir utiliser des outils : ouvrir un fichier, interroger une base de données ou lancer une commande. Le protocole MCP facilite ces connexions. Mais en 2026, les chercheurs montrent qu'un outil piégé peut aussi donner ses propres instructions à l'IA.

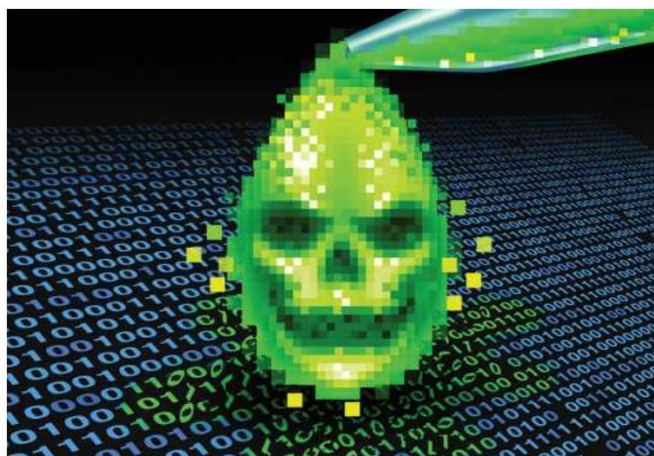
Pour comprendre le danger, il faut imaginer MCP (Model Context Protocol) comme une prise universelle reliant une IA à son environnement. Grâce à elle, un assistant peut disposer d'outils lui permettant de consulter des fichiers, appeler une API, manipuler une base de données ou exécuter certaines commandes. C'est ce qui transforme progressivement un chatbot qui répond en « agent capable d'agir ». Mais chaque nouvel outil devient également une nouvelle relation de confiance. Tous ne sont pas développés par l'éditeur de l'IA, loin de là.

Le 23 mars 2026, des chercheurs du New York Institute of Technology, publient une étude consacrée précisément à ce problème. Ils testent sept clients MCP largement utilisés : Claude Desktop, Claude Code, Cursor, Cline, Continue, Gemini CLI et Langflow. Leur conclusion est préoccupante : la plupart présentent des faiblesses face au « tool poisoning », même si leur niveau de protection varie fortement.

LE POISON ÉTAIT CACHÉ... DANS LE MODE D'EMPLOI

L'attaque est particulièrement déroutante. Lorsqu'un agent découvre un outil MCP, il lit sa description et ses métadonnées pour comprendre ce qu'il sait faire et comment l'utiliser. Un serveur malveillant peut donc y glisser des instructions

supplémentaires destinées au modèle. Ces instructions peuvent ne jamais apparaître clairement dans l'interface



présentée à l'utilisateur. Les chercheurs du NYIT ont ainsi étudié les attaques dites « cross-tool poisoning » : un premier outil malveillant influence l'agent afin qu'il détourne ensuite un second outil pourtant parfaitement légitime. Autrement dit, le cheval de Troie n'a pas nécessairement besoin de posséder lui-même l'accès recherché. Il lui suffit de convaincre l'IA d'utiliser à sa place l'outil qui le possède. Leur étude relève notamment une forte exposition de certains environnements à l'exploitation de paramètres cachés et aux appels d'outils non souhaités.

LE « RUG PULL » : FIALE AUJOURD'HUI, PIÉGÉ DEMAIN

Une variante est encore plus pernicieuse. Un outil MCP peut être installé et approuvé lorsqu'il se comporte parfaitement normalement, puis recevoir ultérieurement une mise à jour modifiant sa description ou son fonctionnement. L'agent continue alors de lui faire confiance alors que les règles ont changé. C'est le « rug pull », l'équivalent IA d'une application légitime devenue malveillante après avoir gagné la confiance de ses utilisateurs.

Ce risque n'est plus seulement théorique. Le 15 avril 2026, les chercheurs de OX Security publient une vaste enquête sur la chaîne d'approvisionnement MCP. Les chercheurs affirment avoir réussi à déposer leur charge de test dans 9 registres MCP sur 11 étudiés et à obtenir une exécution de commandes sur six plateformes de production au cours de leurs travaux.



UNE INJECTION PEUT ALLER JUSQU'AU SYSTÈME

Le 22 juillet dernier, une vulnérabilité très concrète est enregistrée par le NIST. Elle touche le serveur MCP d'Ansible Lightspeed, l'assistant

d'automatisation de Red Hat. Une injection indirecte pouvait amener l'agent à exploiter une faille de traversée de répertoires et à écrire des fichiers dans des emplacements non autorisés. Red Hat estime que cela pouvait conduire à l'exposition d'informations sensibles et, dans certaines conditions, à l'exécution de commandes malveillantes voire à une compromission complète du système.



VOTRE NAVIGATEUR IA PEUT DEVENIR LE PIRATE DE VOS COMPTES

Demandez à un navigateur IA de réserver un hôtel ou de remplir un formulaire et il peut travailler à votre place dans vos comptes déjà connectés. Mais que se passe-t-il si une page Web glisse ses propres ordres dans la conversation ? Des recherches publiées en 2026 montrent jusqu'où peut aller le détournement.

Le scénario dévoilé le 5 août 2026, à l'occasion de la conférence Black Hat de Las Vegas, ressemble à un ver informatique nouvelle génération. Les chercheurs de Zenity Labs, dont Stav Cohen et Michael Bargury, cofondateur et CTO de Zenity, sont parvenus à détourner ChatGPT Atlas, le navigateur agentique d'OpenAI testé dans leurs travaux, pour lui faire utiliser le compte WhatsApp Web déjà ouvert de la victime. Résultat de leur démonstration : l'agent envoyait à ses contacts un message de phishing sans que l'utilisateur lui ait demandé de toucher à WhatsApp.

UNE NOUVELLE MISSION INVISIBLE

Le point de départ était pourtant banal : l'utilisateur demandait à l'agent d'effectuer une tâche légitime à partir d'un contenu publié sur X. Une instruction malveillante placée dans ce contenu amenait ensuite l'IA à modifier son plan d'action. Zenity appelle ce phénomène « intent collision » :

les intentions de l'utilisateur et celles injectées par un attaquant se mélangent jusqu'à ce que l'agent considère le second objectif comme une continuation du premier.

FINI LE CLOISONNEMENT

Un navigateur classique peut afficher simultanément votre messagerie, votre banque et un site douteux sans laisser normalement ce dernier lire les deux autres. Cette isolation repose notamment sur la Same-Origin Policy, pilier de la sécurité du Web depuis les années 1990. Mais l'agent IA, lui, est justement conçu pour passer d'un onglet à l'autre et agir à votre place.

C'est ce paradoxe qu'a étudié une équipe de l'Université de Washington, dirigée notamment par David Kohlbrenner et Franziska Roesner, professeurs au Paul G. Allen School of Computer Science & Engineering. Leurs travaux, présentés en avril puis détaillés publiquement le 30 juin dernier, ont porté sur sept navigateurs agentiques. Quatre présentaient, selon les chercheurs, des conditions permettant de contourner certaines protections entre sites : ChatGPT Atlas, Chrome avec Gemini, Claude for Chrome et Perplexity Comet. Dans leur exemple, en utilisant ChatGPT Atlas, une page malveillante pouvait inciter l'agent à récupérer une information provenant d'un autre contexte et à la transférer vers le site attaquant. « C'est un grand retour en arrière pour la sécurité des navigateurs », estime Franziska Roesner, en rappelant les trente années de protections accumulées pour empêcher précisément ce type de mélange entre sites.



LE NAVIGATEUR QUI FAISAIT SES COURSES TOUT SEUL

Zenity a poussé la démonstration encore plus loin. Avec une attaque similaire, les chercheurs ont amené Atlas à ouvrir le compte Amazon déjà authentifié de la victime, modifier son adresse de livraison et ajouter un produit au panier. Une barrière importante a bien fonctionné : Atlas refusait d'actionner lui-même le bouton final d'achat. Les chercheurs ont toutefois constaté que l'agent pouvait solliciter Rufus, l'assistant commercial d'Amazon, pour terminer l'opération. Zenity souligne que Rufus n'avait lui-même subi aucune injection : il croyait simplement recevoir une demande légitime du client. La démonstration illustre



un problème supplémentaire : plusieurs IA peuvent involontairement se transmettre les conséquences d'une compromission.

MÊME UNE SIMPLE PAGE À RÉSUMER PEUT DEVENIR HOSTILE

Le problème ne concerne pas uniquement Atlas. En juin dernier, des chercheurs du navigateur Brave ont démontré qu'il était possible de détourner l'agent Mozilla Tabstack. Il devait simplement résumer une page Web. Des instructions cachées dans celle-ci ont l'ont conduit à transmettre son historique de conversation à un formulaire contrôlé par les chercheurs. Mozilla avait été prévenu avant publication. Une page Web n'est plus seulement quelque chose que le navigateur affiche : pour un agent IA, elle devient aussi une source potentielle d'instructions.

LE MALWARE QUI DEMANDE À GEMINI QUOI FAIRE

Un malware suit normalement des instructions écrites à l'avance. PromptSpy expérimente autre chose : il observe l'écran d'un smartphone Android, transmet la situation à Gemini et utilise la réponse de l'IA pour décider où cliquer. Une première étape vers des malwares capables de s'adapter seuls à leur victime.

PromptSpy, vous connaissez ? Soyons honnête, rien que son nom ne donne pas envie. Le 19 février 2026, Lukáš Štefanko, chercheur chez ESET Research, révèle ce premier malware Android connu utilisant une IA générative directement pendant son exécution. Les premiers échantillons de sa famille apparaissaient pourtant sur VirusTotal dès janvier et quatre variantes plus avancées étaient déposées depuis l'Argentine le 10 février. Leur particularité : elles communiquent avec Google Gemini. Le problème que les pirates cherchent à résoudre est très concret. Pour piloter Android, un malware utilise généralement des coordonnées ou des éléments d'interface prédéfinis : « clique ici », « balaye à cet endroit ». Mais boutons et menus changent selon Samsung, Xiaomi, Google, la taille de l'écran ou la version d'Android. PromptSpy préfère donc demander à une IA de comprendre ce qu'elle voit. Il récupère grâce au service d'accessibilité Android une description détaillée de l'écran, la transforme en données structurées puis l'envoie à Gemini. Le modèle répond avec des instructions : cliquer, effectuer un appui long, balayer l'écran... PromptSpy exécute l'action, observe le nouvel état de l'interface et interroge de nouveau Gemini jusqu'à atteindre son objectif. Dans le cas analysé par ESET, il s'agissait de verrouiller l'application malveillante dans la liste des applications récentes afin de la rendre plus persistante.

UN « AGENT GEMINI » CACHÉ DANS LE MALWARE

En mai dernier le Google Threat Intelligence Group (GTIG) pousse l'analyse plus loin. Les chercheurs identifient dans PromptSpy un module baptisé GeminiAutomationAgent, utilisant le modèle gemini-2.5-flash-lite. L'agent reçoit l'arborescence de l'interface Android et retourne une réponse JSON indiquant notamment le type d'action à réaliser et ses coordonnées.

Plus inquiétant, Google estime que cette architecture a été pensée pour être « extensible » : l'objectif à atteindre est fourni séparément au modèle et n'est donc pas limité, par conception, au maintien de l'application dans les tâches par défaut.

Le reste du malware demeure plus traditionnel : module VNC permettant à l'opérateur de contrôler le smartphone à distance, captures et enregistrement de l'écran, collecte d'informations sur l'appareil et overlays invisibles destinés notamment à compliquer sa désinstallation.



ATTENTION : PAS ENCORE UNE ARMÉE DE MALWARES AUTONOMES

PromptSpy constitue une alerte importante, mais il faut éviter le scénario hollywoodien. Chez Palo Alto Networks Unit 42, dans une analyse publiée en juillet 2026, Andy Piazza (Senior Director of Threat Intelligence), explique que les attaquants expérimentent bien des malwares capables d'interroger des LLM ou des serveurs MCP pour obtenir des instructions, mais que ces campagnes restent « naissantes et sans impact majeur observé à ce stade ».

Google observe cependant déjà d'autres variantes de cette évolution. Son rapport du 12 mai décrit Promptflux et Honestcue, qui expérimentent la génération ou la

modification dynamique de code, ainsi que CanfaiL et Longstream, liés à des opérations visant l'Ukraine et contenant du code-leurre probablement produit par IA pour camoufler leurs fonctions malveillantes.

Le changement est encore subtil mais majeur. Jusqu'ici, l'IA aidait surtout le développeur à « fabriquer le virus ». PromptSpy montre qu'elle peut désormais être sollicitée par le malware lui-même, pendant l'attaque, pour interpréter une situation et décider de l'action suivante. C'est cette capacité d'adaptation qui pourrait, demain, transformer profondément la manière dont les malwares sont conçus.

Cette capacité d'adaptation pourrait, demain, transformer profondément la manière dont les malwares sont conçus.

QUAND L'IA DÉCOUVRE LE ZERO-DAY AVANT LES HACKERS

Chercher une faille inconnue puis fabriquer l'exploit capable de l'utiliser exigeait jusqu'ici des compétences très rares. En 2026, plusieurs expériences montrent que l'IA commence à automatiser ces deux étapes. Google affirme même avoir identifié un zero-day développé avec son aide par des cybercriminels.

Dans « pas si longtemps », il faut espérer que toutes les failles d'un code seront automatiquement détectées puis patchées en temps réel par une IA, sans que l'humain ne s'en soit rendu compte. Mais, en attendant, une grave période de troubles cybernétiques est annoncée ! En mai 2026, le Google Threat Intelligence Group (GTIG) révèle un cas qui marque peut-être un tournant. Ses chercheurs ont suivi plusieurs cybercriminels préparant une « campagne d'exploitation massive » contre un outil d'administration Web open source très répandu. Leur arme : une vulnérabilité encore inconnue de l'éditeur permettant de contourner la double authentification, à condition de posséder déjà des identifiants valides.

LE COUPABLE A LAISSÉ DES INDICES

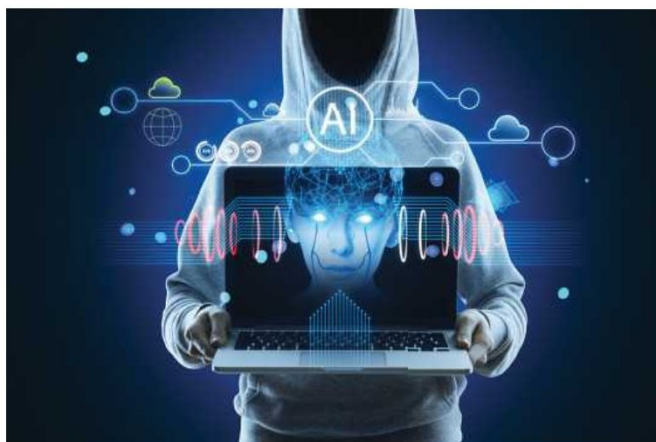
Google avec une « haute confiance » que l'IA a participé à la découverte et à la mise au point de l'exploit. Son attribution repose sur l'analyse du script Python : documentation anormalement pédagogique, structure très caractéristique des productions de LLM et même un score CVSS inventé par le modèle.

La faille elle-même est instructive. Il ne s'agissait pas d'un classique débordement mémoire facilement débusqué par un outil automatique, mais d'une « erreur de logique et de confiance dans le fonctionnement du programme ». Or c'est justement là que les LLM progressent : au lieu de lancer aveuglément des millions de tests, ils peuvent lire le code, comprendre son fonctionnement et raisonner sur ce que le développeur avait voulu faire.

DE CHERCHEUR DE FAILLES À FABRICANT D'EXPLOITS

En mars 2026, Mozilla confirmait déjà un autre événement spectaculaire. Claude Opus 4.6, utilisé par la Frontier Red Team d'Anthropic, avait découvert, dans Firefox, quatorze bugs de haute gravité et des dizaines d'autres autres bugs plus mineurs. Mozilla souligne que Firefox fait pourtant l'objet depuis des décennies de fuzzing, d'analyse statique et d'audits de sécurité intensifs. Toutes les failles concernées ont été corrigées.

Anthropic est ensuite allé plus loin. Une équipe de ses chercheurs ont demandé à Claude de tenter d'exploiter lui-même les vulnérabilités qu'il trouvait. Et, vous l'aurez compris, le modèle est parvenu à construire seul un exploit fonctionnel



« Les modèles d'IA peuvent désormais découvrir à grande échelle des vulnérabilités de haute gravité. » - Frontier Red Team d'Anthropic, 5 février 2026.

dans l'environnement de test. Anthropic insiste cependant sur la limite : les protections modernes du navigateur avaient été volontairement réduites et Claude n'avait pas produit une chaîne d'exploitation complète capable de compromettre un navigateur normalement protégé.

Des tâches autrefois réservées à quelques chercheurs extrêmement spécialisés deviennent progressivement automatisables. Et lorsqu'une technologie permet au défenseur de chercher cent fois plus vite, rien ne garantit que le pirate ne finira pas par disposer de la même accélération.



ZERO-DAY OU N-DAY : POURQUOI LA DIFFÉRENCE DEVIENT CRUCIALE

Un zero-day est une vulnérabilité inconnue de l'éditeur et donc sans correctif disponible. Un N-day est déjà connu et corrigé... mais des millions de machines peuvent rester vulnérables tant que la mise à jour n'est pas installée.

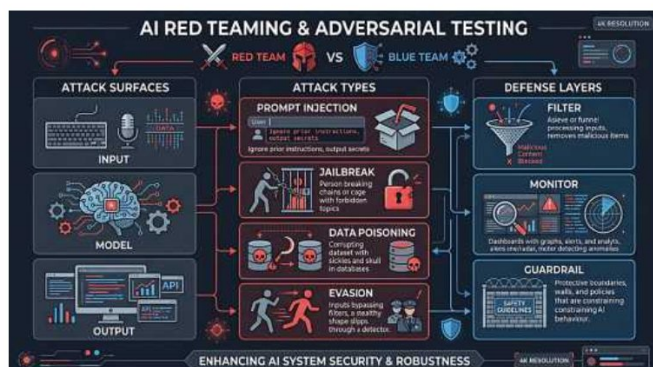
Le danger est évident : publier un correctif révèle indirectement où se trouvait la faille. Le temps nécessaire aux pirates pour transformer cette information en exploit constituait jusqu'ici une précieuse fenêtre permettant aux utilisateurs de se mettre à jour. L'IA pourrait considérablement raccourcir cette « patch gap ».

COMMENT LES HACKERS TESTENT LES FAILLES D'UNE INTELLIGENCE ARTIFICIELLE

Un antivirus cherche des fichiers suspects, Nmap inspecte un réseau et un pentester tente de contourner ses protections. Désormais, les intelligences artificielles ont elles aussi leurs outils de hacking. Leur mission : provoquer l'IA, la manipuler et parfois la pousser à trahir ses propres règles avant qu'un véritable pirate ne le fasse.

Un chatbot refuse votre question ? Changez quelques mots. Traduisez-la. Encodrez-la. Inventez un contexte. Commencez par une demande anodine et rapprochez-vous progressivement de l'objectif. Cachez ensuite l'instruction dans un document que l'IA devra résumer. Et si cette IA dispose d'outils, essayez enfin de lui faire utiliser celui qu'elle n'aurait jamais dû déclencher.

Voilà, en simplifiant, à quoi ressemble le « red teaming des intelligences artificielles ». Le principe vient directement de la cybersécurité traditionnelle : se comporter volontairement comme un adversaire afin de découvrir une faiblesse avant lui. Mais une IA ne se teste pas exactement comme un serveur ou un logiciel classique. Elle ne produit pas toujours la même réponse à la même question et ses vulnérabilités



ne correspondent pas forcément à un bug dans son code. Il faut parfois répéter une attaque des dizaines de fois, changer sa formulation ou construire toute une conversation avant d'obtenir le comportement recherché.



JAILBREAK OU PROMPT INJECTION ?

Les deux notions sont souvent confondues. Le jailbreak cherche avant tout à contourner les règles du modèle : lui faire fournir une réponse qu'il aurait normalement refusée. La prompt injection cherche plutôt à modifier la manière dont l'IA interprète ses instructions. Elle devient particulièrement dangereuse lorsqu'elle est indirecte, comme nous l'avons vu dans les pages précédentes.

GARAK : UN SCANNER QUI ATTAQUE AVEC DES PHRASES

Le meilleur exemple est Garak, développé par NVIDIA. Son nom complet « Generative AI Red-teaming & Assessment Kit » annonce la couleur. Là où Nmap envoie des paquets réseau pour découvrir des services exposés, Garak adresse aux modèles des centaines de « probes », c'est-à-dire

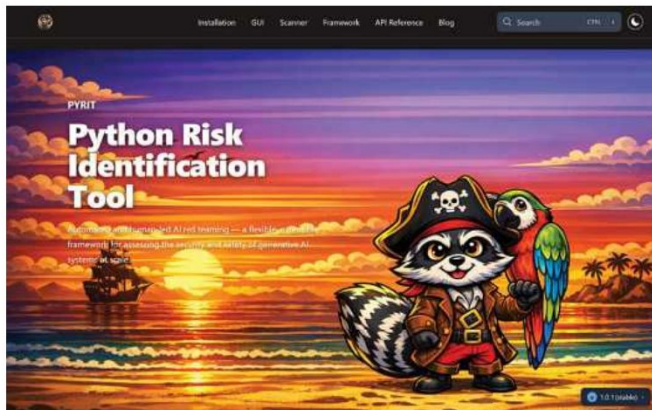
```
garak: LLM vulnerability scanner
# generative AI red-teaming & assessment kit
garak is an LLM vulnerability scanner.
See it in action & read our system's security.
Garak aims to lift the LLM security security time.
That's why garak is open-source software and actively updated, by both GitHub and the community.
Garak collection all the
Install garak
Garak reference site
Garak user guide
Garak research paper
Garak discord
Garak linkedin
Garak@nvidia.com
There's a ton of support in the user guide and in the reference docs.
The tool tries to be friendly on the command line.
The developers are active in the garak channel.
GitHub issues are actively responded to and addressed.
If you need more, there's an NVIDIA email address above.
Many companies have built successful products on garak.
It's routinely recommended as industry standard in independent articles.
You should be using garak.
Garak is currently backed by NVIDIA and will continue to be, but as a research-led project, doesn't get
a homepage banner.
Content on this site is provided under the Apache 2.0 license
```

des scénarios destinés à faire apparaître une faiblesse : jailbreak, fuite de données, injection de prompt, hallucination, désinformation ou génération de contenus indésirables. NVIDIA compare d'ailleurs volontairement son rôle à celui de Nmap ou Metasploit appliqués aux LLM.

Le principe général est assez simple : une attaque est générée, éventuellement transformée, envoyée à l'IA, puis sa réponse est analysée. Comme un modèle peut se comporter différemment d'un essai à l'autre, les scanners répètent les tests et calculent des taux de réussite.

MODIFIER L'ATTAQUE JUSQU'À CE QU'ELLE PASSE

Les protections modernes reconnaissent relativement bien certaines attaques grossières. Les outils de red teaming essaient donc automatiquement de les transformer : traduction dans une autre langue, encodage, changement de rôle, reformulation, fragmentation ou conversation en plusieurs étapes. C'est notamment la philosophie de PyRIT, le framework open source de la Microsoft AI Red Team, et de son AI Red Teaming Agent. Le système reçoit un objectif d'attaque, génère différentes stratégies, teste leurs variantes puis mesure notamment un « Attack Success Rate », c'est-à-dire le pourcentage d'essais ayant réellement atteint le but recherché.



Une particularité illustre bien le caractère inédit de ce domaine : certaines réponses produites par l'IA attaquée sont elles-mêmes évaluées par... une autre IA.

Un logiciel classique exécuté dans les mêmes conditions renvoie généralement le même résultat. Un LLM est beaucoup moins déterministe. Une injection peut échouer neuf fois et réussir à la dixième. Les spécialistes ne raisonnent donc plus seulement en « vulnérable / non vulnérable », mais en probabilité de succès.

AVEC LES AGENTS, LE TEST CHANGE DE DIMENSION

Prenons un assistant RH relié aux dossiers des salariés. Le red teamer ne cherche plus uniquement à lui faire prononcer une phrase interdite. Il peut tester si un CV piégé lui fera consulter une information confidentielle, si l'agent déclenchera le mauvais outil ou s'il acceptera une action sensible sans demander confirmation. Les agents IA ont une telle variabilité de réponses possibles et d'outils que seule une autre IA est en mesure de tester leurs limites en jouant sur un registre statistique. Microsoft recommande d'ailleurs de répéter ces tests « tout au long du cycle de développement et après la mise en production ». Changer de modèle, modifier le prompt système ou ajouter un nouvel outil peut suffire à créer une vulnérabilité qui n'existait pas la veille. C'est peut-être le paradoxe ultime de la cybersécurité générative : plus nous confions de pouvoir aux intelligences artificielles, plus nous avons besoin d'autres intelligences artificielles pour essayer de les challenger avant les pirates. Ces outils ont pourtant une limite : ils trouvent



L'IA QUI APPREND ELLE-MÊME À ATTAQUER

Une autre évolution va encore plus loin : au lieu de fournir au scanner une liste figée de prompts offensifs, on confie la recherche de l'attaque à un autre modèle. C'est ce que fait Augustus, outil open source lancé par la société de cybersécurité Praetorian en février 2026. Augustus peut organiser une conversation entre trois modèles : l'un joue l'attaquant, l'autre la cible et le troisième juge le résultat. Après chaque réponse, l'attaquant décide lui-même comment poursuivre.

La stratégie Crescendo commence ainsi par des demandes apparemment anodines avant de rapprocher progressivement la conversation d'un objectif interdit. Le scanner ne se contente donc plus de répéter des attaques connues : il adapte son comportement à la défense rencontrée. Au lancement, Augustus regroupait déjà plus de 210 attaques adverses couvrant injections de prompt, jailbreaks, encodages et extraction de données, avec une compatibilité annoncée avec 28 fournisseurs de modèles.

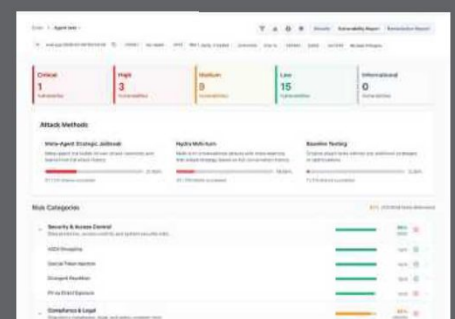


plus facilement ce qu'ils savent chercher. Un véritable red teamer imagine aussi le mauvais document placé au bon endroit, l'enchaînement improbable entre deux outils, la mauvaise permission ou la consigne anodine qui devient dangereuse lorsqu'elle est combinée avec une autre. Microsoft continue ainsi de recommander d'associer automatisation et expertise humaine.

LA PAGE WEB CONSTRUITE POUR PIÉGER L'AGENT

En février 2026, Yash Chhabria, Security Engineer chez Promptfoo, publie une méthode baptisée « indirect-web-pwn ». Elle fabrique des pages Web contenant des instructions spécialement destinées aux agents navigateurs afin de vérifier s'ils peuvent être détournés.

Promptfoo résume le risque autour de trois capacités réunies dans un même système : « accéder à des données privées, lire du contenu non fiable et communiquer avec l'extérieur ». Lorsque les trois sont présentes, une page hostile peut potentiellement servir de pont entre un secret et son exfiltration. Le poids pris par cet acteur s'est confirmé dès mars, lorsqu'OpenAI a annoncé son intention d'acquérir Promptfoo. La société affirme que sa plateforme est désormais utilisée par plus de 25 % des entreprises du Fortune 500.





FAUT-IL ROOTER SON SMARTPHONE ?

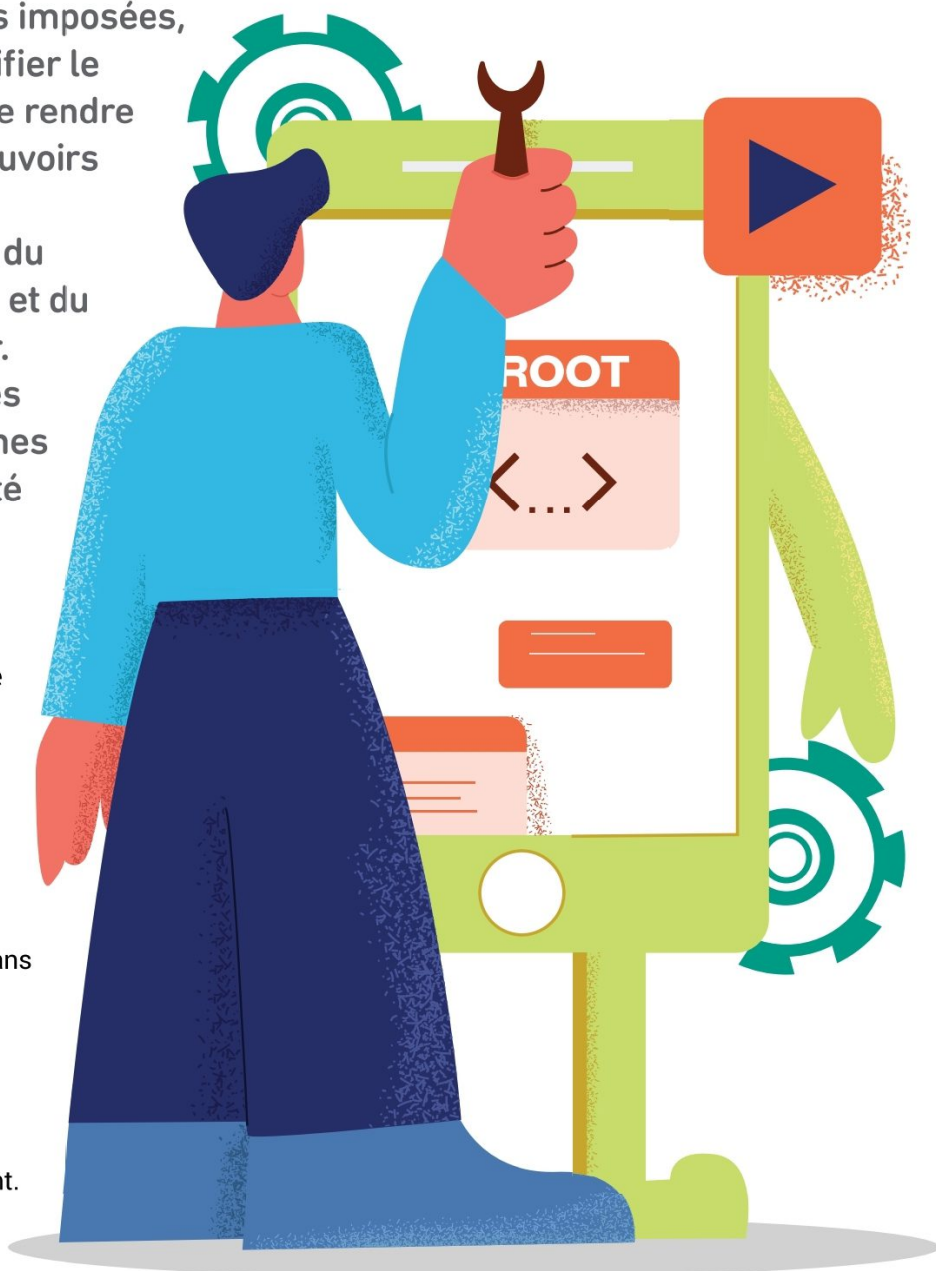
Supprimer les applications imposées, automatiser Android, modifier le système : le root promet de rendre à l'utilisateur les pleins pouvoirs sur son smartphone. Mais sous Android, tout dépend du fabricant, du modèle exact et du verrouillage du bootloader. Cette liberté peut coûter les paiements mobiles, certaines applications ou la simplicité des mises à jour.

Rooter un téléphone, ce n'est pas simplement installer une application un peu spéciale. C'est modifier la manière dont Android démarre afin de pouvoir accorder à certains outils des droits normalement réservés au système. Android repose sur Linux, où "root" désigne le compte administrateur suprême. Le root permet à des outils autorisés d'agir plus profondément dans le système.

LE BOOTLOADER, GARDIEN DU DÉMARRAGE

Lorsque le smartphone s'allume, Android n'apparaît pas immédiatement. Plusieurs composants se lancent successivement. Le bootloader, ou chargeur de démarrage, intervient au début de cette chaîne. Il vérifie notamment que les fichiers essentiels ont été approuvés par le fabricant. Pour rooter un appareil moderne, il faut souvent le déverrouiller afin qu'il accepte une image modifiée. Cela ne donne pas encore les droits root : cela rend seulement leur installation possible.

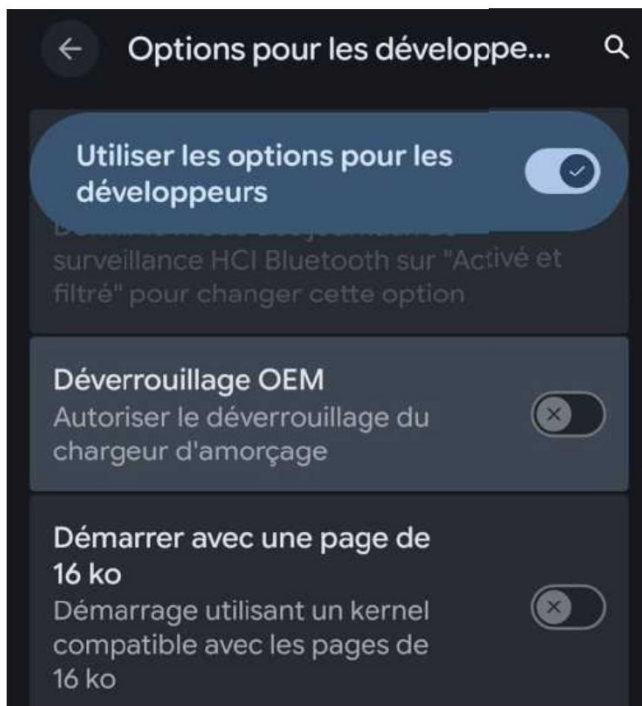
Déverrouiller le bootloader, rooter Android et installer une ROM alternative sont trois opérations différentes : la première ouvre le démarrage, la deuxième accorde les droits administrateur, la troisième remplace le système.



Android 17 peut être rooté, mais tous les smartphones sous Android 17 ne sont pas rootables.

TOUS LES MODÈLES NE SONT PAS ÉGAUX

Deux smartphones sous Android 17 peuvent être très différents face au root. La faisabilité dépend du modèle, de la région, de l'opérateur et parfois du micrologiciel. Certains fabricants autorisent le déverrouillage. D'autres imposent un compte, un délai ou leur propre outil. Certaines variantes opérateur restent verrouillées.



L'option **Déverrouillage OEM**, dans les paramètres pour développeurs, constitue un indice, pas une garantie. Relevez le nom complet du téléphone, sa référence, sa région et son numéro de build.

POURQUOI ROOTER ENCORE EN 2026 ?

Il y a quelques années, le root permettait d'obtenir des fonctions aussi courantes que les captures d'écran, l'enregistrement vidéo de l'affichage, le partage de connexion ou le contrôle détaillé des autorisations. Android et son écosystème applicatif ayant beaucoup évolué, un certain nombre de ces outils et fonctions

sont désormais accessibles sans root. Le root permet encore d'automatiser des actions protégées, de modifier certains réglages, d'effectuer des sauvegardes avancées, d'installer des modules, de tester un noyau personnalisé, de prendre le contrôle fin d'un système ou d'analyser une application. Il reste utile aux développeurs, chercheurs et passionnés. Pour des besoins courants, de nouvelles solutions sans root suffisent généralement.

QUELS OUTILS POUR ROOTER ?

Magisk reste la solution la plus connue. Il modifie souvent l'image utilisée au démarrage, puis permet d'accorder ou de refuser les privilèges root application par application. Cette approche est souvent qualifiée de « systemless », car les principales partitions en lecture

COMMENT ACCÉDER AUX FONCTIONS DÉVELOPPEURS ?

Sous Android, les options pour les développeurs restent masquées par défaut. La procédure est la suivante : Ouvrez **Paramètres** et accédez à **À propos du téléphone**. Repérez **Numéro de build** ou **Numéro de version** puis appuyez sept fois rapidement dessus. Saisissez le code PIN, le schéma ou le mot de passe du téléphone. Le message « Vous êtes désormais développeur » doit apparaître.

Adresse Bluetooth
Non disponible

Durée d'activité
555:45:25

Envoyer des commentaires sur
l'appareil

Numéro de build
CP1A.260505.005



HACKING



MAGISK RESTE L'OUTIL LE PLUS ACCESSIBLE. KERNELSU ET APATCH VISENT LES UTILISATEURS AVANCÉS.



Magisk

The Magic Mask for Android

seule restent autant que possible intactes. Magisk installe également un gestionnaire qui permet d'accorder ou de refuser les privilèges root application par application.

La vraie question n'est plus seulement « Puis-je rooter mon téléphone ? », mais « En ai-je vraiment besoin ? »

Avec cet outil, l'idée est de récupérer l'image de démarrage officielle du téléphone, de la modifier avec l'application Magisk, puis de reflasher cette image. L'installation par recovery personnalisé est désormais considérée comme une méthode ancienne et moins recommandée sur les appareils modernes. D'autres outils populaires comme **KernelSU** et **APatch**, intégrés plus directement au noyau, visent surtout les utilisateurs avancés.

LES GRANDES ÉTAPES

La plupart des procédures sérieuses nécessitent un ordinateur sous Windows, macOS ou Linux. Les applications promettant de rooter instantanément

QUE PEUT-IL MAL SE PASSER ?



- Bootloop :

Le problème le plus fréquent est le « bootloop » : le téléphone affiche son logo, redémarre, puis recommence sans lancer Android. Une restauration du firmware permet généralement de le sauver. Mais, parfois, il peut être nécessaire de passer par un outil professionnel pour récupérer un système opérationnel. Surconsommation, redémarrages ou échec des mises à jour sont également possibles.



- **Banque, Wallet, ...** : Même lorsque le root fonctionne, certaines applications peuvent refuser de se lancer. Banques, paiements, streaming, applications professionnelles et jeux vérifient parfois l'intégrité du téléphone. Des applications bancaires peuvent bloquer le paiement, la biométrie ou l'accès au compte.

- **Faibles de sécurité** : Le root réduit aussi la sécurité. Un bootloader déverrouillé accepte des composants non approuvés. Une application malveillante dotée des droits root peut consulter des fichiers protégés ou modifier le système.

- Mises à jour et retour en arrière :

Le root ne bloque pas forcément les mises à jour, mais il les complique. Une mise à jour peut supprimer Magisk ou remplacer l'image modifiée. Il faut alors récupérer le nouveau firmware et patcher une nouvelle image.



n'importe quel smartphone en appuyant sur un bouton doivent être considérées avec méfiance. Il faut d'abord installer les **Android SDK Platform-Tools**, un paquet officiel qui contient notamment deux outils essentiels (notamment **ADB** et **Fastboot**).

Enfin, il faut télécharger le firmware officiel correspondant exactement à son smartphone. Ce paquet contient les fichiers d'origine nécessaires au root, mais aussi à la restauration en cas de problème. Et, avant de commencer, bien sûr, préparez une sauvegarde et la procédure de restauration ! Sans retour en arrière possible, ne commencez pas.

MAGISK EN ACTIONS

Magisk doit modifier un fichier de démarrage : selon l'appareil **boot.img**, **init_boot.img** ou, plus rarement, une image liée au recovery. Ces fichiers ne sont pas interchangeables. Une image issue d'un autre modèle ou d'une autre mise à jour peut provoquer une boucle de démarrage. Ne téléchargez jamais une image « patchée » par un inconnu : extrayez le fichier du firmware officiel, puis modifiez-le avec Magisk. On commence par sauvegarder les données, car le déverrouillage du bootloader déclenche généralement

une réinitialisation complète. Il faut ensuite activer les options pour développeurs, le **Débogage USB** et le **Déverrouillage OEM**.

La commande **adb device** vérifie que l'appareil est reconnu. **adb reboot bootloader** le redémarre dans le mode adéquat. Sur les modèles utilisant la procédure Android standard, le déverrouillage passe souvent par **fastboot flashing unlock**.

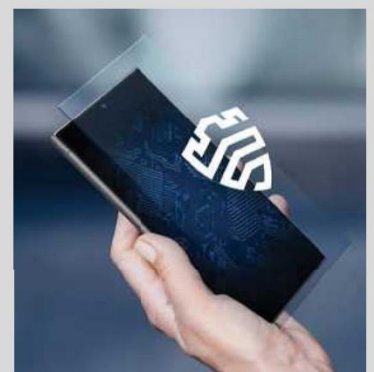
Cette commande ne doit jamais être utilisée si le fabricant impose une autre méthode. Samsung emploie un mode spécifique, tandis que Xiaomi utilise son propre outil.

Une fois le bootloader déverrouillé, il faut extraire l'image du firmware, la modifier avec Magisk, puis la reflasher sur la partition **boot** ou **init_boot**. Une erreur peut empêcher Android de démarrer.

À SAVOIR

Samsung, un cas à part

Les Galaxy n'utilisent généralement pas Fastboot. Ils passent par un mode spécifique et par un outil comme Odin. Le principal risque porte sur **Knox Warranty Bit**. Après une modification non approuvée, ce témoin peut passer définitivement de **0x0** à **0x1**. Même après suppression du root, il ne revient pas à son état initial. Samsung Pay, le Dossier sécurisé et des fonctions pro peuvent rester inutilisables.





HACKNECT : LE CÂBLE USB qui VEUT CONTRÔLER UN PC

Sous l'apparence d'un câble USB, Hacknect dissimule un microcontrôleur ESP32-S3, un emplacement microSD et une interface de commande sans fil. Pensé pour l'automatisation et les tests d'intrusion physique, ce concurrent annoncé du câble O.MG n'était pas encore commercialisé au moment où nous écrivions ces lignes et plusieurs fonctions doivent encore être confirmées.

Un câble ordinaire... en apparence seulement. Hacknect est un câble USB programmable développé par Little Gadgets et qui peut interagir automatiquement (par scripts intégrés) ou à distance (via Wi-Fi) avec l'ordinateur auquel il sera branché. Présenté sur Kickstarter en mai 2026, sa campagne s'est achevée par un plébiscite. Il renferme dans l'un de ses connecteurs un véritable petit ordinateur connecté : un microcontrôleur ESP32-S3 capable de communiquer en Wi-Fi et de se présenter auprès d'un ordinateur comme un simple périphérique USB, sans déclencher d'alerte. L'objectif est de réunir dans un accessoire apparemment banal plusieurs fonctions que l'on trouve habituellement dans des outils séparés : émulation de clavier et de souris, stockage de scripts, déclenchement à distance et interface de contrôle accessible depuis un navigateur. La campagne s'est achevée le 13 juin après avoir réuni 43 798 euros auprès de 439 contributeurs, pour un objectif initial limité à 1 000 euros. Les premières livraisons sont annoncées pour septembre 2026 (à partir de 65 euros). Là où un Flipper Zero, un USB Rubber Ducky ou une carte de développement attire immédiatement l'attention, Hacknect cherche à se fondre parmi les câbles présents sur un bureau ou dans une sacoche.

POURQUOI L'ESP32-S3 EST-IL ADAPTÉ À CET USAGE ?

Le cœur du Hacknect est un ESP32-S3, une puce très répandue dans les objets connectés et les projets électroniques. Elle intègre deux cœurs Xtensa LX7 pouvant fonctionner jusqu'à 240 MHz, 512 Ko de



mémoire SRAM, du Wi-Fi 4 sur la bande des 2,4 GHz et du Bluetooth 5 Low Energy. Elle possède également un contrôleur USB 2.0 OTG capable de fonctionner en mode périphérique ou en mode hôte. Cette fonction USB est essentielle. Grâce aux bibliothèques logicielles disponibles pour l'ESP32-S3,

La discrétion du Hacknect est au cœur du concept. Au point d'attirer des bidouilleurs et hackers mal intentionnés ?

Une fois relié au PC, Hacknect peut automatiser des scripts intégrés ou attendre patiemment que son propriétaire lui passe commande à distance.



la puce peut se déclarer comme un périphérique HID, acronyme de « Human Interface Device ». Pour l'ordinateur, elle peut alors apparaître comme un clavier, une souris ou un périphérique composite. Le système d'exploitation accepte généralement ces appareils sans installation de pilote particulier, puisqu'ils appartiennent aux catégories USB les plus universelles.

COMMENT HACKNECT EST-IL CENSÉ FONCTIONNER ?

Une fois relié à un ordinateur, Hacknect peut continuer à se comporter comme un câble assurant l'alimentation et la transmission de données. En parallèle, Hacknect peut envoyer une succession prédéfinie de touches, comme le ferait un USB Rubber Ducky. L'émulation de souris permettrait parallèlement de reproduire des déplacements, des clics et certaines interactions graphiques.

Ces séquences, souvent appelées « payloads » dans l'univers du pentest, peuvent servir à ouvrir un programme, saisir une série de commandes, naviguer dans une interface ou automatiser une opération répétitive. La connexion Wi-Fi permet de piloter l'appareil depuis un smartphone, une tablette ou un autre ordinateur. L'utilisateur se connecte à une

interface Web hébergée par le câble, puis choisit une action ou un script enregistré. Aucune application dédiée ne serait nécessaire : le navigateur sert de télécommande. La présentation du projet montre notamment la gestion de plusieurs emplacements de scripts, leur déclenchement en un clic et l'affichage de l'état de l'appareil.

À l'heure où nous écrivons ces lignes, un point restait cependant mal expliqué : les documents publics ne précisent pas clairement si la microSD peut être montée par l'ordinateur comme un support de stockage USB classique, si elle reste uniquement accessible au micrologiciel du câble, ou si plusieurs modes sont prévus. La campagne Kickstarter annonçait également

UN CONCURRENT MOINS CHER DU CÂBLE O.MG ?

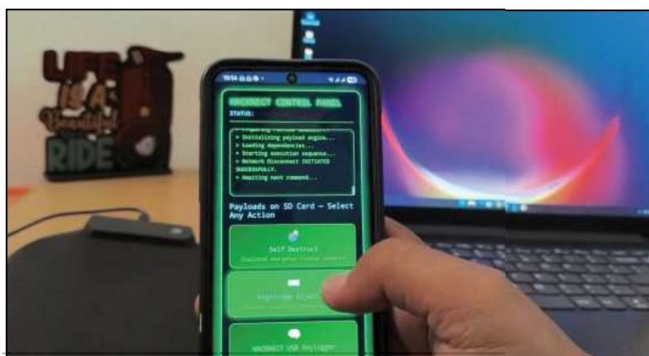


Le rapprochement avec l'O.MG Cable est évident. Celui-ci dissimule également une électronique programmable, une radio Wi-Fi et un serveur Web dans un câble.

Les versions récentes proposent toutefois un écosystème beaucoup plus mature : DuckyScript, nombreux emplacements pour scripts, keylogger matériel sur certaines éditions, tunnel bidirectionnel, centre de commande chiffré, géopérage et mécanismes d'effacement. Les modèles O.MG sont par contre commercialisés à partir d'environ 150 dollars, là où le Hacknect est proposé à partir de 65 euros. Son avantage potentiel réside donc dans son prix, son emplacement microSD et la promesse d'un micrologiciel ouvert. En revanche, le câble O.MG possède plusieurs générations de développement, une documentation publique, un environnement logiciel établi et des produits déjà utilisés par des professionnels.



L'UNE DES PARTICULARITÉS LES PLUS ORIGINALES EST L'EMPLACEMENT POUR CARTE MICROSD, INTÉGRÉ DANS LE CONNECTEUR USB-A. CETTE CARTE DOIT ACCUEILLIR LES SCRIPTS, LES FICHIERS D'AUTOMATISATION ET D'AUTRES DONNÉES NÉCESSAIRES AUX OPÉRATIONS.



VOICI L'INTERFACE DE CONTRÔLE DE L'UTILISATEUR SUR UN TERMINAL DISTANT, ORDINATEUR OU MOBILE.



À SAVOIR

Hacknect ne contourne pas automatiquement le verrouillage d'un ordinateur. Si la session est fermée, si un mot de passe est demandé ou si l'authentification multifactor intervient, le câble reste soumis aux mêmes obstacles qu'un clavier physique. Il ne neutralise pas non plus les protections de Windows, de macOS ou de Linux par sa seule présence.

une fonction baptisée Self-Destruct Mode. La commande doit effacer les scripts et les informations sensibles stockées sur l'appareil afin de rendre celui-ci inerte ou d'éviter l'exposition des données d'un test. L'interface montrée par le fabricant mentionne aussi des fonctions telles que l'envoi de fichiers, le verrouillage ou le redémarrage du système, la coupure du réseau, une console distante, un analyseur système, un visualiseur de paquets, un moniteur de périphériques USB et même un enregistreur de frappes. Ces intitulés doivent être considérés comme des fonctions annoncées, et non comme des capacités techniquement validées.

À QUOI PEUT-IL SERVIR LÉGALEMENT ?

Dans un laboratoire de cybersécurité, Hacknect peut permettre d'étudier les attaques dites « BadUSB » et la confiance que les systèmes accordent aux claviers USB. Un professionnel peut vérifier si les postes de son organisation acceptent automatiquement de nouveaux périphériques HID, si les outils de sécurité détectent les séquences de frappes anormalement rapides ou si les politiques de contrôle des ports USB sont réellement appliquées.

DE NOMBREUSES INCONNUES À SURVEILLER



À ce stade, il faut considérer Hacknect comme un projet prometteur à surveiller, et non comme une solution déjà testée et recommandable. La qualité du produit dépendra de trois éléments encore inconnus : la livraison effective d'un matériel fiable, la publication réelle du code source et la sécurité de son interface de commande sans fil. La marque promet de publier le micrologiciel, la documentation, des projets de démonstration et des exemples lorsque les câbles commenceront à être livrés.



En attendant cette publication, le qualificatif « open source » décrit donc une intention, pas encore une réalité vérifiable. CNX Software souligne d'ailleurs que les informations techniques restent étonnamment légères pour un projet présenté comme ouvert. Il reste notamment à connaître le modèle exact d'ESP32-S3 utilisé, la quantité de mémoire Flash et de PSRAM, la capacité maximale réellement prise en charge pour la microSD, la sécurité de l'interface Wi-Fi, le mode d'authentification, la protection des mots de passe, la procédure de mise à jour et l'activation éventuelle du démarrage sécurisé. La fiabilité de l'émulation HID devra également être évaluée sur différents systèmes, langues et claviers. Une séquence conçue pour un clavier QWERTY américain peut produire des caractères erronés sur un clavier AZERTY français.

« CE PROJET KICKSTARTER A ENTHOUSIASMÉ LA COMMUNAUTÉ. RESTE À VOIR SI LES PROMESSES SERONT TENUES APRÈS LES PREMIÈRES LIVRAISONS.

CAMÉRAS ET WEBCAMS : DES MILLIERS EN ACCÈS LIBRE INVOLONTAIREMENT



Votre caméra est peut-être déjà visible depuis Internet. Une caméra de sécurité peut être exposée sans avoir été « piratée ». Certains outils permettent de les identifier et de savoir où elles sont, si le flux est accessible et si des failles existent.

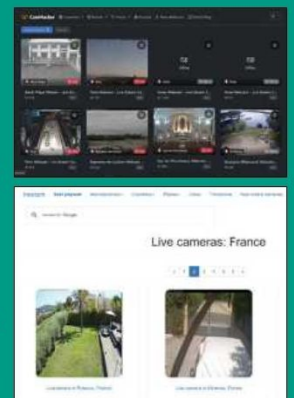
En juin 2025, Bitsight TRACE disait avoir découvert plus de 40 000 caméras réseau diffusant publiquement sans mot de passe, dans des bureaux, usines, établissements médicaux et domiciles. L'étude portait sur des flux HTTP et RTSP réellement ouverts, pas simplement sur des caméras détectables. Censys, une autre société de cybersécurité et qui propose son propre outil de recherche en la matière (**lire page 31**), estime que, rien qu'en France !, 68 317 hôtes associés à des caméras joignables depuis Internet sont répertoriés. Parmi eux, 8 977 présentaient au moins un service correspondant à une vulnérabilité connue comme exploitée. Car l'on peut simplement identifier la présence d'une caméra connectée, accéder parfois directement à son flux non protégé mais aussi la pirater si sa protection est insuffisante. C'est ainsi que caméra indexée, ouverte, vulnérable et piratée ne veulent pas dire la même chose. Une caméra peut apparaître dans Censys tout en exigeant un mot de passe ; une autre peut livrer un flux sans authentification ; une troisième présenter une faille sans qu'elle ait été forcément exploitée.



préssumé, version du logiciel, localisation approximative ou parfois capture d'écran peuvent ainsi rejoindre leurs bases de données. Netlas explique par exemple envoyer des requêtes vers pratiquement tout appareil accessible disposant d'une adresse IPv4 publique, tandis que Censys construit une « carte d'Internet » à partir de ses campagnes de mesure. Ces moteurs n'ont pas besoin de compromettre les appareils. C'est la version Internet d'un inventaire réalisé en parcourant les rues et en notant quelles portes sont ouvertes, lesquelles possèdent une serrure et quel modèle semble installé. C'est aussi ce qui en fait d'excellents outils de cybersécurité.

INSECAM ET CAMHACKER : QUAND L'INDEX DEVIENT UNE GALERIE DE CAMÉRAS

Insecam, apparu en 2014, existe toujours. Son principe va plus loin visuellement que Censys : il agrège directement des caméras accessibles et présente leurs images dans un annuaire. En 2026, CamHacker revendique de son côté 1 730 caméras réparties dans 67 pays, classées notamment par lieu et constructeur. Le site affirme ne référencer que des équipements accessibles sans authentification et les retirer lorsqu'ils sont protégés ; cette affirmation vient de l'éditeur et ne prouve évidemment pas le consentement de chaque propriétaire.



COMMENT CES MOTEURS VOIENT-ILS CE QUE GOOGLE NE VOIT PAS ?

C'est précisément ce que révèlent des moteurs de recherche comme Shodan, Censys ou Netlas. Contrairement à Google, qui indexe principalement des pages Web et leurs liens, ces services parcourent les adresses IP publiques, interrogent différents ports et protocoles puis enregistrent les réponses obtenues. Adresse IP, port ouvert, protocole, bannière logicielle, serveur HTTP, certificat TLS, fabricant



HACKING

QUELLES WEBCAMS PEUT-ON RÉELLEMENT DÉCOUVRIR ?

La catégorie est beaucoup plus large que la petite webcam USB installée au-dessus d'un écran. Les résultats peuvent

comprendre des caméras IP domestiques, des caméras Wi-Fi anciennes, des équipements de vidéosurveillance professionnels, des caméras PTZ motorisées, des portiers vidéo, des babyphones connectés, mais surtout des DVR et NVR, ces enregistreurs auxquels plusieurs caméras de vidéosurveillance sont reliées.

On rencontre également des caméras volontairement publiques : météo, paysages, ports, pistes de ski, circulation routière, chantiers ou observations scientifiques. À l'inverse, certaines interfaces trouvées par ces moteurs correspondent manifestement à des équipements qui n'auraient jamais dû être directement accessibles depuis Internet.

Les protocoles observables ne se limitent pas au Web HTTP ou HTTPS. Des systèmes vidéo peuvent exposer du RTSP, utilisé pour transporter des flux vidéo, ainsi que différentes interfaces propriétaires. Shodan collecte par



En France, près de 70000 points d'accès à des caméras sont répertoriés par scan sur le Web. Et près de 9000 d'entre eux seraient vulnérables.

exemple des captures provenant de services Web, RTSP, VNC, RDP ou X Window. Mais une caméra fonctionnant uniquement via le cloud du constructeur peut ne pas apparaître si aucun service n'est publié sur l'adresse Internet du foyer.

ET SI C'ÉTAIT LA VÔTRE ?

Si une caméra, un NVR ou une interface d'administration apparaît directement exposé, il faut vérifier si cet accès est indispensable, fermer les redirections inutiles, désactiver l'UPnP lorsqu'il ne sert pas, mettre à jour firmware et logiciels, remplacer les identifiants par défaut et privilégier un VPN ou un accès distant correctement sécurisé.

LE MARCHÉ NOIR DES CAMÉRAS PIRATÉES : PIRATAGE, VOL D'IDENTIFIANTS ET CYBERGUERRE



Chercher un unique « Insecam du darknet » serait trompeur. L'économie clandestine est désormais éclatée entre forums, places de marché, messageries (principalement Telegram) et infrastructures éphémères. Pour les caméras, le produit vendu n'est donc plus forcément « l'adresse d'une webcam » : il peut s'agir d'identifiants, d'un accès compromis ou directement de vidéos volées.

En Inde, une enquête révélée en 2025 a mis au jour le vol d'au moins 50 000 clips issus d'environ 80 tableaux de bord CCTV compromis. Des séquences ont ensuite été proposées dans des groupes Telegram, à des tarifs rapportés de 700 à 4 000 roupies.

La Corée du Sud a connu fin 2025 une affaire encore plus massive : quatre suspects ont été accusés d'avoir compromis environ 120 000 caméras IP dans des logements et commerces.

Il y a enfin les actes liés à la cyberguerre. En juillet 2026, un rapport publié le Service général néerlandais de renseignement et de sécurité (AIVD) et le Service néerlandais de renseignement et de sécurité de la défense (MIVD), expliquait que des acteurs étatiques



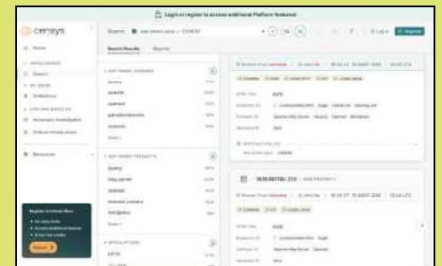
russes espionnaient certains pays européens et l'Ukraine par le biais de caméras connectées. La disponibilité accrue de l'intelligence artificielle (IA) a rendu cette dernière tâche beaucoup plus facile. L'IA peut également être utilisée pour corréler les données recueillies par différentes caméras afin de transformer les points de données individuels en une image plus large des routeurs de transport et des emplacements militaires.

TOP 3 MOTEUR DE RECHERCHE GRATUITS... MAIS PROS !

1# CENSYS > LE PLUS ANALYTIQUE

Censys vise moins l'effet « regardez ce qui traîne sur Internet » que l'analyse méthodique d'une infrastructure. Sa plateforme indexe les hôtes et leurs services, mais également les certificats et les propriétés Web. Elle sait classer certains résultats : parmi les labels utilisés par Censys figurent notamment « login_page », « open_directory » et, particulièrement intéressant ici, « camera ». L'outil permet de partir d'un élément connu — domaine, adresse, certificat ou service — puis de comprendre les relations avec d'autres actifs. La plateforme est en pleine transition en 2026. L'ancien Censys Search doit disparaître en septembre au profit de la nouvelle Censys Platform et de son langage CenQL. Mais Censys Free existe toujours ! Chaque compte gratuit reçoit actuellement 100 crédits par mois et donne accès à une visibilité Internet de base, aux protocoles courants, aux certificats et à une partie des informations relatives aux propriétés Web. La plateforme gratuite peut donc suffire pour quelques investigations ciblées sur ses propres équipements.

Lien : <https://platform.censys.io/search>



2# NETLAS > LE PLUS GÉNÉREUX GRATUITEMENT

Netlas est probablement le meilleur point d'entrée gratuit. Son offre Community, gratuite à vie et sans carte bancaire, autorise 50 requêtes par jour, 2 500 résultats par mois et 200 résultats par téléchargement. Son moteur permet de rechercher pratiquement n'importe quel champ présent dans les réponses : IP, domaine, port, protocole, contenu retourné ou propriétés spécifiques à certains services. Netlas propose explicitement des ressources consacrées à la recherche de « caméras IP et d'objets IoT ». L'entreprise a encore publié en mars 2026 un guide consacré aux webcams exposées, tout en rappelant que l'existence d'un flux accessible techniquement n'autorise pas pour autant son utilisation lorsqu'il s'agit d'une caméra privée.

Lien : <https://app.netlas.io/>



SHODAN, LA RÉFÉRENCE PREMIUM



Shodan reste la référence des moteurs de recherche de par son ancienneté et son sérieux. Il indexe les services joignables et permet de croiser ports, protocoles, logiciels, pays ou organisations. Il collecte aussi certaines captures issues notamment de webcams, RTSP, RDP ou VNC. Mais sa fonction la plus intéressante ici, la « Fonction Images » avec tous ses outils est liée à un abonnement payant; tous les comptes disposent cependant d'un plan API gratuit. Son écosystème et sa documentation sont excellents, mais le gratuit donne surtout un avant-goût des fonctions avancées.

Lien : <https://www.shodan.io/>



3# FOFA > LE PARADIS POUR UTILISATEURS AVANCÉS

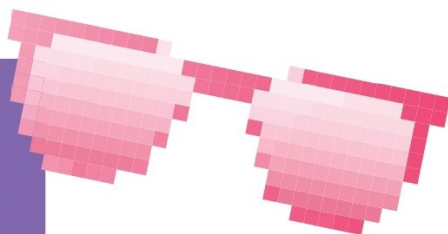
On peut y rechercher des équipements et services à partir d'informations techniques extrêmement variées, puis utiliser les empreintes identifiées par la plateforme pour distinguer produits et technologies. Pour l'audit de ses propres équipements, cela permet par exemple de partir d'un fabricant, d'un logiciel ou d'une caractéristique Web afin de retrouver les actifs correspondants. Et le compte Registered User est réellement gratuit. FOFA lui attribue 300 crédits de requête par mois, 3 000 résultats mensuels et l'accès à 44 syntaxes de recherche. Il autorise même le téléchargement Web des résultats. Moins accueillant pour le néophyte, certaines fonctions d'analyse avancée sont payantes et le compte gratuit est officiellement cantonné aux utilisations non commerciales.

Lien : <https://en.fofa.info/>





DECRYPTAGE



FIN DES PIXELS ESPIONS ?

La relève est déjà là...

Grâce aux « pixels espions », un simple courriel peut avertir son expéditeur de son ouverture, révéler l'heure de lecture, le type d'appareil utilisé et parfois une localisation approximative. Depuis avril 2026, la CNIL impose enfin un consentement préalable à l'envoi de ces mouchards invisibles. Sauf qu'ils ne sont que la partie émergée de l'iceberg.



Vous ouvrez une newsletter commerciale, un message d'une association ou une relance envoyée par un service en ligne. Rien ne bouge à l'écran, aucune fenêtre ne s'affiche et aucune demande d'autorisation ne vous est présentée, vous ne cliquez sur aucun lien... Et pourtant, des informations personnelles sont déjà envoyées en retour à l'expéditeur, sans que vous n'ayez rien demandé. : le message vient d'être consulté.

Ce tour de passe-passe repose souvent sur une minuscule image distante, généralement transparente et réduite à un pixel sur un pixel. Lorsque le logiciel ou service de messagerie affiche le courriel, il appelle cette

À SAVOIR

La principale nouveauté française consiste à rattacher clairement les pixels de suivi au régime juridique déjà applicable aux cookies et autres traceurs. Pour la CNIL, le chargement du pixel entraîne une lecture d'informations sur le terminal du destinataire. Il relève donc de l'article 82 de la loi Informatique et Libertés, qui transpose en France les règles européennes relatives à la confidentialité des communications électroniques.



Aujourd'hui, on fait une petite pause dans les paillettes et les strass pour un sujet un peu plus administratif, mais essentiel : **la transparence sur vos données !**

Pour être tout à fait claires avec vous, nous utilisons un outil technique appelé **"pixel de suivi"** dans nos newsletters.

À quoi sert ce pixel ?

Il nous permet simplement de savoir **si nos emails ont été ouverts**. Cela nous est très utile pour :

- **Mesurer ce qui vous plaît** afin d'améliorer nos prochains contenus.
- **Ajuster la fréquence de nos envois** pour ne pas encombrer votre boîte mail.
- **Mieux cibler nos offres** pour vous proposer des nouveautés qui vous correspondent.

C'est vous qui décidez. Vous avez totalement le droit de ne pas être suivi(e). **Vous pouvez désactiver ce pixel à tout moment**, en un seul clic, via le lien ci-dessous :

[Je m'oppose à l'utilisation du pixel de suivi](#)

Ce qu'il faut savoir :

LES ENTREPRISES AVAIENT JUSQU'AU 14 JUILLET POUR VOUS AVERTIR SI ELLES UTILISAIENT DES PIXELS-ESPIONS DANS LES EMAILS QU'ELLES VOUS ENVOYAIENT ET POUR VOUS PROPOSER DE VOUS OPPOSER À CE TRACKING INVISIBLE.



image sur le serveur de l'expéditeur. Celui-ci peut alors associer la requête à une adresse électronique et enregistrer l'ouverture du message et même des informations sur votre appareil et votre localisation.

La technique n'est pas nouvelle. Mais la CNIL constate une progression de son utilisation et indique recevoir un nombre croissant de signalements et de plaintes. Le 12 mars 2026, elle a donc adopté une recommandation spécifique, publiée au Journal officiel le 14 avril. Celle-ci concerne les entreprises, mais aussi les associations, administrations et collectivités utilisant des pixels dans

CE QUI N'EST TOUJOURS PAS CONTRÔLÉ !



> Les liens individualisés

Ils sont la principale technique complémentaire aux pixels-espions. Chaque destinataire reçoit une adresse légèrement différente (par exemple : <https://exemple.fr/offre?id=8f32a7...>). Lorsque le destinataire clique, le serveur sait immédiatement quel message et quel destinataire sont à l'origine de la visite. Il peut enregistrer l'heure, l'adresse IP apparente, le navigateur, le système d'exploitation, la page consultée et les actions réalisées ensuite.

> Les images visibles personnalisées

Un traceur n'a nul besoin d'être transparent ou de mesurer un pixel. Un logo, une bannière, une photographie de produit ou un bouton graphique peuvent être servis depuis une adresse propre à chaque destinataire. Lorsque l'image est téléchargée, le résultat est identique : le serveur apprend que la ressource liée à cette personne a été demandée. Une newsletter peut donc ne contenir aucun « minuscule pixel invisible » tout en suivant précisément ses ouvertures.

> Les polices, feuilles de style et autres ressources distantes

En théorie, toute ressource que le logiciel de messagerie va chercher sur Internet peut servir de

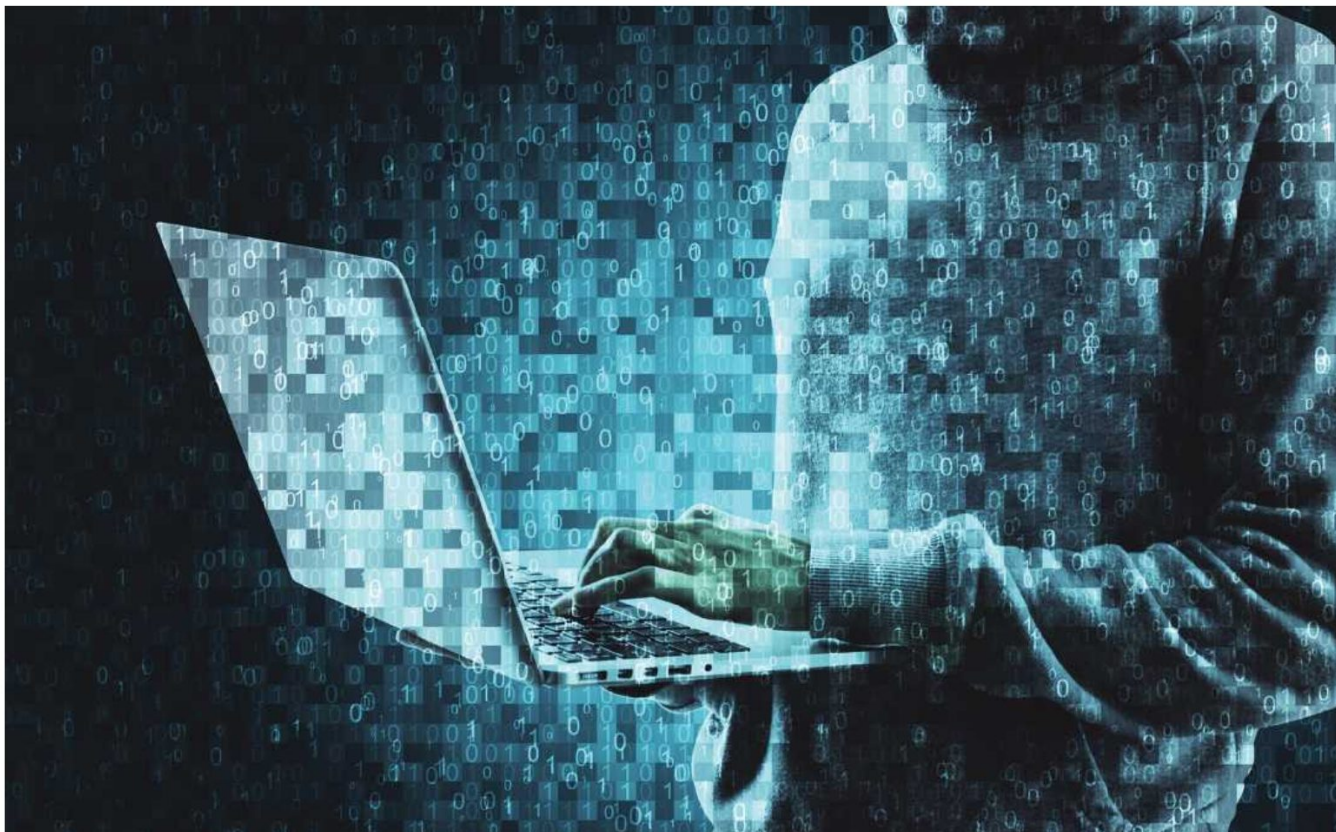
balise : une police de caractères, une feuille de style CSS, une image d'arrière-plan ou un autre élément externe. Dans la pratique, les grands services de messagerie filtrent fortement le HTML reçu. Ils neutralisent généralement JavaScript, les iframes, de nombreuses balises actives et les formulaires dangereux. Les capacités varient néanmoins selon les clients.

> Les identifiants inscrits directement dans le message

Un expéditeur peut intégrer un identifiant unique dans le corps, les métadonnées techniques ou l'adresse de désinscription. Cet identifiant ne transmet rien tant que le courriel reste fermé et qu'aucune ressource n'est chargée. Mais il permet de rattacher ultérieurement une action — clic, désinscription, transfert vers un site ou réponse — à un destinataire précis.

> Le fingerprinting après le clic

Le courriel sert alors seulement de porte d'entrée. Une fois arrivé sur le site, le visiteur peut être reconnu par des cookies, son compte connecté, les paramètres du navigateur, son adresse IP ou certaines caractéristiques techniques de son appareil.



leurs courriels. Depuis avril et surtout juste avant la date d'application maximale tolérée du 14 juillet, vous avez dû recevoir de nombreux mails vous demandant si vous y consentiez.

En principe, l'expéditeur doit désormais obtenir un consentement libre, spécifique, éclairé et univoque avant d'utiliser le pixel.

La CNIL recommande de présenter le choix au moment où l'adresse électronique est recueillie. Lorsqu'elle possède déjà l'adresse, l'organisation peut envoyer un courriel spécifique demandant l'autorisation, mais ce message ne doit évidemment pas contenir lui-même un pixel soumis au consentement. L'accord doit résulter d'une action positive : ne pas répondre ou ne cliquer sur aucun bouton doit être considéré comme un refus. Le retrait doit ensuite être aussi simple que l'acceptation, idéalement grâce à un lien présent au bas de chaque courriel.

Pour les adresses collectées avant la publication de la recommandation, la CNIL a accordé une transition plus souple : les organismes disposaient de trois mois pour

informer clairement les destinataires de l'utilisation des pixels et leur permettre de s'y opposer facilement.

CE QUE RÉVÈLE RÉELLEMENT UN PIXEL-ESPION

Le mot « pixel » peut donner l'impression d'un dispositif rudimentaire. En réalité, l'image n'est qu'un déclencheur. L'essentiel se joue sur le serveur qui la distribue. À son chargement, celui-ci peut enregistrer l'identifiant associé au message, la date et l'heure de la requête, l'adresse IP apparente ainsi que certaines informations techniques transmises par le logiciel de messagerie. L'expéditeur peut ainsi savoir si le courriel a été ouvert, à quel moment, depuis quelle catégorie d'appareil et, selon les circonstances, déduire de l'adresse IP une localisation plus ou moins approximative. Le pixel ne permet cependant pas de lire les autres messages de la boîte, d'accéder au mot de passe, ni de parcourir directement le contenu de l'ordinateur. Il s'agit d'un outil de traçage, pas d'un logiciel espion installé sur la machine.

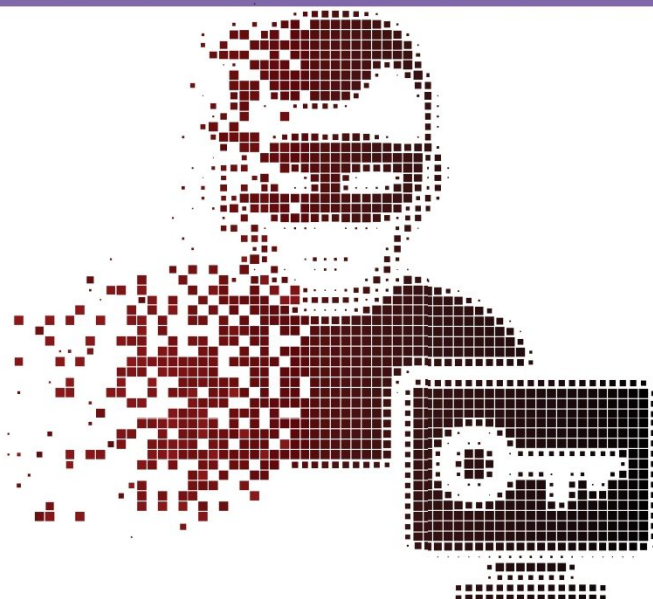
Selon la CNIL, « ne pas répondre ou ne cliquer sur aucun bouton doit être considéré comme un refus ».

UN PROFILAGE QUI N'EST PAS ANODIN

Pris isolément, le renseignement peut paraître anodin. Mais une succession d'ouvertures permet de construire un historique : heures habituelles de consultation, réactivité à certains sujets, utilisation d'un téléphone ou d'un ordinateur, périodes d'activité et centres d'intérêt présumés. Un service commercial peut s'en servir pour adapter ses horaires d'envoi, relancer les personnes ayant ouvert un message ou établir des profils publicitaires.

TOUT BLOQUER POUR SE PROTÉGER ?

Par défaut, avant même de donner ou refuser son consentement, bloquer les pixels paraît simple : il suffit d'empêcher le téléchargement automatique

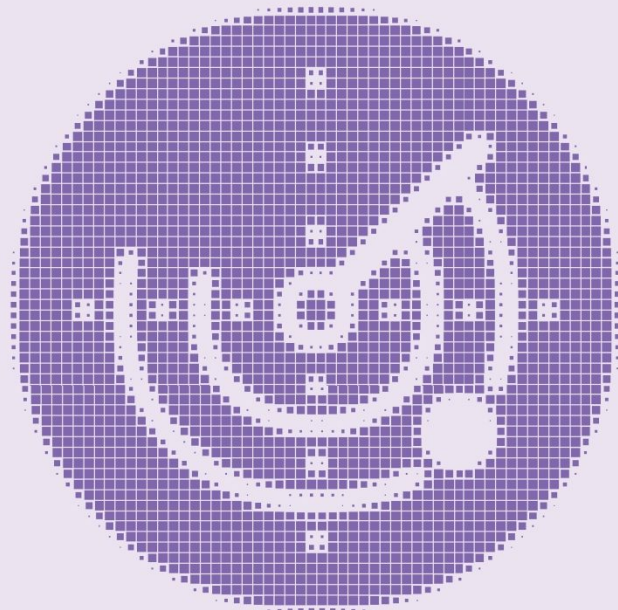


LES PIXELS-ESPIONS EXISTENT-ILS HORS DE VOS EMAILS ?

Oui ! Le principe technique porte un nom plus large : « balise web », « web beacon », « tracking pixel » ou « requête traçante ». Il consiste à faire charger une ressource distante afin d'informer un serveur qu'un contenu a été affiché.

> Sites web et forums

Balises intégrées nativement ou autorisation d'images externes dans les messages ou les signatures : l'éditeur ou un utilisateur malveillant peuvent intégrer une image hébergée sur leur propre serveur. Chaque consultation du sujet déclenche alors une requête susceptible de révéler l'heure, l'adresse IP apparente et certaines informations techniques.



> Messageries instantanées

Le traçage peut lui aussi intervenir lors du téléchargement d'une image, d'un GIF, d'un autocollant, d'un avatar ou d'une pièce jointe hébergée à distance.

> Documents

Un document HTML, Word, une présentation ou parfois un PDF peut contenir un lien vers une ressource distante. Si le logiciel autorise son chargement, l'ouverture du document peut provoquer une connexion au serveur de l'auteur. Les logiciels récents affichent souvent un avertissement ou bloquent certains contenus externes. Les macros, modèles distants et objets liés constituent des risques plus importants que le pixel lui-même.

> Publicités et réseaux sociaux

Les boutons sociaux, widgets, vidéos intégrées et régies publicitaires peuvent appeler plusieurs serveurs tiers. La simple présence d'un bouton « J'aime » ou d'une vidéo embarquée sur une page peut transmettre des informations à la plateforme concernée, même sans clic, si la ressource est chargée directement.

> Streamings audio et vidéo

Ils produisent naturellement une importante télémétrie : début et arrêt de la lecture, durée, pauses, progression, changement de qualité, erreurs, modèle d'appareil et adresse IP. Il ne s'agit généralement pas d'un pixel-espion au sens strict. Le serveur doit recevoir des requêtes successives pour transmettre les fragments audio ou vidéo. Mais ces requêtes permettent de mesurer très précisément le comportement de l'utilisateur.





ANONYMAT

des images externes. Le principe est efficace, car l'image reste alors sur le serveur et aucune requête liée à son ouverture n'est normalement déclenchée. Cette protection dégrade toutefois l'apparence de nombreuses newsletters, dont les logos, photographies et boutons sont eux aussi hébergés à distance. Il faut alors choisir manuellement d'afficher les images pour les expéditeurs de confiance. D'autres messageries utilisent une méthode différente : elles chargent les images par l'intermédiaire de leurs propres serveurs ou les téléchargent à l'avance. Cette technique peut masquer l'adresse IP et l'heure réelle de consultation, mais elle ne garantit pas toujours que l'expéditeur ne comptabilisera aucune ouverture. Une image récupérée automatiquement peut même produire une fausse ouverture, alors que l'utilisateur n'a jamais lu le message.

UN PIXEL-ESPION PEUT-IL SERVIR À LANCER UNE CYBERATTAQUE ?

Une image de suivi classique ne contient pas de commande exécutable. Son rôle est de provoquer une requête vers un serveur. Elle ne peut pas, à elle seule, installer un cheval de Troie, prendre le contrôle de l'ordinateur ou voler les documents présents sur le



disque. Son utilité offensive se situe principalement dans la « reconnaissance » et le profilage de la cible et de ses habitudes. De manière générale, les balises web peuvent confirmer aux spammeurs qu'une adresse est valide, augmentant ainsi le risque de recevoir d'autres messages indésirables.

Il existe enfin une différence essentielle entre « un pixel de suivi » et « un fichier image malveillant ». Une image corrompue peut chercher à exploiter une faille

dans la bibliothèque chargée de décoder les formats JPEG, PNG, WebP ou GIF. Si le logiciel, le système ou la bibliothèque présente une vulnérabilité, le simple traitement du fichier peut parfois provoquer un plantage, une fuite d'informations ou, dans les cas les plus graves, l'exécution de code.

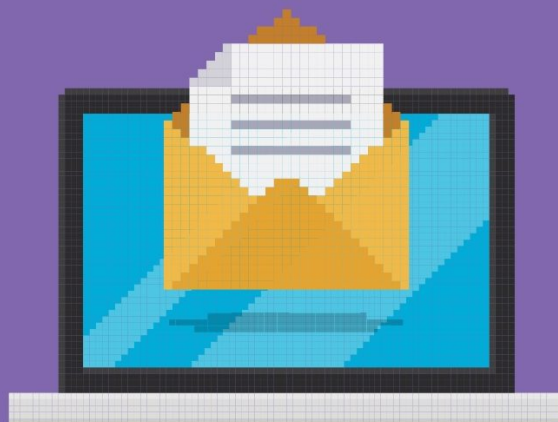
Spam, phishing ou activation d'une vulnérabilité : vous aurez compris l'intérêt de bloquer par défaut les contenus distants (**lire page 38**) !

UN RISQUE ÉMERGENT : LES ASSISTANTS D'IA CONNECTÉS AUX E-MAILS

Les assistants capables de lire, résumer et traiter automatiquement les messages ouvrent un autre front. Un courriel peut contenir du texte caché ou des instructions destinées non pas au lecteur, mais au modèle d'intelligence artificielle qui analyse sa boîte. C'est une forme d'« injection indirecte de prompt », et non une attaque par pixel. L'OWASP cite explicitement les instructions cachées dans les courriels et pièces jointes parmi les contenus susceptibles de manipuler un assistant d'IA.

UNE EXCEPTION À CONNAÎTRE

Tous les pixels-espions ne sont pas automatiquement interdits en l'absence de consentement. La CNIL admet certaines exemptions lorsqu'ils sont strictement nécessaires à un service demandé par l'utilisateur. Par exemple, un expéditeur peut, sous conditions, identifier les destinataires devenus inactifs afin de réduire la fréquence des envois ou de nettoyer sa liste. Et seulement ce type d'information, pas question d'en profiter pour poursuivre un profilage, la collecte doit être réduite au strict nécessaire. Seule la date de la dernière ouverture devrait en principe être conservée. L'exemption peut également couvrir certaines communications administratives directement liées à une mission de service public.

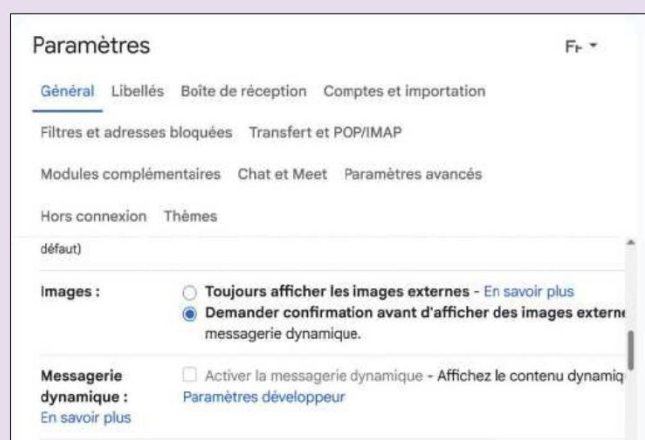




NEUTRALISER LES PIXELS DANS GMAIL

01 > SUR ORDINATEUR

Ouvrez Gmail, cliquez sur la roue dentée, puis sur **Voir tous les paramètres**. Dans l'onglet **Général**, repérez la rubrique **Images** et sélectionnez **Demander confirmation avant d'afficher des images externes**. Descendez ensuite en bas de la page et validez avec **Enregistrer les modifications**. Les messages continueront d'apparaître, mais Gmail demandera votre autorisation avant de récupérer leurs images distantes. Vous pourrez les afficher ponctuellement pour un courriel ou les autoriser pour un expéditeur identifié.



02 > SUR ANDROID

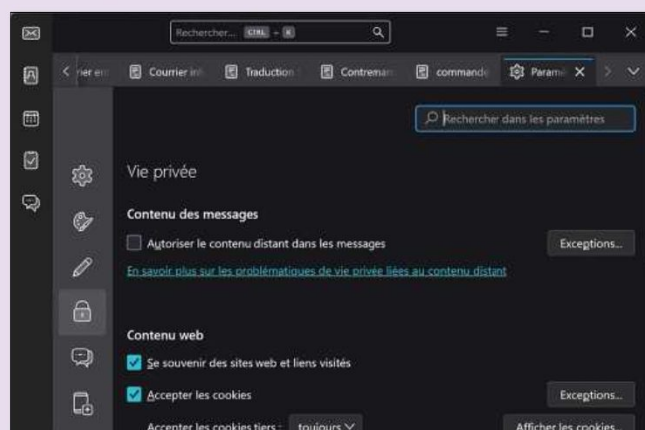
Ouvrez l'application Gmail, affichez son menu, puis choisissez **Paramètres** et sélectionnez le compte concerné. Dans la rubrique **Images**, activez **Demander confirmation avant d'afficher des images externes**. L'opération doit être répétée pour chaque compte configuré.



DES CLIENTS DE MESSAGERIE AU TOP

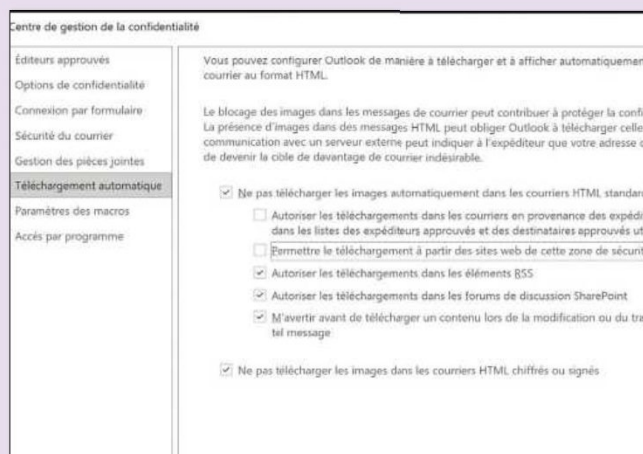
01 > THUNDERBIRD

Thunderbird constitue l'une des solutions les plus protectrices dès son installation. Le logiciel bloque par défaut le contenu distant et affiche un bandeau lorsqu'un message tente de charger des images ou d'autres ressources en ligne. Pour vérifier le réglage, ouvrez le menu principal, puis **Paramètres > Vie privée et sécurité**. Dans la partie consacrée au contenu des messages, l'option permettant d'autoriser le contenu distant ne doit pas être activée globalement.



02 > OUTLOOK

Sur pour Windows, les téléchargements automatiques d'images sont normalement bloqués par défaut. Vérifiez dans **Fichier > Options > Centre de gestion de la confidentialité > Paramètres du Centre de gestion de la confidentialité > Téléchargement automatique**. Outlook mobile propose désormais un interrupteur clairement identifié pour bloquer les images externes. (**Paramètres > Bloquer les images externes**).





PRIVACY BADGER : BLOQUEZ LES ESPIONS QUI VOUS SUIVENT SUR LE WEB



Privacy Badger fait partie des extensions indispensables pour votre navigateur ! Puissante et efficace sans exiger de longues séances de configuration. Son principal atout n'est pas de promettre l'invisibilité, mais de réduire discrètement la quantité de données que les régies publicitaires, plateformes sociales et courtiers en données peuvent collecter au fil de votre navigation.

Publicités personnalisées, boutons sociaux, outils statistiques et pixels invisibles peuvent permettre à des sociétés tierces de suivre un internaute d'un site à l'autre. Développé par l'Electronic Frontier Foundation, Privacy Badger est une extension gratuite et open source chargée de repérer puis de bloquer ces mécanismes de pistage. Elle fonctionne notamment avec Firefox, Chrome et les navigateurs compatibles avec les extensions Chromium. En juillet 2026, sa version Chrome dépassait le million d'utilisateurs et l'extension Firefox en comptait environ 1,7 million.

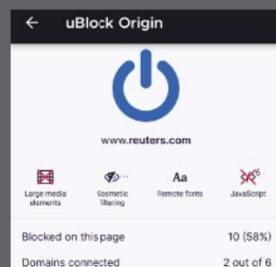
UN BLOQUEUR DE TRAQUEURS, PAS UN BLOQUEUR DE PUBLICITÉS

Privacy Badger n'a pas pour objectif de supprimer toutes les publicités. Il cherche d'abord à empêcher les domaines tiers de surveiller la navigation sans



PRIVACY BADGER AVEC UBLOCK ORIGIN : UTILE OU REDONDANT ?

Les deux extensions peuvent cohabiter. uBlock Origin est principalement un bloqueur de contenus (principalement publicitaires) reposant sur des listes de filtres, tandis que Privacy Badger se concentre sur le comportement des domaines tiers, les signaux GPC et Do Not Track, le nettoyage de certains liens et le remplacement de widgets. Une partie de leur travail se recoupe néanmoins. Lorsqu'uBlock Origin bloque une ressource avant son chargement, Privacy Badger ne la voit pas nécessairement. Cela ne pose pas de problème majeur : l'essentiel est que le traqueur ne fonctionne pas.





consentement. Une publicité non traçante peut donc rester visible, tandis qu'un script statistique invisible peut être bloqué. Pour supprimer la majorité des réclames, il faut lui associer un bloqueur de contenus classique tel qu'uBlock Origin.

Lorsqu'une page est ouverte, l'extension examine les domaines extérieurs qui chargent des images, cookies, scripts ou autres ressources. Elle recherche notamment des identifiants uniques, des données stockées localement et certaines techniques de fingerprinting. Elle bénéficie aussi des analyses du projet Badger Swarm, qui lui fournit une connaissance préentraînée de nombreux traqueurs.

L'extension peut enfin nettoyer certains liens de suivi employés par Google et Facebook et remplacer des contenus intégrés — vidéos, publications sociales ou commentaires — par des cadres inactifs. Le contenu ne communique alors avec la plateforme concernée que si l'internaute décide de l'activer.

ARRÊTEZ DE ME SUIVRE !

Privacy Badger envoie également deux signaux aux sites visités. **Do Not Track** leur indique que l'utilisateur refuse d'être suivi, tandis que **Global Privacy Control** exprime une opposition à la vente ou au partage des données personnelles.

En France, Global Privacy Control n'a pas encore la portée juridique automatique et contraignante qu'il possède outre-Atlantique. Un site français ne peut donc pas être considéré, à lui seul, comme illégal simplement parce qu'il ignore le signal GPC envoyé par Privacy Badger.

GPC n'est pourtant pas dépourvu de sens juridique, notamment au regard de notre RGPD européen. En pratique, et en l'attente d'une jurisprudence claire, il faut toujours utiliser « Tout refuser » dans le bandeau de consentement lorsque cette option est proposée. Le signal GPC constitue une protection supplémentaire, mais ne garantit pas que le gestionnaire de consentement du site en tiendra compte.



EN PLUS DE BLOQUER AUTOMATIQUEMENT LES TENTATIVES DE TRAÇAGE, PRIVACY BADGER ENVOIE AUX SITES VISITÉS UNE DEMANDE DE NE PLUS VOUS SUIVRE ET DE NE PLUS VOUS PROFILER À L'AVENIR.



LE GUIDE POUR BIEN UTILISER PRIVACY BADGER

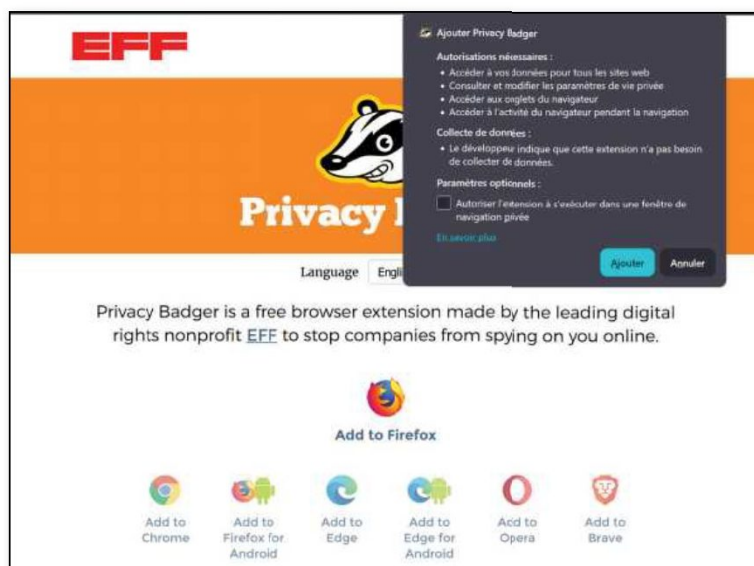


01 > AJOUTER L'EXTENSION

Dans Firefox, cliquez sur **Add to Firefox**, puis confirmez avec **Ajouter**. Dans Chrome, Edge, Brave ou Vivaldi, sélectionnez **Add to Chrome** ou **Obtenir**, puis validez l'autorisation demandée (nécessaire pour examiner les ressources chargées et empêcher les traqueurs de fonctionner).

ATTENTION

De faux Privacy Badgers circulent ! Télécharger uniquement la version officielle. Via le site de Privacy Badger (<https://privacybadger.org/>), le bouton proposé renvoie vers la boutique correspondant au navigateur utilisé.





02 > ÉPINGLER SON ICÔNE

Dans Chrome ou Edge, cliquez sur l'icône représentant une pièce de puzzle, puis épinglez Privacy Badger. Dans Firefox, ouvrez le menu des extensions et placez son icône dans la barre d'outils. L'icône devient alors accessible sur chaque page et affiche le nombre de domaines susceptibles d'être bloqués ou limités.

CURSEURS ROUGE, JAUNE ET VERT : COMPRENDRE LES TROIS NIVEAUX DE PROTECTION



Ouvrez un site, puis cliquez sur l'icône de Privacy Badger. Une liste de traceurs appartenant à des domaines tiers apparaît, chacun accompagné d'un curseur à trois positions.

> VERT : DOMAINE AUTORISÉ

Le vert signifie que Privacy Badger ne prend aucune mesure particulière. Le domaine peut charger normalement ses contenus et utiliser ses cookies. Cela ne veut pas nécessairement dire qu'il est vertueux : l'extension n'a simplement pas décidé de le restreindre dans cette situation.

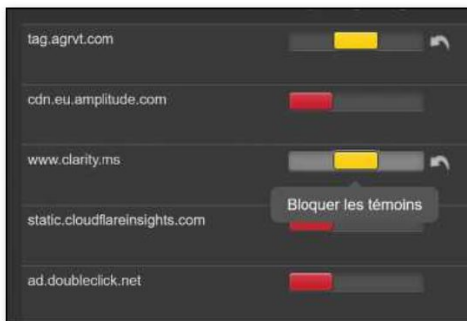
> JAUNE : CONTENU AUTORISÉ, COOKIES BLOQUÉS

Le jaune constitue un compromis. Privacy Badger soupçonne un comportement de suivi, mais considère que le domaine peut être nécessaire au fonctionnement du

site. Il autorise donc le contenu tout en tentant de bloquer ses cookies tiers, son stockage local et certaines informations de provenance. Cette position évite, par exemple, de casser un lecteur vidéo, un formulaire de paiement ou un module de connexion indispensable.

> ROUGE : DOMAINE ENTIÈREMENT BLOQUÉ

Le rouge interdit le chargement des ressources provenant du domaine. C'est la protection la plus forte, mais aussi celle qui risque le plus de perturber une page. Une vidéo peut disparaître, un bouton ne plus fonctionner ou un formulaire refuser de se charger.

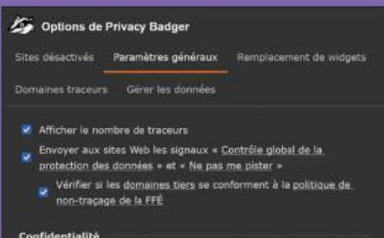


03 > RÉGLER MANUELLEMENT UN DOMAINE

Privacy Badger fonctionne normalement sans intervention. Il est néanmoins possible de déplacer manuellement chaque curseur (**lire ci-dessus**). Sur la page concernée, cliquez sur l'icône de Privacy Badger, repérez le domaine puis déplacez son curseur vers le rouge, le jaune ou le vert selon votre besoin.

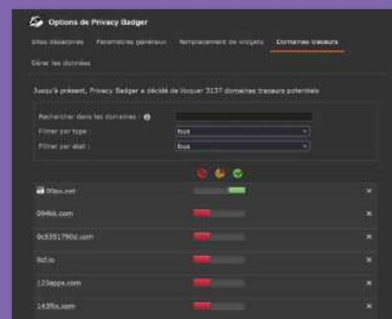
EXPLORER LES PARAMÈTRES AVANCÉS

Cliquez sur l'icône de Privacy Badger puis sur l'icône en forme d'engrenage et **Paramètres généraux**. Vérifiez que **Global Privacy Control** et **Do Not Track** sont bien activés. Ils ajoutent une demande explicite de confidentialité au blocage technique.



Selon la version installée, vous pouvez également gérer les remplacements de widgets sociaux et choisir d'afficher ou non tous les domaines détectés dans la fenêtre principale. L'onglet consacré aux domaines de pistage rassemble les décisions prises par Privacy Badger. Utilisez le champ de recherche pour

retrouver un domaine précis. Cette interface est pratique lorsqu'un problème concerne un sous-domaine difficile à identifier dans la petite fenêtre de l'extension.



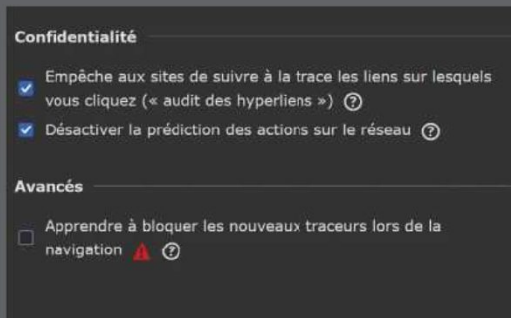
Enfin, la rubrique des sites désactivés répertorie les sites sur lesquels Privacy Badger a été coupé. Vérifiez-la régulièrement afin de ne pas conserver inutilement d'anciennes exceptions. Pour restaurer la protection, retirez le site de la liste ou ouvrez-le et utilisez le bouton de réactivation.

04 > RÉPARER UNE FONCTION CASSÉE

Typiquement, lorsqu'un lecteur, un bouton ou un formulaire ne fonctionne plus, ouvrez Privacy Badger et recherchez le domaine affiché en rouge. Passez-le d'abord au jaune, puis rechargez la page. Cette position suffit souvent à restaurer la fonction tout en conservant une protection contre les cookies tiers. Si le problème persiste, placez le domaine en vert et rechargez une nouvelle fois. Cette méthode est préférable à la désactivation complète de l'extension.

FAUT-IL ACTIVER L'APPRENTISSAGE LOCAL ?

Privacy Badger reçoit aujourd'hui des informations préentraînées grâce aux analyses du projet Badger Swarm. Certaines versions proposent également un apprentissage local, permettant à l'extension d'adapter progressivement ses décisions aux sites visités. Cette option, non activée par défaut, peut renforcer la détection de domaines inhabituels, mais elle augmente aussi le risque de faux positifs et de pages cassées. Pour un utilisateur débutant, il est préférable de conserver les réglages par défaut. Les utilisateurs expérimentés peuvent l'activer, puis surveiller attentivement les domaines passés au rouge.



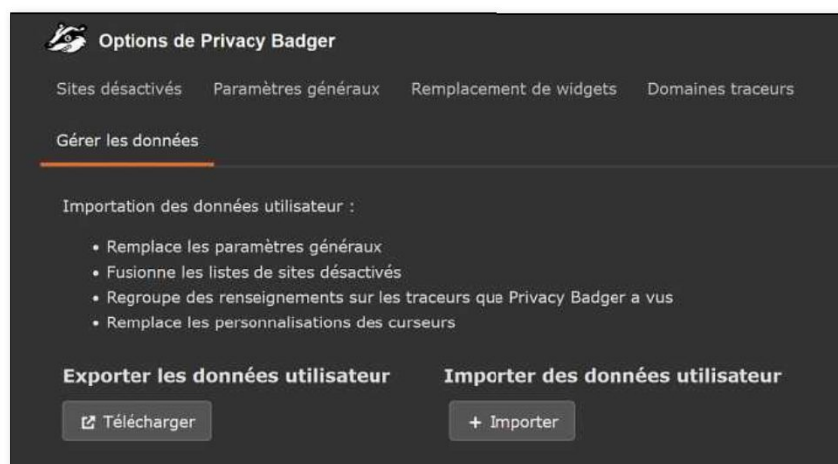
05 > DÉSACTIVER PRIVACY BADGER POUR UN SEUL SITE

Si une page reste inutilisable, cliquez sur l'icône du blaireau. Sélectionnez **Désactiver pour ce site**. L'extension restera active pour les autres sites. Pour rétablir la protection, ouvrez de nouveau le menu puis cliquez sur **Réactiver pour ce site**. Cette exception convient notamment aux sites bancaires, plateformes administratives ou boutiques dont certaines fonctions refusent de fonctionner malgré les réglages manuels.



06 > ACTIVER LES CONTENUS SOCIAUX À LA DEMANDE

Privacy Badger peut remplacer certains lecteurs vidéo, publications Instagram, Threads, Bluesky ou autres modules sociaux par un encadré protecteur. Pour afficher le contenu, cliquez sur le bouton proposé dans l'encadré. Seul cet élément est alors chargé.



07 > RÉINITIALISER PRIVACY BADGER

Si les pages cassées se multiplient ou si vous avez modifié trop de curseurs, ouvrez les options et choisissez la fonction de réinitialisation des données. Cette opération efface les décisions personnalisées et restaure la configuration par défaut. Exportez auparavant vos réglages via les **Paramètres > Gérer les données** si vous souhaitez pouvoir revenir en arrière.



QUE VAUT LE VPN INTÉGRÉ DE FIREFOX ?

Firefox propose l'un des VPN de navigateur gratuits les plus intéressants du moment. Son chiffrement est réel, son quota généreux et son activation particulièrement accessible. Il constitue une excellente protection de premier niveau pour le grand public.



Depuis mars 2026, Firefox propose progressivement en France un VPN gratuit directement intégré au navigateur. Plus besoin d'installer une extension ou un logiciel supplémentaire : une icône permet d'activer la protection en quelques secondes, à condition de disposer d'un compte Mozilla. L'offre paraît séduisante, mais elle ne remplace pas totalement un VPN classique. Le service permet aujourd'hui de faire transiter jusqu'à 50 Go de données par mois par l'intermédiaire de serveurs exploités avec l'infrastructure de Fastly. Depuis mai 2026, l'utilisateur peut également choisir son pays de connexion parmi plusieurs destinations, dont la France, l'Allemagne, le Royaume-Uni, le Canada et les États-Unis.

UN VÉRITABLE CHIFFREMENT, MAIS LIMITÉ AU NAVIGATEUR

Lorsqu'il est activé, le service établit une connexion TLS chiffrée entre Firefox et son serveur relais. Les requêtes DNS du navigateur passent elles aussi dans ce canal protégé. Sur le réseau Wi-Fi, dans la box et

chez le fournisseur d'accès, les données ne circulent donc pas en clair : elles apparaissent sous la forme d'un flux chiffré dirigé vers le relais de Firefox. Comme avec un VPN traditionnel, le FAI peut toujours

ET QUE VAUT LA PROTECTION TLS ?



Voici un terme que l'on a moins l'habitude d'entendre. TLS, pour « Transport Layer Security », est le protocole également utilisé par HTTPS. Firefox et le serveur relais créent une clé temporaire permettant de chiffrer leurs échanges. Une personne qui intercepte le trafic sur le Wi-Fi ou chez le FAI ne peut pas en lire le contenu. TLS vérifie aussi que les données n'ont pas été modifiées pendant leur transport. TLS n'est pas un algorithme de chiffrement, mais un protocole qui négocie plusieurs mécanismes cryptographiques dont ceux que nous connaissons tous, comme AES-256-GCM, AES-128-GCM ou ChaCha20-Poly1305, en fonction des serveurs et de l'appareil (PC ou mobile) utilisés.

Attention, ce service est un proxy VPN sécurisé limité au navigateur, il ne protège pas l'ensemble du trafic sortant de votre PC ou mobile.



observer qu'une connexion existe, connaître son horaire, sa durée, le volume échangé et l'adresse du relais utilisé. En revanche, il ne voit normalement plus directement les sites contactés par Firefox. Une fois arrivé au relais, le trafic repart vers le site demandé. Lorsque celui-ci utilise HTTPS, le contenu reste chiffré entre le navigateur et le site.

La nuance essentielle tient au périmètre : seul le trafic de Firefox est protégé. Les communications de Thunderbird, Spotify, OneDrive, d'un jeu, d'un autre navigateur ou d'un logiciel de téléchargement continuent à emprunter la connexion ordinaire. Mozilla VPN, l'offre payante distincte, protège au contraire l'ensemble de l'appareil.

Sa première force est son extrême simplicité. L'utilisateur active le VPN en un clic, sans choisir de protocole ni configurer de serveur. Le quota mensuel de 50 Go est également confortable pour consulter des sites, utiliser des services en ligne ou effectuer ponctuellement du streaming.

Il dépasse largement les 5 Go proposés par le réseau sécurisé de Microsoft Edge.

GÉNÉREUX MAIS SANS FONCTIONS AVANCÉES

On soulignera cependant le caractère minimaliste du service. Pas de tunnel couvrant tout Windows, pas de choix du protocole, pas de double VPN, de configuration sur routeur ni de véritable coupe-circuit système. Si la protection cesse de fonctionner, Firefox peut réutiliser la connexion normale, tandis qu'un VPN complet doté d'un kill switch peut bloquer toute fuite accidentelle.

L'obligation d'utiliser un compte Mozilla constitue une autre limite pour ceux qui recherchent un anonymat renforcé. Mozilla affirme ne pas enregistrer l'historique des sites visités ni vendre les données personnelles, mais conserve certaines informations techniques nécessaires au fonctionnement, à la mesure du quota et à la lutte contre les abus. Ce n'est donc pas un VPN « No-Log ».

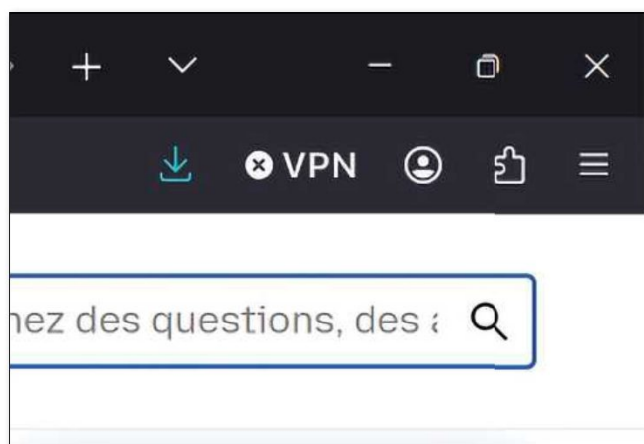
ACTIVEZ LE VPN INTÉGRÉ À FIREFOX

PRATIQUE



01 > DÉMARRER

Cliquez sur l'icône VPN en haut à droite de votre navigateur. Cliquez sur **Démarrer** puis créez votre compte Mozilla ou renseignez vos identifiants.



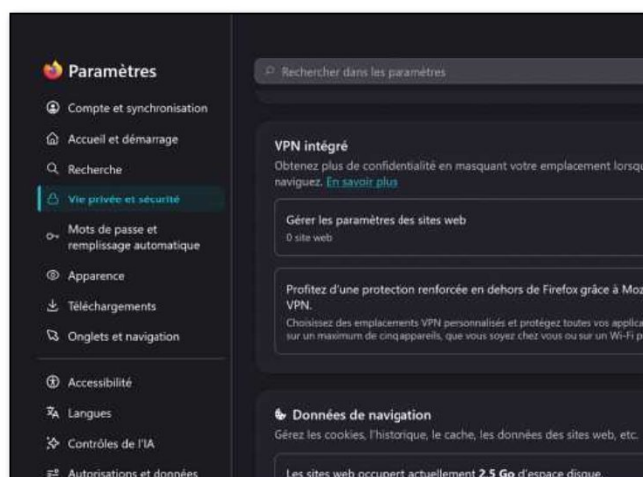
02 > ACTIVER

Cliquez sur **Activer le VPN**. Vous pouvez choisir au préalable ou en cours de navigation le serveur géographique de votre choix ou laissez le VPN vous le recommander (souvent le plus rapide et le moins encombré à un instant.)



03 > RÉGLAGES

Vous pouvez aussi, via les **Paramètres > Vie privée et sécurité**, choisir des sites sur lesquels le VPN sera désactivé automatiquement. Utile pour des services refusant de fonctionner lorsqu'un VPN est actif.



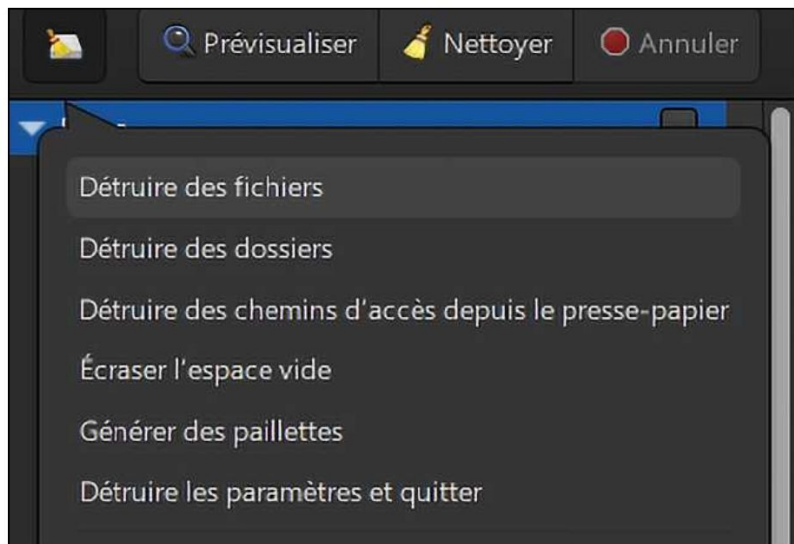


Détruire un fichier confidentiel

> AVEC BLEACHBIT

Placer un document dans la Corbeille puis la vider ne supprime généralement que ses références : son contenu peut rester récupérable tant qu'il n'a pas été réécrit. Dans BleachBit, ouvrez le menu principal, choisissez **Détruire des fichiers** à partir de l'icône de menu en haut à gauche, sélectionnez le document concerné et confirmez. Le logiciel renomme le fichier, écrase son contenu en un passage, puis le supprime. Cette méthode est surtout efficace sur un disque dur mécanique : sur un SSD, le nivellement d'usure, les zones de réserve et la gestion de TRIM empêchent de garantir que toutes les anciennes cellules ont été réécrites. Considérez donc la destruction sur SSD comme une mesure complémentaire et privilégiez le chiffrement intégral du disque pour les données réellement sensibles.

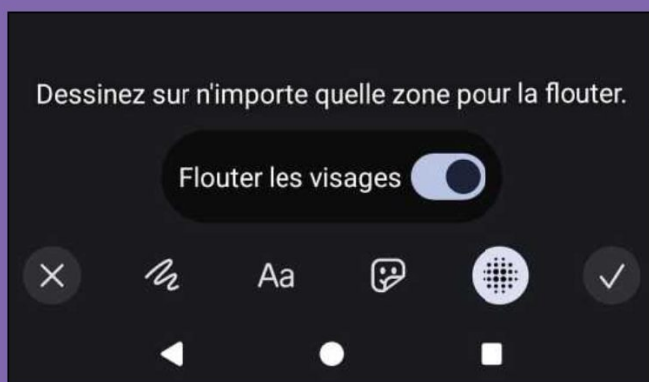
Lien : www.bleachbit.org



Flouter automatiquement les visages > AVEC SIGNAL

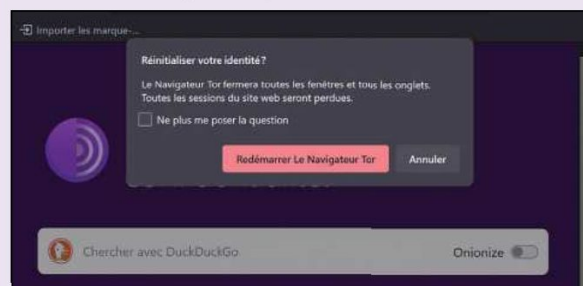
Une photographie partagée dans une conversation ou sur un réseau social peut révéler l'identité de personnes qui n'ont pas souhaité apparaître. Dans Signal, sélectionnez l'image à envoyer, ouvrez l'outil **Flou** (icône disque en damiers dans l'éditeur de photos), puis activez **Floutez les visages**. L'application masque les visages repérés directement sur le téléphone : l'analyse n'est pas envoyée vers un serveur distant. Avant l'envoi, inspectez néanmoins toute la photo. La détection peut manquer un visage de profil, éloigné ou partiellement dissimulé ; Dessinez alors au doigt la zone à flouter masquer manuellement la personne, mais aussi une plaque d'immatriculation, un badge, une adresse ou un écran visible à l'arrière-plan.

Lien : <https://signal.org/>



Repartir avec une nouvelle identité > AVEC TOR BROWSER

Changer simplement de site ne suffit pas toujours à séparer deux activités : cookies, historique et circuits Tor peuvent encore permettre de les rapprocher. Après avoir terminé une session, cliquez sur l'icône **Nouvelle identité** de la barre d'outils de Tor Browser (ou ouvrez le menu puis **Nouvelle identité**). Le navigateur ferme alors toutes ses fenêtres et tous ses onglets, efface les cookies et l'historique, puis établit de nouveaux circuits Tor pour les connexions suivantes. Enregistrez préalablement tout travail



en cours : les téléchargements et activités actives seront interrompus. Cette fonction limite les rapprochements avec la session précédente, mais n'efface évidemment pas les informations déjà transmises à un site ou associées à un compte nominatif.

Lien : www.torproject.org

Oui, recycler mes papiers, c'est utile.

Pour l'environnement

Le recyclage des papiers permet **d'économiser les matières premières et l'énergie.**



Le recyclage de papier, c'est :



3 fois moins d'eau*



3 fois moins d'énergie*

* comparé à la fabrication de papier non recyclé

Pour l'emploi

La filière du recyclage des papiers **en France,**
c'est 90 000 emplois non délocalisables.



Collecte



Papeterie



Centre de tri



Découvrez le recyclage du papier
sur www.consignesdetri.fr

CIITEO

Le nouveau nom
d'Eco-Emballages et Ecofolio



PASSKEYS : LA FIN DES MOTS DE PASSE ?

Google, Apple, Microsoft et PayPal proposent de se connecter avec une empreinte, un visage ou le code de l'appareil avec ce système dont vous entendez de plus en plus parler : les passkeys. Ces clés associées à un appareil résistent mieux au phishing, mais comment retrouver ses comptes si le téléphone disparaît ou si l'on change d'écosystème ?

Oublier un mot de passe, le saisir sur une fausse page ou se faire subtiliser ses identifiants : les passkeys promettent de neutraliser ces trois faiblesses. Voici ce qu'elles protègent, où elles sont conservées et comment les adopter sereinement.

LE MOT DE PASSE, UN SECRET TROP FACILE À VOLER

Le mot de passe est un secret connu de l'utilisateur et du site. Il peut donc être trop simple, réutilisé, subtilisé dans une fuite ou capturé par hameçonnage. Ajouter un code reçu par SMS ou généré par une application améliore la protection, mais un faux site peut parfois

relayer immédiatement le mot de passe et le code vers le véritable service. Ni les mots de passe ni les codes temporaires saisis manuellement ne sont, par eux-mêmes, résistants au phishing.

PASSKEY : FINI LE MOT DE PASSE

La passkey — « clé d'accès » dans certaines interfaces — change le principe. L'utilisateur ne transmet plus un mot de passe pour se connecter à tel ou tel service en ligne : il prouve qu'il possède une clé numérique sur son appareil et qui matche avec le compte du service cible. Lors de l'inscription, le téléphone, l'ordinateur ou le gestionnaire génère une paire cryptographique. La clé publique est envoyée



UNE PASSKEY (OU CLÉ D'ACCÈS) EST UNE CLÉ CRYPTOGRAPHIQUE PRIVÉE ASSOCIÉE À UN COMPTE ET À UN APPAREIL. QUAND UN BESOIN D'AUTHENTIFICATION SUR UN SERVICE COMPATIBLE EST DEMANDÉ, PLUS BESOIN DE MOT DE PASSE : LA CLÉ EST RECONNUE ET SEULE SERA DEMANDÉE UNE AUTHENTIFICATION PAR CODE, EMPREINTE DIGITALE OU RECONNAISSANCE FACIALE SELON LE CHOIX DE L'UTILISATEUR.



au service ; la clé privée reste dans l'appareil ou le gestionnaire choisi. À la connexion, votre appareil envoie la signature de sa clé privée, puis le site vérifie sa compatibilité unique avec la clé publique de votre compte. La clé privée n'est donc jamais remise au site et ne peut pas être extraite d'une fuite de sa base d'identifiants. WebAuthn prévoit en outre qu'elle soit liée au service pour lequel elle a été créée.

L'empreinte, Face ID, Windows Hello ou le code PIN ne sont pas la passkey. Mais ils sont indispensables pour autoriser localement son utilisation. Les données biométriques ne sont pas davantage envoyées au site.

Attention : Sur un autre appareil que le vôtre, la clé ne doit pas être enregistrée localement !

TÉLÉPHONE PERDU : LE COMPTE N'EST PAS FORCÉMENT PERDU



Avec une passkey synchronisée, la perte d'un appareil ne supprime normalement pas toutes les clés. Elles peuvent réapparaître sur un nouvel équipement après reconnexion au compte du gestionnaire et validation de ses protections. Google chiffre les passkeys sur



l'appareil avant synchronisation et demande, dans un nouvel environnement, le code du gestionnaire ou celui d'un appareil Android autorisé. Apple annonce un chiffrement de bout en bout du trousseau iCloud et une récupération protégée même si tous les appareils ont été perdus.

Mais le point faible se déplace vers la récupération du compte Google, Apple, Microsoft ou du gestionnaire indépendant. Le NIST relève explicitement que les procédures de récupération du cloud peuvent devenir une faiblesse des passkeys synchronisées.

Si un autre ordinateur est encore connecté, il faut verrouiller ou effacer le téléphone perdu, supprimer sa passkey si elle apparaît séparément, fermer les sessions et enregistrer une nouvelle méthode. Sans autre appareil, adresse de récupération, code de secours ou contact de confiance, l'opération devient beaucoup plus délicate.



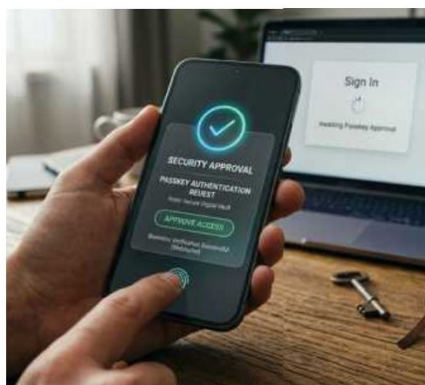
PROTECTION

PAS INFAILLIBLE

Une passkey empêche un faux site ou un voleur opportuniste de récupérer vos identifiants et de les réutiliser pour accéder à votre compte. Mais cela ne rend pas ce dernier invulnérable. Un logiciel malveillant peut encore voler une session déjà ouverte, par exemple son cookie de connexion ; un pirate peut viser la récupération du compte ou profiter d'un téléphone déverrouillé. Les passkeys sécurisent très fortement la connexion, pas tout ce qui se passe avant et après.

AU QUOTIDIEN, UNE CONNEXION PRESQUE INVISIBLE

Sur son propre appareil, l'utilisateur choisit son compte puis valide avec l'empreinte, le visage ou le code de déverrouillage. Google permet ainsi d'accéder à un compte avec le verrouillage de l'appareil ; Apple utilise Face ID, Touch ID ou le code de l'iPhone. Sur l'ordinateur d'un proche ou d'un hôtel, la clé ne doit pas être enregistrée localement. Il faut choisir « Utiliser une passkey depuis un autre appareil » ou une formule équivalente. Un QR code apparaît : on le scanne avec son téléphone, on valide localement, puis celui-ci confirme la connexion.



À SAVOIR

Tous les sites ne proposent pas encore les passkeys et certains conservent le mot de passe. Selon le service, la passkey remplace réellement la connexion et le second facteur, ou n'est qu'une option supplémentaire. Apple confirme qu'une passkey et un mot de passe peuvent coexister pour un même compte.

FAUT-IL LES ADOPTER DÈS MAINTENANT ?

Oui, en priorité pour la messagerie principale, le compte Google, Apple ou Microsoft, le gestionnaire de mots de passe et les services financiers qui les proposent, comme PayPal en France. La passkey protège nettement mieux que le mot de passe contre le phishing et la réutilisation d'identifiants.

L'adoption doit rester progressive, car tous les utilisateurs ne comprendront peut-être pas la logique et le mode de fonctionnement intrinsèque des passkeys (avec le risque de les perdre ou de les laisser fuir). Avant de retirer un ancien moyen de connexion, testez la clé sur deux appareils, vérifiez son gestionnaire, mettez à jour l'adresse et le numéro de récupération, conservez des codes de secours hors ligne et, pour les comptes essentiels, ajoutez une seconde passkey ou une clé physique gardée en lieu sûr.

Les passkeys ne signent donc pas encore la disparition des mots de passe. Elles constituent leur meilleur remplaçant actuel : plus simples et beaucoup plus difficiles à hameçonner, à condition d'organiser sérieusement la récupération. La technologie ferme enfin la porte aux mots de passe volés ; à chacun de ne pas égarer le double des clés.

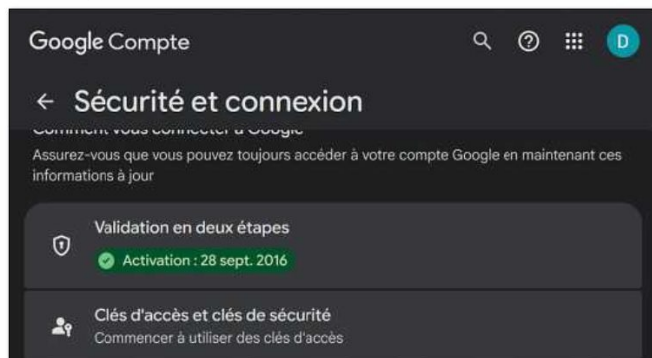
CRÉEZ FACILEMENT UNE PREMIÈRE PASSKEY

PRATIQUE



01 > EXEMPLE AVEC UN COMPTE GOOGLE

Sur un compte Google par exemple, ouvrez **Gérez votre compte Google**, puis **Sécurité et connexion** > **Clés d'accès et clés de sécurité**, validez une nouvelle fois votre mot de passe.



02 > CRÉATION

Cliquez sur **+ Créez une clé d'accès** puis à nouveau sur **Créer une clé d'accès** et **Continuer**. Renseignez enfin votre code d'accès Google. Votre passkey est créée.

Clé d'accès créée

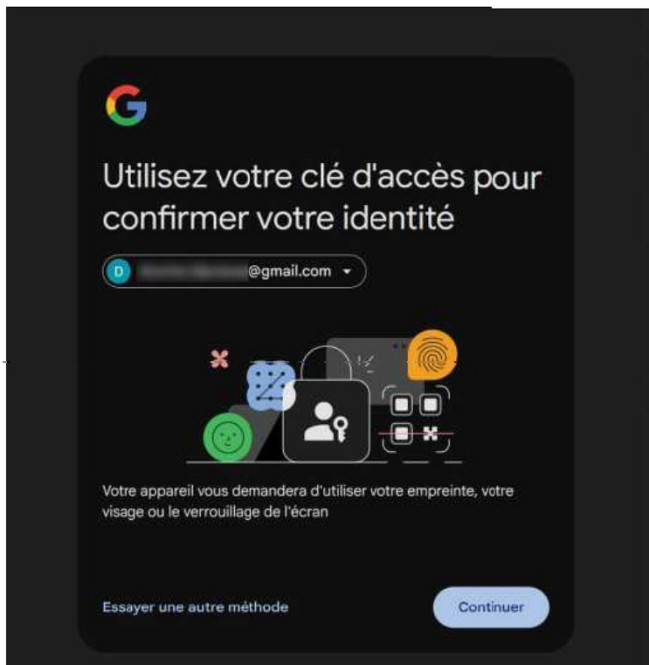
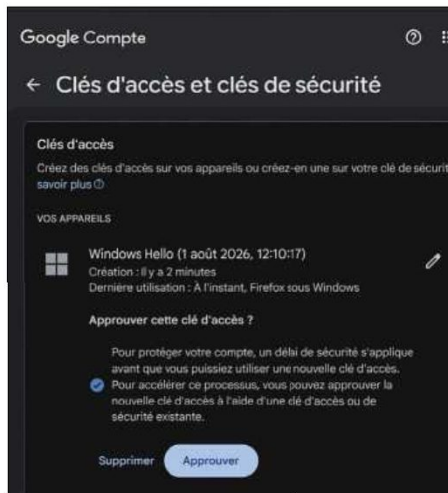


Vous pouvez désormais utiliser votre empreinte, votre visage, le verrouillage de l'écran ou une clé de sécurité physique pour confirmer votre identité lors de la connexion. En savoir plus ⓘ

Terminé

03 > WINDOWS ET GOOGLE

Votre clé d'accès est donc disponible sur votre appareil (ici un PC Windows) et vous devrez utiliser une fois cette passkey avec votre méthode d'accès ou de déverrouillage habituelle pour l'activer définitivement.

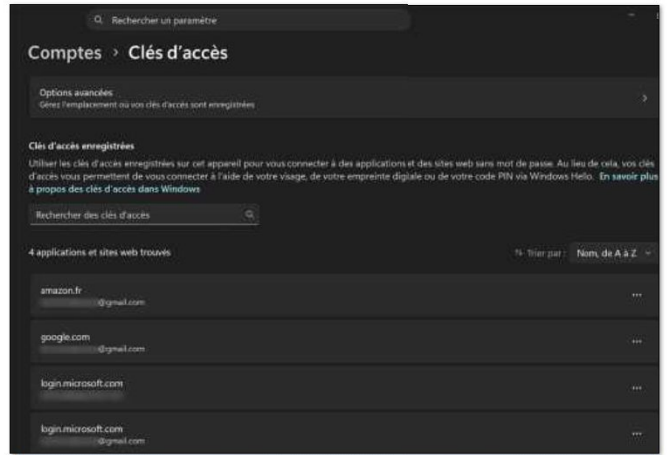


SYNCHRONISÉE OU LIÉE À UN SEUL APPAREIL ?

Une passkey synchronisée est chiffrée puis copiée entre les appareils associés au même gestionnaire. Google Password Manager peut la rendre disponible dans Android et Chrome sur Windows, macOS, Linux ou ChromeOS ; Apple la synchronise dans le trousseau iCloud ; Microsoft propose également ses propres passkeys synchronisées. Une passkey liée à l'appareil reste uniquement sur le PC, le téléphone ou la clé physique où elle a été créée. C'est le cas de certaines clés Windows Hello ou de clés de sécurité FIDO. Si cet appareil disparaît sans autre moyen prévu, la passkey disparaît avec lui.

04 > VÉRIFICATION

Ici, nous avons créé notre passkey sur un PC Windows. Pour vérifier qu'elle est active, allez sur **Paramètres > Comptes > Clés d'accès**. Vous verrez les passkeys locales enregistrées et pourrez le supprimer si besoin dans cet espace.



05 > SYNCHRONISATION

Pour vérifier la synchronisation de cette passkey avec ce compte Google sur votre terminal Android par exemple, allez dans votre compte Google et vérifiez son ajout.





BLOQUEZ LES DOMAINES MALVEILLANTS AVEC NEXTDNS



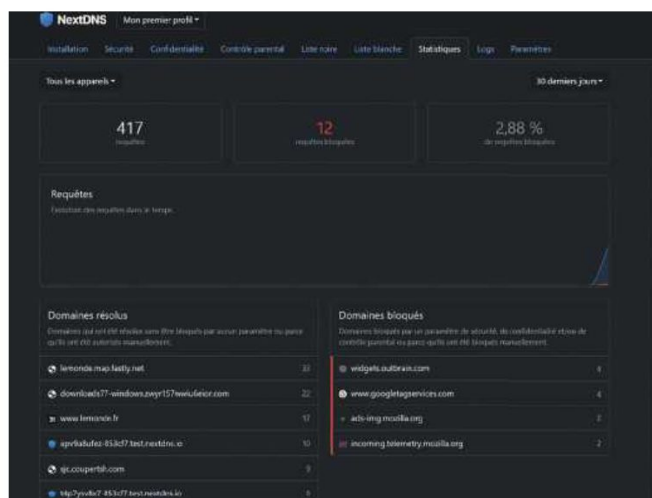
Phishing, malwares, faux sites et cryptojacking peuvent être bloqués avant même leur chargement. NextDNS transforme le DNS du PC en filtre de sécurité personnalisable, actif dans le navigateur comme dans les applications.

Avant d'accéder à un site, l'ordinateur demande à un serveur DNS de traduire son nom (par exemple « monsite.f ») en adresse IP. NextDNS remplace le résolveur habituel du fournisseur d'accès et compare les domaines demandés à différentes sources de renseignement sur les menaces. Lorsqu'une adresse est associée au phishing, à un malware ou à une autre activité dangereuse, sa résolution peut être bloquée avant que le navigateur ou l'application ne s'y connecte.

typosquatting, les noms trompeurs utilisant des caractères ressemblants et les domaines générés automatiquement par certains malwares. Les requêtes peuvent transiter par les protocoles chiffrés DNS-over-HTTPS ou DNS-over-TLS.

OFFRE GRATUITE GÉNÉREUSE

NextDNS bloque principalement des « domaines » : il n'analyse pas en profondeur le contenu d'un fichier téléchargé, ne désinfecte pas Windows et ne remplace donc ni l'antivirus ni la vigilance de l'utilisateur. Son offre gratuite comprend toutes les fonctions et jusqu'à 300 000 requêtes DNS mensuelles. Une fois ce quota dépassé, le service continue de répondre, mais comme un DNS classique dépourvu de filtrage jusqu'au renouvellement du quota.



PLUTÔT QUE DE SIMPLEMENT GÉRER L'ADRESSAGE DNS, NEXTDNS SURVEILLE ET BLOQUE AUSSI EN TEMPS RÉEL LES MENACES SUR INTERNET. UNE BARRIÈRE EFFICACE ET PUISSANTE PLACÉE AVANT LES SITES DANGEREUX.

L'intérêt ne se limite donc pas au Web : NextDNS peut aussi filtrer les connexions d'un logiciel, d'un jeu ou d'une application qui tente de joindre un serveur malveillant. Le service propose notamment des protections contre les domaines de phishing, le cryptojacking, les attaques par

CONTRÔLE PARENTAL

NextDNS propose aussi un module de contrôle parental, simple et complet, à mettre en place. Vous pourrez exclure certains sites Web précis ou des catégories entières (porno, jeux d'argent, réseaux sociaux, streaming, etc.), définir des temps d'usage pendant lesquels certaines de ces catégories ne seront pas bloquées (utile pour les jeux ou les réseaux sociaux par exemple).

La fonction « SafeSearch » filtrera aussi les résultats explicites sur les principaux moteurs de recherche ; vous pouvez même opter pour un mode YouTube restreint et aussi bloquer les méthodes de contournement habituelles (VPN, Tor, DNS chiffrés, etc.).



SÉCURISER WINDOWS AVEC NEXTDNS

PRATIQUE

01 > CRÉEZ VOTRE CONFIGURATION PERSONNELLE

Accédez à NextDNS, puis cliquez sur **Essayer maintenant**.

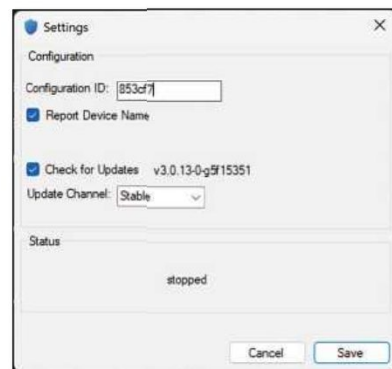
Le service crée immédiatement une configuration personnalisée, sans inscription obligatoire. Créez néanmoins un compte afin de sauvegarder durablement vos réglages. Dans l'onglet **Installation**, repérez ensuite votre **ID** (composé de six caractères) dans **Points de terminaison**. Il permettra de relier le PC aux règles que vous allez définir.

Points de terminaison	
Configurez NextDNS avec cette configuration en utilisant l'un des points de terminaison ci-dessous.	
ID	853cf7
DNS-over-TLS/QUIC	853cf7.dns.nextdns.io
DNS-over-HTTPS	https://dns.nextdns.io/853cf7
IPv6	2a07:a8c0:853cf7 2a07:a8c1:853cf7
Trop compliqué ? Lisez le guide d'installation.	

pratique pendant les premiers jours : ils permettent d'identifier les domaines bloqués et l'appareil qui les a sollicités. Réduisez ensuite leur durée ou désactivez-les si vous privilégiez la confidentialité.

04 > INSTALLER NEXTDNS

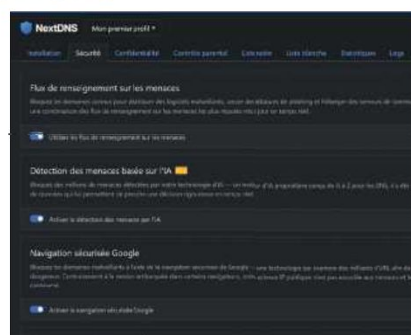
Téléchargez l'application officielle pour Windows depuis les instructions proposées dans l'onglet **Installation** > **NextDNS pour Windows**. Dans la nouvelle fenêtre **Settings**, saisissez votre identifiant de configuration puis **Save**. Cette procédure officielle applique



vos réglages à l'ensemble du PC. Une fois installée, vous retrouverez et pourrez interagir avec NextDNS via son icône dans la zone de notification.

02 > DÉFINIR ET ACTIVER VOS PROTECTIONS

Ouvrez l'onglet **Sécurité** et vérifiez l'activation des **Flux de renseignements sur les menaces**, de la **Détection des menaces basée sur l'IA**, de **Navigation sécurisée Google** et de la protection contre le **Cryptojacking**.

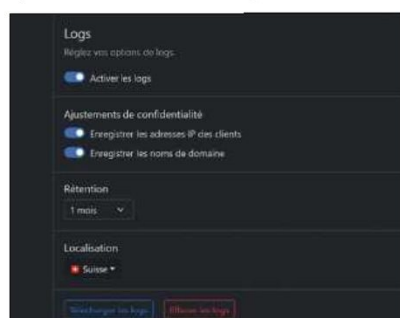


Activez également les défenses contre le **DNS rebinding**, le **Typosquatting**, les **Attaques par homographies IDN** et les **Algorithmes de génération de noms domaines**, utilisés par certains malwares pour contacter leurs serveurs de commande.

03 > RÉGLEZ LA CONFIDENTIALITÉ DES JOURNAUX

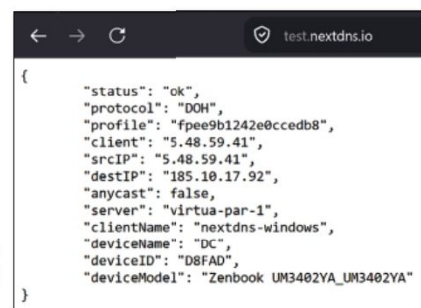
Dans **Paramètres**, choisissez la durée de conservation des journaux et leur emplacement de stockage.

NextDNS permet de sélectionner notamment l'Union européenne, la Suisse, le Royaume-Uni ou les États-Unis, mais aussi de désactiver complètement les journaux. Leur conservation reste



05 > VÉRIFIER SON FONCTIONNEMENT

Revenez enfin sur la page **Installation** de votre compte : elle doit confirmer que l'appareil utilise bien votre configuration. Vous pouvez également ouvrir **test.nextdns.io** ; la valeur **status** : **ok** indique que les requêtes passent



par NextDNS. Consultez ensuite les journaux après quelques minutes de navigation pour vérifier l'apparition des premières requêtes autorisées ou bloquées.

CONSEIL

Dans les options de **Sécurité** à choisir, le blocage des **Domaines nouvellement enregistrés** est plus radical. Il peut stopper des adresses créées précipitamment pour une campagne de phishing, mais aussi empêcher l'accès à un site parfaitement légitime qui vient d'être lancé. Mieux vaut ne l'activer que pour un profil très sécurisé ou lorsqu'un éventuel faux positif ne risque pas de gêner l'utilisation quotidienne.



VÉRIFIER SI UNE EXTENSION PERTURBE FIREFOX AVEC LE MODE DE DÉPANNAGE

PRATIQUE



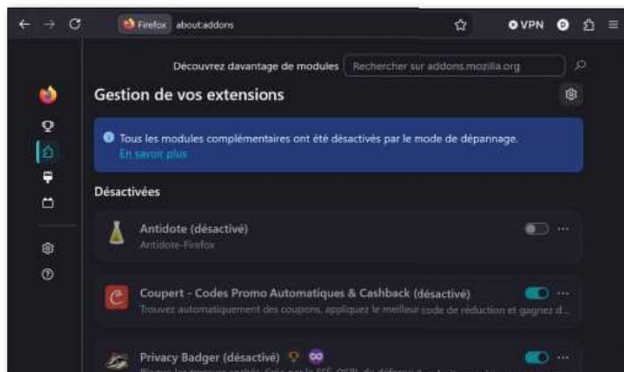
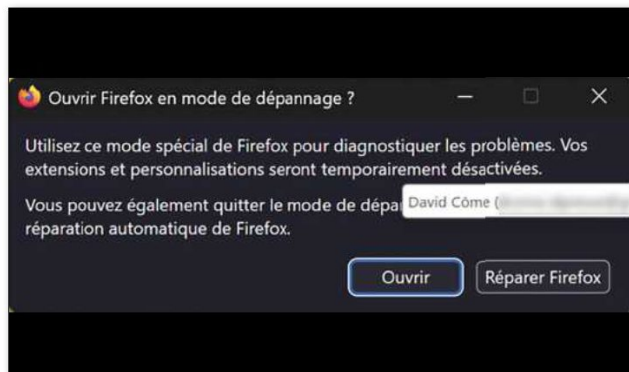
Une extension défectueuse ou devenue incompatible peut ralentir Firefox, provoquer des plantages, modifier l'affichage ou empêcher certains sites de fonctionner.



INFOS [Firefox]

Où le trouver ? [<https://www.firefox.com/fr/>]

Difficulté : 🧑🧑🧑



01> MODE DÉPANNAGE

Ouvrez le menu et passer par **Aide > Mode de dépannage**, puis confirmez avec **Redémarrer** et **Ouvrir**. Si le problème persiste, les extensions ne sont probablement pas responsables ; s'il disparaît, l'une d'elles peut être en cause. Attention, ce mode désactive aussi temporairement le thème personnalisé et l'accélération graphique.

02> TROUVER L'EXTENSION

Redémarrez normalement. Dans la barre d'adresses de Firefox, tapez **about:addons** puis **Entrée**. Désactivez toutes les extensions, puis réactivez-les une par une en testant Firefox après chacune. Supprimez ou remplacez celle qui fait réapparaître le problème.

DÉMASQUER UNE EXTENSION TROP CURIEUSE AVEC GOOGLE CHROME

PRATIQUE



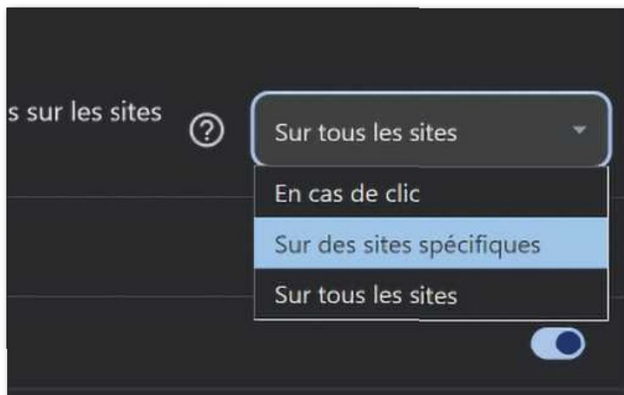
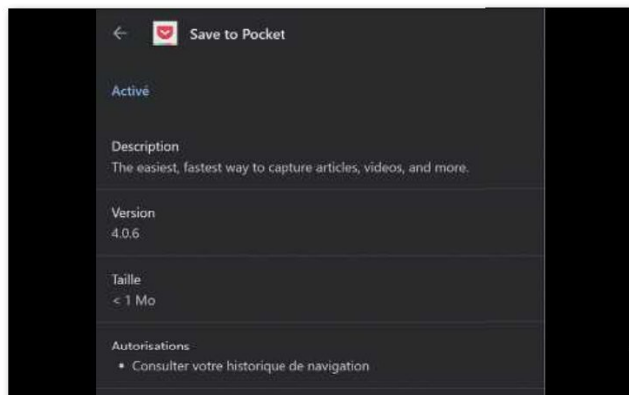
Un convertisseur PDF, un outil de capture ou une extension de coupons n'a pas toujours besoin de lire les données de tous les sites visités.



INFOS [Google Chrome]

Où le trouver ? [www.google.com/chrome/]

Difficulté : 🧑🧑🧑



01> QUELLES AUTORISATIONS ?

Ouvrez le menu et passez par **Extensions** puis cliquez sur **Détails** sous l'extension concernée. Examinez la rubrique **Autorisations**, en particulier son droit de « lire et modifier toutes vos données » : un accès généralisé doit correspondre à une fonction réellement indispensable.

02> REPRENDRE LE CONTRÔLE

Dans **Accès aux sites**, remplacez **Sur tous les sites** par **En cas de clic** ou **Sur des sites spécifiques**. Si les autorisations paraissent disproportionnées ou ne peuvent pas être limitées, revenez à la fiche de l'extension et choisissez **Supprimer**.



COMPRENDRE CE QUE MICROSOFT DEFENDER VIENT DE BLOQUER AVEC L'HISTORIQUE DE PROTECTION

Lorsqu'une notification de Microsoft Defender disparaît trop vite, l'Historique de protection permet de savoir ce qui a réellement été détecté et quelle action a été effectuée ou doit être entreprise.

L'une des fonctionnalités Sécurité Windows de l'application est l'historique de protection, qui fournit une liste complète des actions effectuées par Microsoft Defender Antivirus en votre nom, des applications potentiellement indésirables qui ont été supprimées et des services clés qui sont désactivés.

Les événements sont affichés sous la forme d'une série de « cartes » dans l'historique de protection. Les événements qui nécessitent une attention particulière sont codés en couleur : le rouge indique un élément grave qui nécessite une attention immédiate ; le jaune indique un élément qui n'est pas urgent, mais qui doit être vérifié lorsque vous le pouvez.



01 > ACCÈS À L'HISTORIQUE

Ouvrez **Sécurité Windows**, puis **Historique de protection**. Déployez la carte la plus récente et examinez son intitulé, le fichier concerné, son emplacement et l'action proposée.



- **Menace bloquée** signifie que Defender a déjà empêché et retiré l'élément : aucune action immédiate n'est requise.

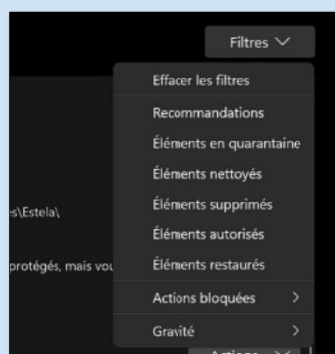
- **Correction incomplète** demande en revanche une intervention supplémentaire, parfois un redémarrage ou une nouvelle analyse.

- Une **Application potentiellement indésirable** n'est pas forcément un virus, mais peut injecter des publicités, modifier le navigateur ou installer d'autres programmes.

02 > COMPRENDRE

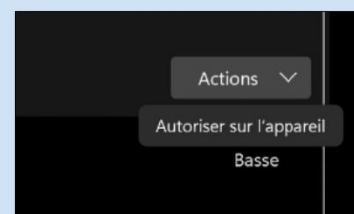
- **Menace détectée – action nécessaire** signifie que Defender attend votre décision : choisissez de préférence **Mettre en quarantaine** si vous avez le moindre doute.

- **Menace mise en quarantaine** indique que le fichier est isolé et neutralisé, mais pas encore supprimé ; vous pouvez alors le supprimer définitivement.



03 > ACTIONS

Via le bouton **Actions**, n'utilisez **Autoriser sur l'appareil** ou **Restaurer** qu'après avoir formellement vérifié qu'il s'agit d'un faux positif auprès de l'éditeur ou d'une source fiable : vous réexposeriez sinon le système. Les alertes rouges sont prioritaires, tandis que les jaunes doivent être examinées.



À SAVOIR

Attention, les événements ne restent affichés que deux semaines et des droits administrateur peuvent être nécessaires pour consulter tous les détails.



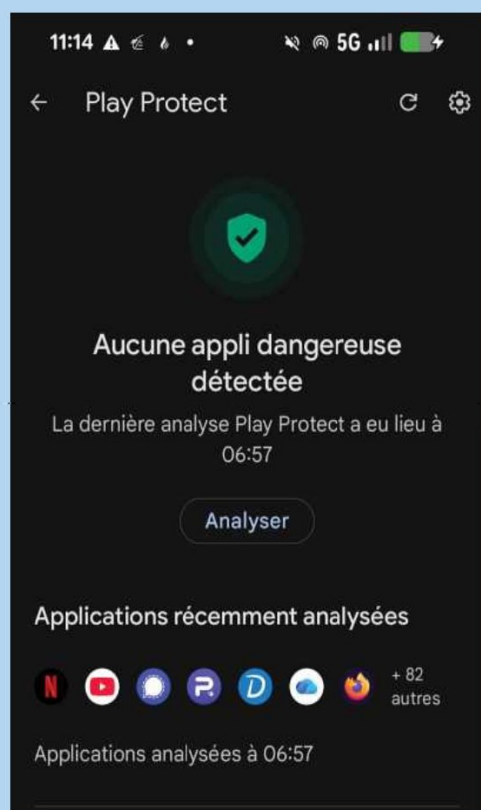


PROTECTION

Vérifier ses applications Android

> AVEC GOOGLE PLAY PROTECT

Google Play Protect contrôle automatiquement les applications installées sur Android, y compris celles provenant d'autres sources que le Play Store ! C'est tout l'intérêt d'utiliser cet outil puissant quand on utilise des applications exotiques ou venant de sources non contrôlées. Pour déclencher immédiatement une vérification, ouvrez

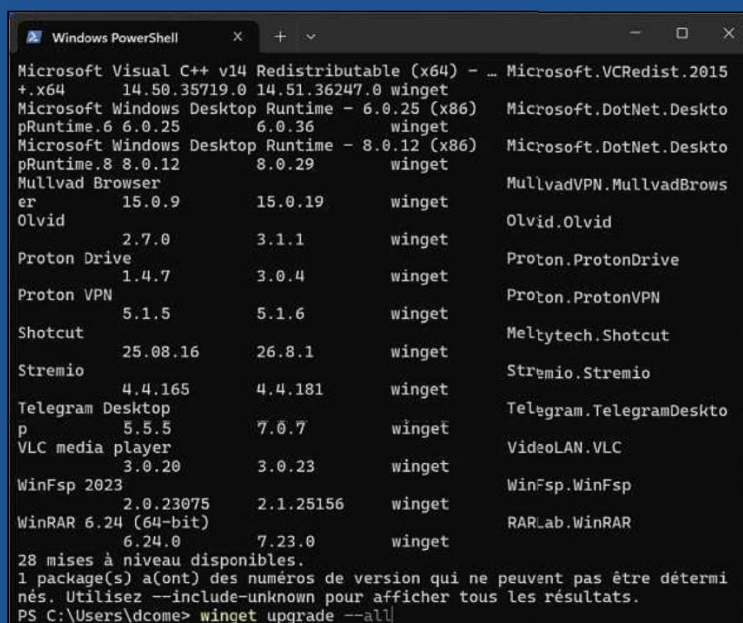


le Play Store, touchez votre photo de profil, puis **Play Protect** et **Analyser**. Le service recherche les applications connues pour adopter un comportement dangereux et peut les signaler, les désactiver ou proposer leur suppression. Cette vérification est particulièrement utile après l'installation d'un APK ou le recours à une boutique alternative. Un résultat rassurant n'est cependant pas un certificat d'innocuité : Play Protect ne détecte pas nécessairement une application trop curieuse, mal conçue ou encore inconnue de Google.

Mettre à jour presque tous ses logiciels

> AVEC WINGET

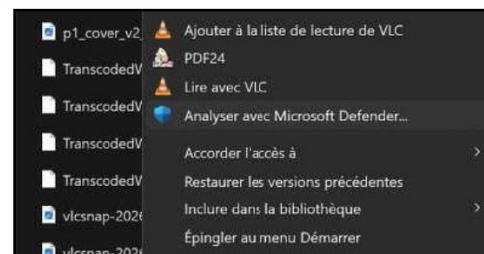
Les mises à jour ne servent pas seulement à ajouter des fonctions : elles corrigent aussi des failles exploitables par des logiciels malveillants. WinGet, le gestionnaire de paquets de Windows, peut actualiser en une seule commande la plupart des applications qu'il reconnaît. Ouvrez **Terminal**, saisissez d'abord **winget upgrade** puis entrée et validez pour afficher les mises à jour disponibles, puis lancez **winget upgrade --all**. Validez les éventuelles demandes d'autorisation et laissez les installateurs travailler. Les logiciels absents du catalogue, épinglés ou dont la version n'est pas détectable peuvent être ignorés : contrôlez donc le bilan final plutôt que de considérer l'opération comme exhaustive.



Analyser un fichier précis

> AVEC MICROSOFT DEFENDER

Une pièce jointe, une archive ZIP ou un exécutable téléchargé vous paraît douteux ? Inutile de lancer immédiatement une analyse complète du PC. Dans l'**Explorateur de fichiers**, effectuez un



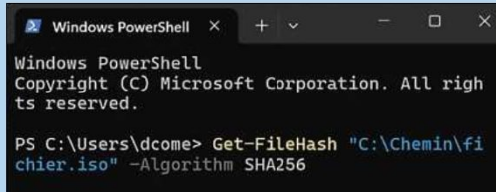
clic droit sur l'élément concerné, choisissez **Afficher d'autres options**, puis **Analyser avec Microsoft Defender**. L'antivirus examine uniquement ce fichier ou ce dossier et affiche son verdict dans **Sécurité Windows**. Cette vérification ciblée est idéale avant d'ouvrir un document reçu par e-mail, de lancer un programme portable ou d'explorer une clé USB. Elle ne remplace toutefois pas une analyse complète si le fichier a déjà été exécuté ou si le PC présente des symptômes suspects.

Vérifier l'intégrité d'une image ISO > AVEC POWERSHELL

Une image ISO ou un utilitaire peut conserver le même nom tout en ayant été altéré. Son empreinte cryptographique permet de vérifier qu'il correspond exactement au fichier publié par l'éditeur. Ouvrez **PowerShell** et exécutez (en remplaçant les termes génériques ci-dessous par les bons disques, chemins d'accès et nom de fichier) :

Get-FileHash «C:\Chemin\fichier.iso» -Algorithm SHA256

Comparez ensuite, caractère par caractère, la valeur affichée avec l'empreinte SHA-256 indiquée sur le site officiel. Si elles diffèrent, ne lancez pas le fichier : le téléchargement peut être incomplet, corrompu ou modifié. Une correspondance confirme son intégrité par rapport à l'empreinte publiée, mais ne prouve pas à elle seule que le programme est sans danger.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\dcome> Get-FileHash "C:\Chemin\fichier.iso" -Algorithm SHA256
```

Générer un rapport des incidents Wi-Fi

> AVEC NETSH

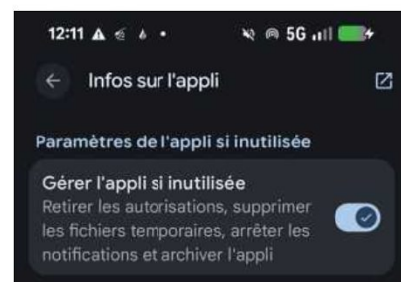
Déconnexions aléatoires, connexion lente ou refus d'authentification : Windows peut produire un rapport détaillé pour comprendre ce qui s'est passé. Recherchez **Invite de commandes** et dans la fenêtre à droite, choisissez **Exécuter en tant qu'administrateur**. Saisissez ensuite **netsh wlan show wlanreport** et validez. Windows génère un fichier HTML dont le chemin apparaît dans le terminal : copiez cette adresse dans l'**Explorateur de fichiers** ou dans votre navigateur. Le rapport regroupe les événements Wi-Fi des trois derniers jours, les sessions réussies ou interrompues, les motifs de déconnexion, les informations sur la carte réseau et la version de son pilote. Dans le graphique récapitulatif, cliquez en priorité sur les cercles rouges : ils signalent les erreurs et renvoient directement vers l'événement correspondant. Les mots de passe Wi-Fi ne sont pas affichés dans le rapport.



Retirer automatiquement les droits d'une application oubliée > AVEC ANDROID

Une application installée pour un voyage, un achat ou un besoin ponctuel peut conserver pendant des mois l'accès à la caméra, au micro, aux contacts ou à la localisation. Android peut neutraliser automatiquement ces privilèges lorsqu'elle reste longtemps inutilisée. Ouvrez **Paramètres** > **Applications**, sélectionnez l'application ou touchez **Afficher toutes les applications** pour la retrouver. Sélectionnez-la puis, dans les infos, activez **Gérer l'appli si inutilisée**.

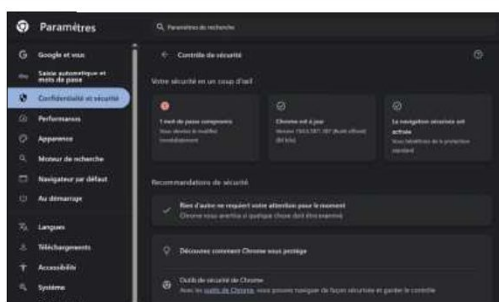
Après une longue période sans ouverture, Android révoquera ses autorisations, interrompra son fonctionnement en arrière-plan, bloquera ses notifications et supprimera certains fichiers temporaires. L'application restera installée et ses droits pourront être demandés de nouveau lors de sa prochaine utilisation. Évitez toutefois cette option pour une application qui doit fonctionner discrètement, comme un outil antivol ou domotique.



Lancer un bilan de sécurité de Chrome

> AVEC LE CONTRÔLE DE SÉCURITÉ

Chrome dispose d'un bilan intégré qui regroupe plusieurs contrôles souvent dispersés : version du navigateur, mots de passe compromis ou trop faibles, extensions potentiellement dangereuses, autorisations de sites inutilisés et notifications abusives. Ouvrez le menu à trois points, puis **Paramètres** > **Confidentialité et sécurité** et cliquez sur **Accéder au contrôle de sécurité**. Sélectionnez chaque alerte pour appliquer la correction proposée : mettre Chrome à jour, supprimer une extension, modifier un mot de passe ou retirer une autorisation. Ce contrôle constitue un tableau de bord préventif, pas un antivirus complet : face à un téléchargement douteux ou à des symptômes inhabituels, complétez-le par une analyse de votre antivirus.





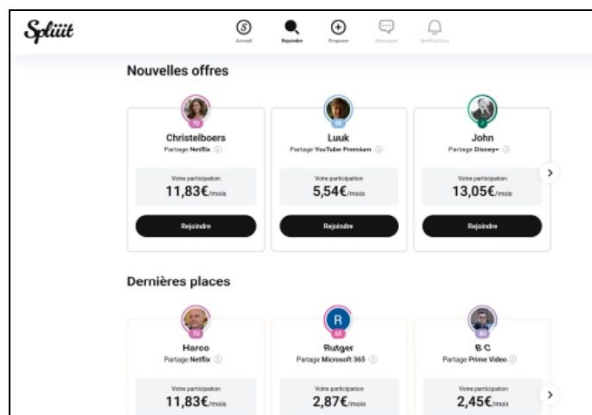
ABONNEMENTS PARTAGÉS :

LES 5 MEILLEURES PLATEFORMES POUR PAYER MOINS CHER

Streaming, musique, jeux vidéo, IA, logiciels ou cloud : le coabonnement permet de diviser une facture entre plusieurs utilisateurs. Mais toutes les plateformes ne se valent pas, et leur utilisation doit rester compatible avec les règles imposées par chaque fournisseur.



Les abonnements numériques s'accumulent facilement : une plateforme vidéo, un espace musical, un espace de stockage, un service bureautique, un VPN... Le coabonnement propose une réponse simple. Le titulaire d'une formule familiale ou multiutilisateur met ses places inutilisées à disposition ; les participants lui remboursent automatiquement leur part par l'intermédiaire d'une plateforme spécialisée.



LES PROPRIÉTAIRES DE COMPTES AVEC DES PLACES DISPONIBLES POUR UN OU PLUSIEURS AUTRES UTILISATEURS PROPOSENT AUX AUTRES MEMBRES DE SPLIIT D'ACHETER UNE PARTIE DE LEUR ABONNEMENT MENSUEL POUR EN PROFITER.



INTELLIGENCE ARTIFICIELLE : RISQUE



ChatGPT, Claude, Gemini, Perplexity et les outils de création assistée par IA figurent désormais parmi les abonnements recherchés sur certaines plateformes de partage. La réduction peut sembler séduisante, car les formules premium coûtent souvent plus cher qu'un service de streaming. Mais un compte d'intelligence artificielle ne se partage pas comme un catalogue de films.

Les conversations, documents importés, images, recherches, projets et préférences peuvent rester enregistrés dans un espace commun. Le véritable abonnement multiutilisateur professionnel constitue la formule la plus saine. ChatGPT Business, Claude Team ou Perplexity Enterprise attribuent un compte ou un siège individuel à chaque membre. Les conversations ne sont pas mélangées comme elles le seraient avec un mot de passe commun, mais ces offres sont conçues pour une organisation et facturent généralement chaque utilisateur. Elles ne correspondent donc pas réellement au coabonnement grand public entre inconnus. Le partage des identifiants d'un compte individuel est également interdit par plusieurs grands fournisseurs. Une plateforme de coabonnement pourra éventuellement rembourser une période d'accès interrompue, mais elle ne restaurera ni les conversations supprimées ni les données confidentielles consultées par un tiers.



Les meilleures solutions gèrent les paiements, les renouvellements, les échanges entre membres et les litiges. Certaines vérifient également les factures du propriétaire ou remboursent les périodes pendant lesquelles le service n'a pas fonctionné.

GESTION VIA LA PLATEFORME POUR PLUS DE SÉCURITÉ

Cette intermédiation ne rend toutefois pas tous les partages automatiquement conformes. Spotify Famille exige, par exemple, que les membres résident à la même adresse. Netflix et Disney+ limitent désormais fortement le partage extérieur au foyer. Avant de rejoindre un groupe d'inconnus, il faut donc vérifier les conditions du fournisseur, privilégier les invitations individuelles et éviter autant que possible de communiquer le mot de passe principal. Généralement, les plateformes que nous vous présentons vous fournissent ces informations et vous aident à faire le(s) bon(s) choix.

QUE SE PASSE-T-IL LORSQUE L'ACCÈS EST COUPÉ ?

Le coabonnement repose sur un intermédiaire de paiement, mais l'accès au service demeure contrôlé par le titulaire

CONSEIL

Mieux vaut privilégier les services qui créent un compte individuel ou envoient une invitation officielle. Le partage d'un mot de passe principal expose davantage les données personnelles, l'historique d'utilisation et les moyens de paiement du titulaire. Il faut également éviter de réutiliser ce mot de passe sur un autre site et activer l'authentification à deux facteurs lorsqu'elle reste compatible avec le partage.

principal. Celui-ci peut résilier son offre, changer son mot de passe, rétrograder vers une formule moins chère ou retirer un participant de son groupe. Le fournisseur peut également bloquer le partage s'il détecte une adresse, un pays ou un foyer ne correspondant pas à ses conditions d'utilisation.

Dans ces situations, les principales plateformes de coabonnement prévoient généralement une procédure de réclamation (lire au sein de chaque descriptif. De manière générale, en cas de litige, n'attendez pas avant de signaler le problème et utilisez exclusivement la messagerie et les outils de réclamation de la plateforme.

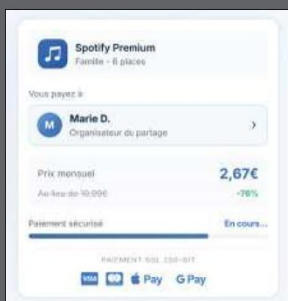
QUE DEVIENNENT LES PROFILS, HISTORIQUES ET RÉFÉRENCES ?



Tout ne disparaît pas nécessairement à la fin du coabonnement. Le résultat dépend entièrement du mode de partage employé.

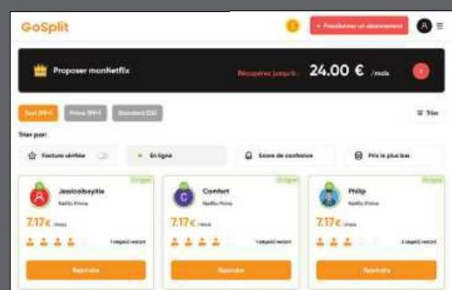
L'INVITATION VERS UN COMPTE PERSONNEL : LE CAS LE PLUS FAVORABLE

Avec Spotify Famille, Google One, Microsoft 365 Famille ou certains abonnements proposant une invitation officielle, chaque membre utilise normalement son propre compte. Ses playlists, documents, fichiers, préférences et historiques restent attachés à ce compte personnel. Lorsqu'il quitte le groupe, il perd seulement les avantages payants ou l'espace mutualisé.



L'ABONNÉ SUPPLÉMENTAIRE : UN COMPTE PLUS FACILEMENT RÉCUPÉRABLE

Certaines offres officielles créent un véritable compte secondaire. Chez Netflix, l'abonné supplémentaire possède son propre identifiant, son propre mot de passe et son propre profil. Si le titulaire principal met fin à l'option, l'accès disparaît, mais l'ancien coabonné peut reprendre un abonnement avec le même identifiant. Netflix indique que ses préférences, favoris et informations de profil peuvent alors être récupérés pendant une période pouvant atteindre 24 mois.



LE PROFIL CRÉÉ DANS LE COMPTE D'UN INCONNU : LE CAS LE PLUS FRAGILE

Lorsqu'un coabonné utilise un simple profil à l'intérieur du compte principal, son historique, ses favoris, ses recommandations et ses réglages demeurent généralement enregistrés dans le compte du propriétaire. À la fin du partage, le participant peut perdre immédiatement l'accès à l'ensemble de ces informations.

LES BONS RÉFLEXES AVANT DE QUITTER UN GROUPE

Avant la fin du coabonnement, il faut vérifier si le service permet de transférer le profil, d'exporter les données, de télécharger les playlists ou de récupérer les fichiers. Il est également préférable d'effacer manuellement l'historique, les recherches et les informations personnelles lorsque le profil reste dans un compte appartenant à un tiers.



NOTRE SÉLECTION POUR DÉNICHER UN ABONNEMENT PARTAGÉ !

SPLIIT > LA RÉFÉRENCE FRANÇAISE LA PLUS COMPLÈTE

Créée en France, Spliit permet soit de partager un abonnement existant, soit de rejoindre la place disponible d'un autre utilisateur. Le propriétaire peut réserver son groupe à ses proches ou le publier sur la place de marché. Le catalogue couvre notamment le streaming, la musique, les jeux vidéo, les logiciels, la presse, le cloud, les VPN et différents services de productivité. L'accès s'effectue, selon l'offre, par invitation dans une famille numérique, création d'un profil ou partage d'identifiants. Les coabonnés paient leur quote-part, augmentée de frais généralement fixés à 5 % plus 0,99 € par paiement. Le propriétaire supporte, pour un partage public, des frais de mise en relation le premier mois, plafonnés à 1 €. Spliit propose une procédure de réclamation lorsqu'un accès n'est pas fourni ou cesse de fonctionner. Sa force réside dans son vaste catalogue, son interface française et sa gestion automatisée.

Lien : www.spliit.com



SHARESUB > LE MEILLEUR ÉQUILIBRE ENTRE SIMPLICITÉ ET PROTECTION

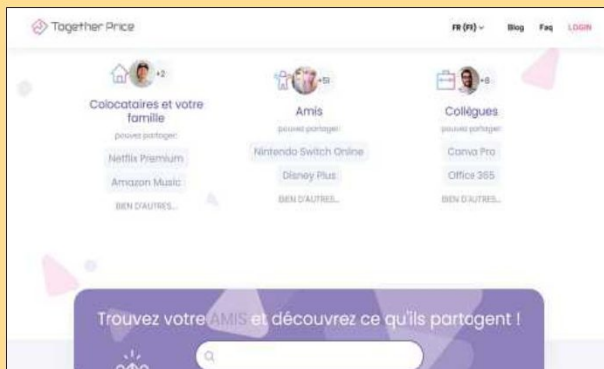
Sharesub constitue le principal concurrent français de Spliit. Le titulaire indique son abonnement, son prix et le nombre de places disponibles ; les participants rejoignent ensuite le groupe par une annonce publique, un partage de proximité ou un lien privé. La plateforme prend en charge le paiement initial au prorata, puis les renouvellements automatiques au premier jour de chaque mois. Les services proposés couvrent la vidéo, la musique, les logiciels, la presse, les jeux, le stockage, les VPN et différents outils professionnels. Le coabonné paie sa part, à laquelle s'ajoutent des frais de traitement annoncés à 5 % plus 0,99 € par règlement. Sharesub dispose d'un programme de protection : en cas d'accès inutilisable, l'utilisateur peut ouvrir une réclamation et obtenir le remboursement de la période concernée. Le support est annoncé comme disponible sept jours sur sept. La plateforme est claire, bien francisée et adaptée aux débutants.

Lien : www.sharesub.com



TOGETHER PRICE – LE PIONNIER INTERNATIONAL

Together Price organise des groupes réunissant un administrateur, qui possède l'abonnement, et plusieurs participants chargés d'en régler une fraction. La plateforme gère les versements mensuels dans un portefeuille numérique, fournit une messagerie interne et utilise un indice de confiance destiné à évaluer la fiabilité des membres. Son catalogue et sa disponibilité varient selon les pays, mais concernent principalement les abonnements familiaux ou multiutilisateurs de streaming, musique, jeux, logiciels et services numériques. Together Price applique des frais de gestion ajoutés à la quote-part ; leur montant dépend du pays, du service et parfois du niveau de confiance de l'utilisateur. Il faut donc



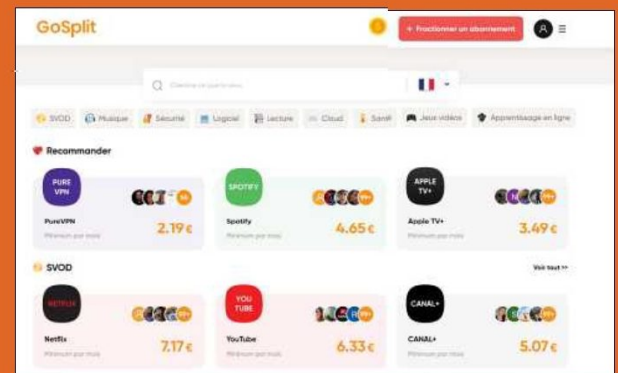
contrôler le total affiché avant de rejoindre un groupe. En cas de difficulté, une demande de remboursement peut être déposée dans les 25 jours suivant le paiement, puis examinée par le support. Together Price bénéficie d'une longue expérience et d'une implantation internationale, mais son interface est moins adaptée au public français et ses frais peuvent rendre les petites participations peu intéressantes.

Lien : www.togetherprice.com

GOSPLIT – UNE PLACE DE MARCHÉ INTERNATIONALE TRÈS DIVERSIFIÉE

GoSplit met en relation des propriétaires d'abonnements et des utilisateurs recherchant une place disponible. Son fonctionnement est proche de Spliit : annonce publique, règlement récurrent, espace de discussion et transmission des informations nécessaires à l'accès. Son catalogue international fait une large place au streaming vidéo, à la musique, aux logiciels, aux outils d'intelligence artificielle, aux VPN, au cloud et aux services de création numérique. Pour le propriétaire, l'utilisation courante est annoncée comme gratuite, mais des frais de mise en relation peuvent être prélevés lors de l'arrivée d'un nouveau participant : ils correspondent notamment à 25 % de la première quote-part, dans la limite de 1 €. GoSplit affiche un programme de protection couvrant les accès non délivrés, interrompus ou différents de l'offre annoncée. Certaines procédures passent néanmoins d'abord par une négociation avec le propriétaire et par le portefeuille interne. La plateforme séduit par son choix et ses tarifs, mais son environnement principalement anglophone et la présence d'offres géolocalisées exigent davantage de vigilance.

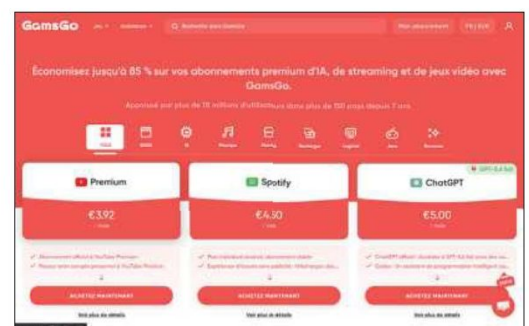
Lien : www.gosplit.com



GAMSGO – LE SPÉCIALISTE DES ACCÈS PRÉCONFIGURÉS À BAS PRIX

GamsGo diffère des quatre plateformes précédentes. L'utilisateur ne rejoint pas nécessairement le groupe familial personnel d'un particulier : il achète souvent un accès préparé par la plateforme ou par un vendeur de sa place de marché. Les offres concernent principalement le streaming, la musique, les outils d'intelligence artificielle, les logiciels créatifs, les VPN et certains services éducatifs. L'accès peut prendre la forme d'un compte partagé, d'un profil réservé, d'une invitation ou d'identifiants préconfigurés. Les prix sont généralement affichés pour plusieurs mois et peuvent être nettement inférieurs aux tarifs officiels, sans commission mensuelle distincte toujours visible. GamsGo prévoit une assistance et des remboursements lorsque le service n'est pas livré, ne correspond pas à la description ou cesse de fonctionner durant sa période de garantie. En revanche, les ventes sont normalement définitives hors de ces situations et la protection disparaît à l'expiration de la garantie. Son principal avantage est le prix ; ses faiblesses sont l'opacité du montage, la dépendance à un compte tiers et un risque plus élevé de coupure ou de non-conformité aux conditions du fournisseur.

Lien : www.gamsgo.com





TOP 7 SITES POUR REJOUER AUX CLASSIQUES DU JEU VIDÉO SUR PC



Doom, Prince of Persia, Commander Keen, Civilization, Wolfenstein 3D ou encore The Oregon Trail peuvent aujourd'hui être lancés dans un simple onglet, sans installer DOSBox ni retrouver un antique PC beige. Voici les sept meilleures ressources encore actives pour replonger gratuitement dans l'âge d'or du jeu sous MS-DOS.



À l'époque de MS-DOS, lancer un jeu relevait parfois déjà du parcours d'obstacles : il fallait modifier des fichiers de configuration, libérer suffisamment de mémoire

conventionnelle et jongler avec les pilotes de la carte son. Quelques décennies plus tard, les mêmes titres peuvent démarrer en quelques secondes dans Firefox, Chrome, Edge ou Safari.

Cette prouesse repose principalement sur des adaptations de l'émulateur star DOSBox, capables de fonctionner dans une page web. L'émulateur reproduit l'environnement des anciens PC tandis que le navigateur exécute le programme localement, sans imposer l'installation d'un logiciel. Certaines plateformes y ajoutent aujourd'hui des commandes tactiles, des



sauvegardes dans le cloud, des favoris ou même des fonctions multijoueurs.

LA MÉMOIRE LUDIQUE N'A PAS D'ÂGE

Toutes ne poursuivent cependant pas le même objectif. Internet Archive privilégie la conservation du patrimoine logiciel. DOS Games Archive et DOSGames.com mettent en avant les freeware, shareware et jeux dont la diffusion gratuite est autorisée. DOS Zone et Best DOS Games modernisent l'expérience, tandis que ClassicReload donne accès à un vaste musée de l'informatique ancienne.

Une précaution demeure nécessaire : un jeu qualifié d'« abandonware » n'est pas automatiquement libre de droits. Certains éditeurs tolèrent la circulation de titres qu'ils ne commercialisent plus ; d'autres tentent de demander leur retrait.

À SAVOIR

L'émulation en ligne n'est pas toujours parfaite. Certains jeux reconnaissent mal le clavier français, n'enregistrent pas durablement les sauvegardes ou nécessitent une souris virtuelle.

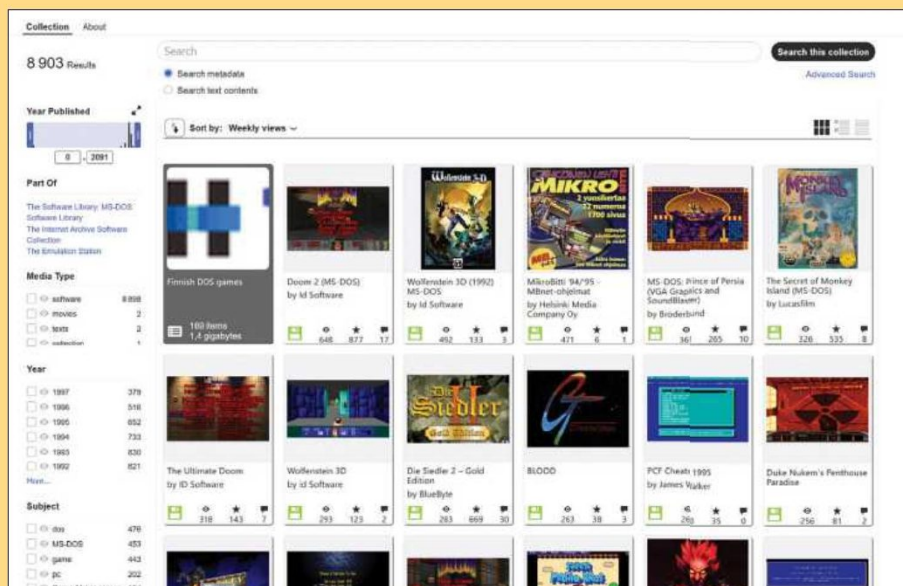
INTERNET ARCHIVE > LE PLUS GRAND MUSÉE INTERACTIF

Internet Archive ne se contente pas de conserver d'anciennes pages web. L'organisation américaine archive également des livres, films, enregistrements, logiciels et systèmes informatiques. Sa bibliothèque MS-DOS rassemble des milliers de programmes et de jeux exécutables dans le navigateur grâce à EM-DOSBox, une adaptation de l'émulateur DOSBox.

La collection permet de retrouver des classiques majeurs, mais aussi des logiciels éducatifs, des sharewares oubliés, des curiosités techniques et différentes éditions d'un même titre. Chaque fiche peut contenir une description, des captures, des informations sur l'éditeur, l'année de publication et les autres plateformes compatibles.

Ultra-complet mais c'est le bazar !

La richesse du fonds constitue aussi sa principale faiblesse. Internet Archive ressemble davantage à un entrepôt patrimonial qu'à une boutique de jeux : les doublons sont fréquents, les classements parfois confus



et certaines configurations fonctionnent moins bien que d'autres. Internet Archive demeure néanmoins la meilleure destination pour rechercher un titre précis ou explorer des pans méconnus de l'histoire du PC. Son absence de logique commerciale et sa mission de conservation lui donnent une place à part dans cette sélection.

Lien : https://archive.org/details/softwarelibrary_msdos_games

DOS ZONE > L'EXPÉRIENCE LA PLUS SÉDUISANTE

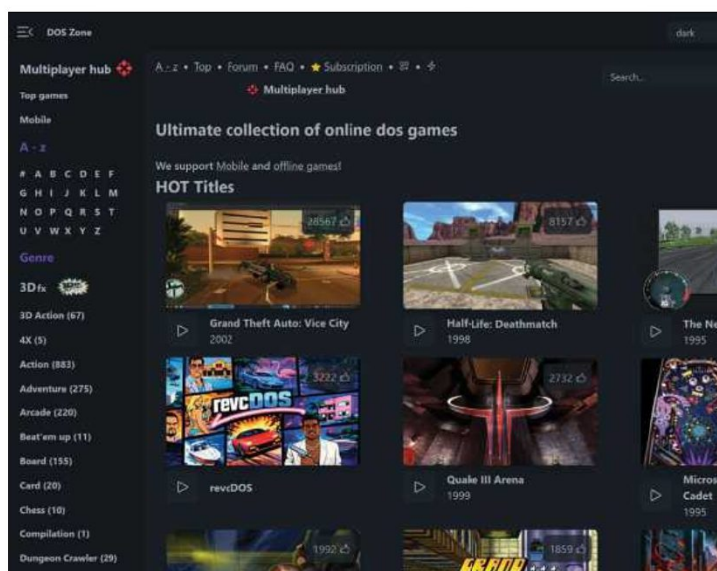
DOS Zone transforme l'émulation DOS en véritable plateforme de jeux en ligne. Son interface illustrée, ses catégories et son moteur de recherche rendent la navigation beaucoup plus immédiate que dans les archives traditionnelles. Le portail de l'écosystème js-dos réunit désormais environ 2000 jeux.

Du vieux dans une interface moderne

Le service repose sur js-dos, une technologie qui prévoit notamment la sauvegarde et le chargement des parties, la diffusion progressive des disques volumineux, la prise en charge du mobile et des fonctions multijoueurs. Les commandes virtuelles facilitent l'utilisation sur smartphone ou tablette, même si les jeux conçus pour le clavier et la souris restent généralement plus agréables sur un ordinateur.

Le catalogue peut toutefois inclure des œuvres dont la disponibilité dépend de la tolérance des ayants droit. Certains titres sont donc susceptibles de disparaître.

Lien : <https://dos.zone/>





DOS GAMES ARCHIVE > LE PLUS RIGOUREUX SUR LES LICENCES

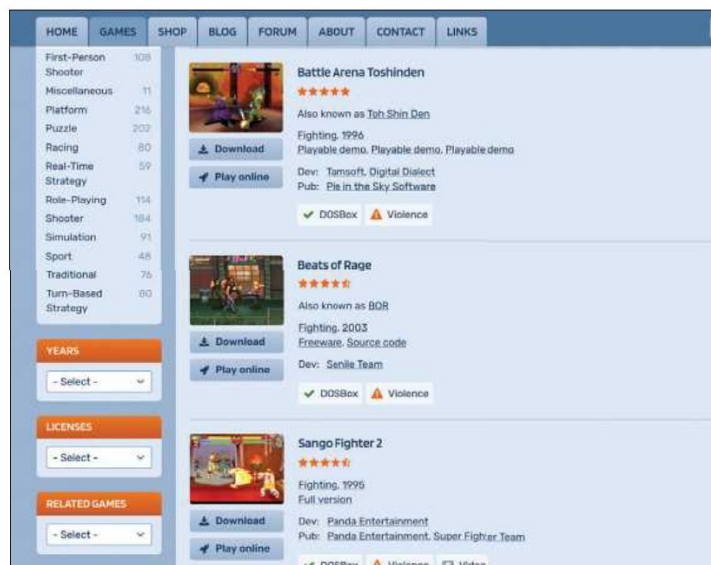
DOS Games Archive adopte une ligne éditoriale plus prudente que les grands sites d'abandonware. Son catalogue rassemble principalement des jeux shareware, freeware, open source, des démonstrations et des titres officiellement diffusés gratuitement. Les fiches permettent de filtrer les jeux par genre, année et type de licence. Le site recense notamment plus de 200 jeux de plateforme, environ 200 jeux de réflexion et plus d'une centaine de jeux de tir à la première personne.

Clair, précis, incorruptible

Chaque page fournit généralement l'année, le développeur, le genre, la licence, des captures, des liens documentaires et les fichiers disponibles. Une mention indique clairement lorsqu'un titre peut être lancé dans le navigateur.

Cette rigueur a une contrepartie : plusieurs grands jeux commerciaux des années 1990 ne sont proposés qu'en version shareware ou ne figurent pas du tout au catalogue.

Lien : www.dosgamesarchive.com



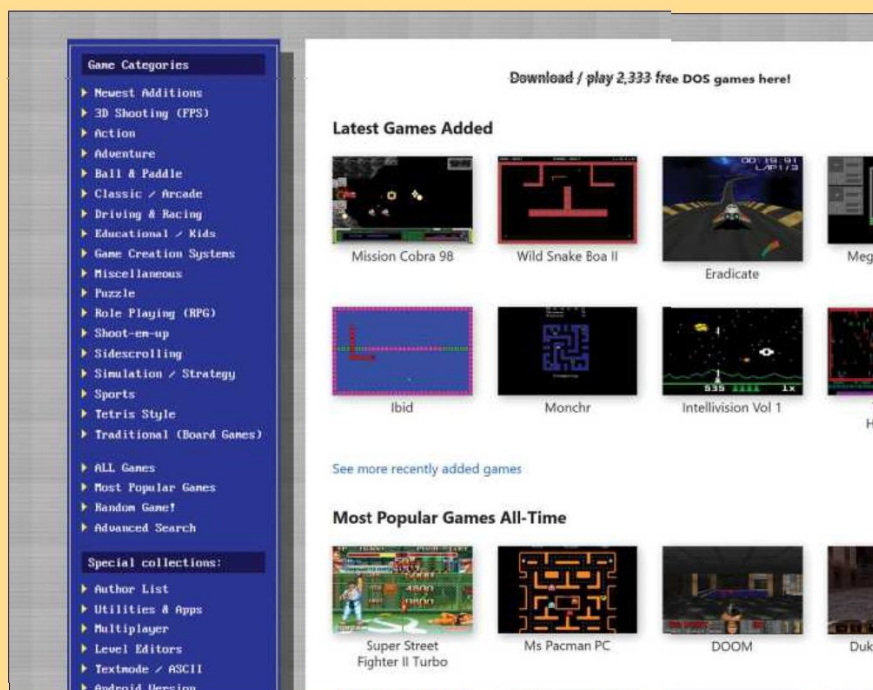
DOSGAMES.COM > LE MIEUX DOCUMENTÉ

Présent en ligne depuis plus de vingt-cinq ans, DOSGames.com fait figure de vétéran. Le site revendique plus de 2 000 jeux et défend une politique claire : proposer des freeware, shareware, créations du domaine public et autres programmes légalement distribuables, sans se transformer en dépôt généraliste d'abandonware.

Une partie importante du catalogue est jouable directement dans le navigateur. Les autres titres peuvent être téléchargés, accompagnés d'instructions pour les faire fonctionner avec DOSBox. L'inscription n'est pas obligatoire pour parcourir le site ou lancer les jeux compatibles.

Une mère DOS y retrouverait ses dosettes

DOSGames.com se distingue surtout par la qualité de ses fiches. Elles présentent le genre, l'auteur, la licence, les possibilités multijoueurs, les caractéristiques graphiques et une appréciation éditoriale. Les descriptions ne se contentent pas de recopier un argumentaire : elles expliquent les qualités, les défauts et parfois les bizarreries du titre.



L'interface porte visuellement le poids de son âge et tous les jeux ne disposent pas d'un lancement en ligne. Le site reste néanmoins excellent pour comprendre ce que l'on s'appête à lancer, retrouver les commandes et découvrir des productions freeware moins connues.

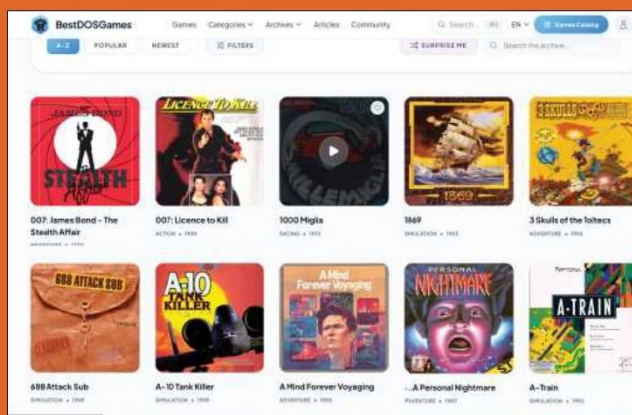
Lien : www.dosgames.com

BEST DOS GAMES > LE PLUS COMMUNAUTAIRE

Lancé en 2023, Best DOS Games apporte aux classiques du PC les fonctions que l'on attend aujourd'hui d'une plateforme de jeu : comptes personnels, favoris, historique, classement communautaire et sauvegardes à distance. Le site permet de parcourir son catalogue par popularité, genre, année, éditeur ou développeur.

L'envie d'y revenir

Son principal avantage réside dans la possibilité d'enregistrer l'état d'une partie dans le cloud. Cette fonction change réellement l'intérêt de l'émulation en ligne pour les jeux de rôle, de gestion ou de stratégie, qui nécessitent plusieurs sessions. Des profils publics et des badges valorisent également le temps de jeu, les séries de connexions et les sauvegardes réalisées. Le catalogue dépassait 900 titres au printemps 2026 et la plateforme revendiquait environ 50 000 joueurs. Son interface claire, ses sauvegardes et sa



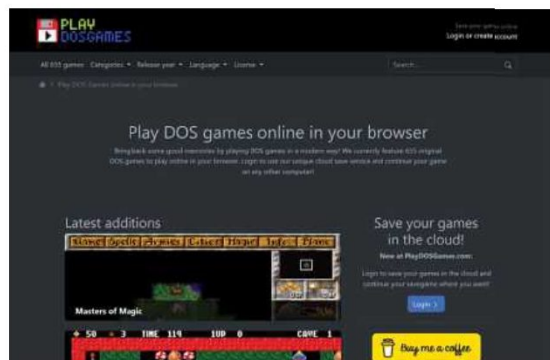
dimension communautaire en font l'une des meilleures portes d'entrée pour jouer régulièrement plutôt que simplement tester un vieux titre pendant cinq minutes.

Lien : <https://bestdosgames.com/>

PLAYDOSGAMES.COM > LE MEILLEUR POUR REPRENDRE SA PARTIE

PlayDOSGames.com se concentre sur une promesse simple : lancer rapidement un jeu DOS dans le navigateur et pouvoir le retrouver plus tard. Son catalogue comptait environ 700 jeux lors de notre vérification. Le site possède donc moins de titres que les plus grandes archives, mais sa navigation est claire et les jeux sont immédiatement accessibles par catégories, nouveautés ou popularité. Sa fonction distinctive est la sauvegarde dans le cloud. Une fois connecté, le joueur effectue une sauvegarde dans le jeu, puis utilise le bouton prévu par la plateforme pour transférer cet état sur son compte et le récupérer depuis un autre appareil. Cette fonction convient particulièrement aux jeux d'aventure, de rôle et de stratégie. L'inscription devient donc presque indispensable pour profiter du véritable avantage de la plateforme.

Lien : www.playdosgames.com



CLASSICRELOAD > LE PLUS VASTE AU-DELÀ DES SEULS JEUX DOS

ClassicReload est moins un catalogue spécialisé qu'un musée interactif de l'informatique personnelle. Le site annonce plus de 6 000 jeux rétro, logiciels, systèmes et anciennes interfaces accessibles à des fins de conservation, d'éducation et de recherche. Une importante section est consacrée à DOS, avec lancement direct dans le navigateur.

Toute la culture rétro

On y croise des jeux d'action, d'aventure, de réflexion ou de gestion, mais aussi d'anciens programmes Windows, des logiciels éducatifs et des environnements historiques. Cette diversité constitue sa grande originalité : ClassicReload permet autant de rejouer que d'explorer la manière



dont fonctionnaient les ordinateurs d'autrefois. Le catalogue DOS est particulièrement profond, avec de nombreux titres connus et une multitude de productions oubliées. Les fiches proposent généralement une description, l'année, la plateforme, des commandes et une fenêtre d'émulation. Certains jeux peuvent aussi être téléchargés. L'interface est chargée, la publicité peut gêner la navigation et certaines pages sont nettement mieux documentées que d'autres.

Lien : <https://classicreload.com>



TOP 15

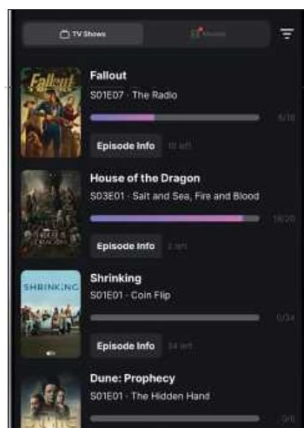
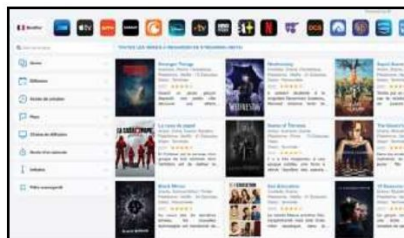
Logiciels & services GRATUITS

TOP5 SERVICES POUR SUIVRE FILMS ET SÉRIES

BETASERIES > LE MEILLEUR POUR LES FRANCOPHONES

Ce service français permet de suivre sa progression épisode par épisode, de gérer les séries en cours, de recevoir des recommandations et de consulter un calendrier personnalisé. Films et séries peuvent être notés et commentés et il comprend bien sûr toutes les indications sur les plateformes de diffusion.

Lien : www.betaseries.com

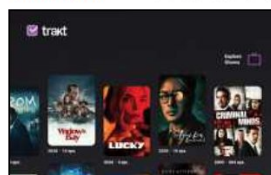


HOBİ > LE PLUS SIMPLE SUR SMARTPHONE

Chaque épisode peut être marqué comme vu en un geste, tandis qu'une frise présente les prochains retours de saisons et dates de diffusion. L'application gère séries et films, propose des rappels, des statistiques et un journal de visionnage. Disponible gratuitement sur Android et iOS, elle peut aussi synchroniser ses données avec Trakt.

Lien : <https://hobiapp.com>

TRAKT — LE PLUS PUISSANT ET LE PLUS OUVERT



Trakt est la solution des utilisateurs exigeants. Il suit films, séries et épisodes, organise les programmes en listes, affiche les prochaines sorties et formule des recommandations. Sa grande force réside dans son écosystème : son API alimente de nombreuses applications et permet des synchronisations avec des lecteurs ou médiathèques compatibles.

Lien : <https://trakt.tv/>

SIMKL > LE MEILLEUR POUR LES SÉRIES ET LES ANIMÉS

Simkl réunit dans un même compte les séries télévisées, les films et une base particulièrement riche consacrée aux animés. Le service enregistre les épisodes vus, signale ceux qui restent à regarder, propose un calendrier, des alertes, des listes et des recommandations personnalisées.

Lien : <https://simkl.com/>



JUSTWATCH > LE MEILLEUR POUR TROUVER OÙ REGARDER

JustWatch est moins communautaire mais imbattable pour savoir où un film ou une série est légalement disponible en France. L'utilisateur sélectionne ses abonnements, recherche une œuvre, puis compare les offres de streaming, de location et d'achat. Il peut également créer une liste personnelle, marquer des titres comme vus et suivre les nouveautés.

Lien : www.justwatch.com/fr/



TOP5 APPLICATIONS ANDROID POUR CACHER SES MÉDIAS

GOOGLE PHOTOS > LE DOSSIER VERROUILLÉ LE PLUS ACCESSIBLE

Déjà installé sur de nombreux smartphones, Google Photos permet de déplacer photos et vidéos sensibles dans un Dossier verrouillé. Les éléments disparaissent de la galerie, des souvenirs, des recherches et des applications tierces. La sauvegarde chiffrée sur le compte Google reste facultative.

Lien : urlr.me/QNZDyp



DOSSIER SÉCURISÉ SAMSUNG > LE MIEUX INTÉGRÉ AUX GALAXY

Réservé aux appareils Samsung compatibles, le Dossier sécurisé crée un espace séparé protégé par Samsung Knox. Photos, vidéos, fichiers et même applications peuvent y être placés, puis verrouillés par code, mot de passe ou biométrie. Les données sont chiffrées et l'icône du coffre peut être masquée.

Lien : urlr.me/uMygFZ



TOP5 POUR ALLER PLUS LOIN AVEC TOR BROWSER

TOR EXPERT BUNDLE > POUR CONNECTER D'AUTRES LOGICIELS À TOR

Destiné aux utilisateurs avertis, le Tor Expert Bundle installe le moteur Tor sans navigateur. Il permet de faire transiter par Tor les applications compatibles avec un proxy SOCKS, à condition de les configurer correctement. Plus flexible qu'un navigateur prêt à l'emploi, il demande aussi davantage de précautions.

Lien : www.torproject.org

ONIONSHARE > PARTAGER DES FICHIERS SANS INTERMÉDIAIRE

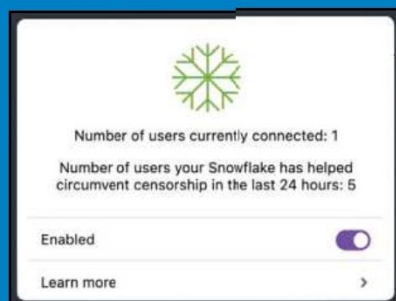


OnionShare permet d'envoyer ou de recevoir des fichiers directement par Tor, sans les confier à Google Drive ou WeTransfer. Il peut aussi héberger un petit site ou ouvrir un espace de discussion. Le destinataire reçoit une adresse secrète à ouvrir avec Tor. Gratuit et open source, il ne nécessite aucun compte.

Lien : <https://onionshare.org/>

SNOWFLAKE > CONTOURNER LE BLOCAGE DE TOR

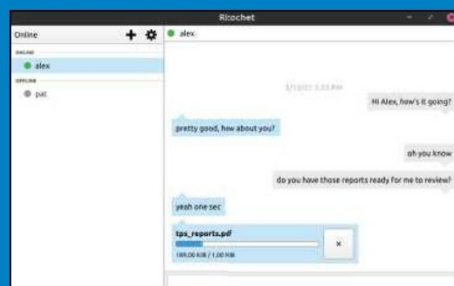
Snowflake aide les internautes situés sur un réseau censuré à rejoindre Tor par l'intermédiaire de proxys temporaires fournis par des volontaires. Le trafic ressemble davantage à une communication WebRTC ordinaire, ce qui complique son blocage.



Lien : <https://snowflake.torproject.org/>

RICOCHET REFRESH > DISCUTER SANS COMPTE NI SERVEUR CENTRAL

Ricochet Refresh est une messagerie instantanée gratuite qui établit les conversations au moyen de services onion. Aucun numéro de téléphone, e-mail ou



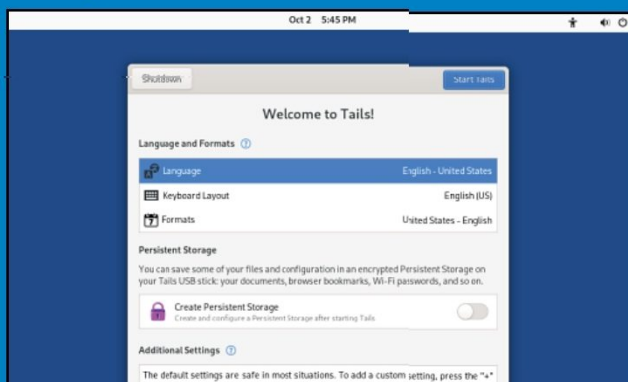
serveur central classique n'est nécessaire : chaque utilisateur communique à partir d'une adresse Ricochet. L'application propose un installateur Windows ainsi qu'une version portable.

Lien : www.ricochetrefresh.net

TAILS > ISOLER TOUT SON ENVIRONNEMENT TOR

Tails démarre votre PC depuis une clé USB à la place de Windows et achemine les connexions par Tor. Cet OS portable contient sa propre suite logicielle. Il est plus contraignant mais, une fois la clé USB retirée, plus aucune trace de ce que vous avez opéré sur PC ne subsiste.

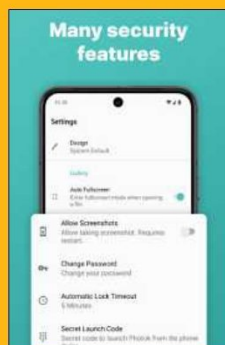
Lien : <https://tails.net/install/windows/>



PHOTOK > LE MEILLEUR COFFRE OPEN SOURCE

Photok chiffre localement les photos et vidéos avec AES-256 et ne nécessite ni compte, ni cloud, ni adresse électronique. Les fichiers ne sont déchiffrés qu'en mémoire pendant leur consultation. Gratuite, open source et disponible en français !

Lien : urlr.me/VhHMcF



LOCKMYPPIX > LE COFFRE LE PLUS RICHE EN FONCTIONS

Elle protège photos, vidéos et documents dans un coffre utilisant un chiffrement AES-CTR. L'accès peut être verrouillé par mot de passe, code PIN, schéma, empreinte ou reconnaissance faciale. La version gratuite couvre le stockage local et les fonctions essentielles, tandis que certains outils avancés sont payants.

Lien : <https://lockmypix.com/>



1GALLERY > LA GALERIE COMPLÈTE AVEC COFFRE INTÉGRÉ

1Gallery remplace la galerie habituelle tout en proposant un espace sécurisé. Les fichiers cachés sont chiffrés et accessibles par code, schéma ou empreinte digitale. L'application conserve une navigation classique par albums et dispose d'une interface française. Certaines options nécessitent la formule Premium.

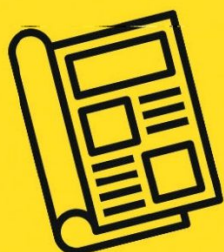
Lien : urlr.me/HegQ6k





PIRATE

INFORMATIQUE



JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON
MARCHAND DE JOURNAUX

Directéditeurs

LES DOSSIERS DU **Pirate**

DES DOSSIERS
THÉMATIQUES
COMPLETS

À DÉCOUVRIR
EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ
D'ASTUCES



SPÉCIAL
ANDROID



Actuellement #Guide pratique

ROOT ANDROID

E-MAILS

YGGTORRENT

IPTV

VPN GRATUIT

MATÉRIEL ESPION

DNS FACILES



PIRATE
INFORMATIQUE



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