

100%
PRATIQUE

[JEUX VIDÉO]
Hacks & fun !

[MULTIMÉDIA]
Stream & Télécharger

[NOUVEAU]
Découvrez Tails 6.0

LES DOSSIERS DU **Pirate** **LA BIBLE** **DU HACKER**

3⁹⁰€
seulement

0%
PUBLICITÉ

LES 145 MEILLEURS OUTILS
100 % PIRATES  **100 % GRATUITS**

BEST-OF
2024

ANONYMAT

PC & WEB :
Les VRAIES
SOLUTIONS !

+ BEST-OF

HACKING
& CRACK
de MOTS DE PASSE !





SOMMAIRE

EN PARTENARIAT
AVEC

LES CAHIERS DU HACKER
PIRATE
[INFORMATIQUE]

➤ HACKING

p.6
TOP 20 > Logiciels
GRATUITS mais pros !

p.16
TOP 5 > Crack de
MOTS DE PASSE

p.18
TOUT SAVOIR
sur les
ATTQUES DDoS :
- Comment font les pirates
- Quels logiciels utilisés ?



➤ ANONYMAT & PROTECTION

p.28
TOP 5 > NAVIGATEURS qui
protègent vraiment vos données

p.30
TOP 3 > MESSAGERIES
vraiment sécurisées

p.32
TOP 10 > EXTENSIONS
pour FIREFOX

p.38
TOP 5 > Logiciels
de CHIFFREMENT

p.40
DOSSIER
TAILS anonymise votre PC
+ TOP 5 > ALTERNATIVES à Tails

p.48
TOP 5 > ANTIMALWARES
sur ANDROID



➤ MULTIMÉDIA

p.52
TOP 5 > TÉLÉCHARGER sur YOUTUBE

p.54
TOP 3 > CAPTUREZ du STREAM en DIRECT

p.57
TOP 3 > Clients TORRENTS



p.58

TOP 5 > MEDIACENTERS

p.60

TOP 5 > Trouver de la MUSIQUE
LIBRE DE DROIT

▼ TROUSSE À OUTILS

p.64

TOP 5 >
RECONNAISSANCE
FACIALE



p.67

TOP 3 >
Trouver des logiciels OPEN SOURCE

p.68

TOP 5 > RÉCUPÉRATEURS de fichiers

p.70

Inclassables... mais indispensables :
Les MEILLEURS LOGICIELS
& SERVICES !

p.78

TOP 5 > SE FORMER
en CYBERSÉCURITÉ & HACKING

▼ BONUS JEUX VIDÉO

p.82

RÉTROGAMING :
TOP 10 UTILITAIRES et
ÉMULATEURS de jeux pour PC



p.88

TOP 5 > ÉMULATEURS ANDROID

p.90

L'arsenal des tricheurs :
11 TECHNIQUES AU CRIBLE

LES DOSSIERS DU Pirate

N°38 – Avril / Juin 2024

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

Directeur de la publication :
David Côme

Maquettiste :
Sergei Afanasiuk

Imprimé en France par
/ Printed in France by :

Mordacq Impression
Rue de Constantinople
62120 Aire-sur-la-Lys

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours
ISSN : 2267-6295

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

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.

CHEZ VOTRE
MARCHAND DE JOURNAUX
**LES PIRATES CRYPTENT,
NOS LECTEURS DÉCRYPTENT !**

HACKING

ANTI-CENSURE

FILMS & SÉRIES

MOBILE

PROTECTION

ANONYMAT

CONFIDENTIELS

MOTS
DE PASSE

SURVEILLANCE

LA BIBLE
DU PIRATE
4,90 €
SEULEMENT !

N°59 # Casser les codes et décrypter l'info #

PIRATE
INFORMATIQUE

Février / Avril 2014

HACKING
TOUT SAVOIR SUR
LES **ATTAQUES DDOS**

**BEST of
2024**

HACKING

Les vraies **SOLUTIONS**
GRATUITES

ANONYMAT
ACTIVER
L'ANTI-CENSURE
SUR **TOR**

TOP 5
Les **MESSAGERIES**
qui évitent
VRAIMENT
d'être **SURVEILLÉ**

BLACK DOSSIER
Les meilleurs
VPN
AU BANC D'ESSAI

VPN
Le GUIDE 2024

ALIAS
CHANGEZ
D'IDENTITÉ
AVEC **ANONADDY**

HACKING





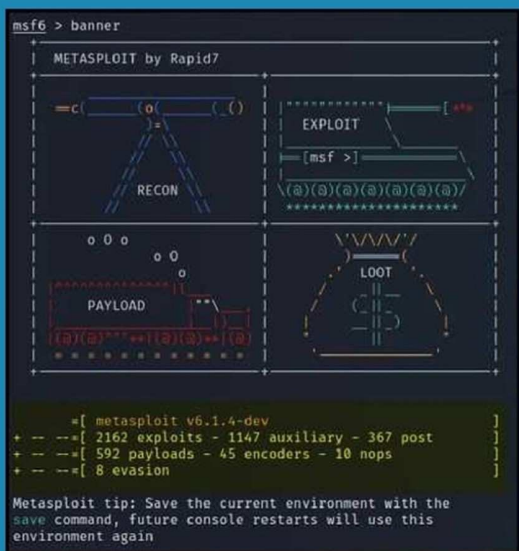
TOP 20 LOGICIELS GRATUITS... MAIS PROS !



> MULTI-INTRUSION

Metasploit fournit une suite complète d'outils. Cela inclut une vaste base de données d'exploits et de vulnérabilités connus pour aider à identifier les faiblesses d'un système cible. Son interface conviviale est idéale pour développer et exécuter des exploits. Idéal également pour les modules auxiliaires qui effectuent des tâches telles que la prise d'empreintes digitales, la reconnaissance et l'analyse des vulnérabilités. Metasploit s'intègre à d'autres outils et frameworks, tels que Nmap et Burp Suite. Il fournit une suite complète de fonct

Lien : www.metasploit.com



ZAP > ANALYSE DES VULNÉRABILITÉ D'UN SERVICE

ZAP (Zed Attack Proxy) est un outil de test de sécurité d'application Web polyvalent qui analyse les réponses reçues d'une application Web cible. Il peut identifier les vulnérabilités potentielles, notamment les attaques par injection

SQL, cross-site scripting (XSS) et par débordement de tampon. Il prend en charge les analyses passives et actives. De plus, il dispose d'une interface graphique facile à utiliser, d'un proxy d'interception, de scanners automatisés et d'une variété de plug-ins. Comme Nmap, ZAP fonctionne sur plusieurs plateformes.

Lien : www.zaproxy.org



WPSCAN

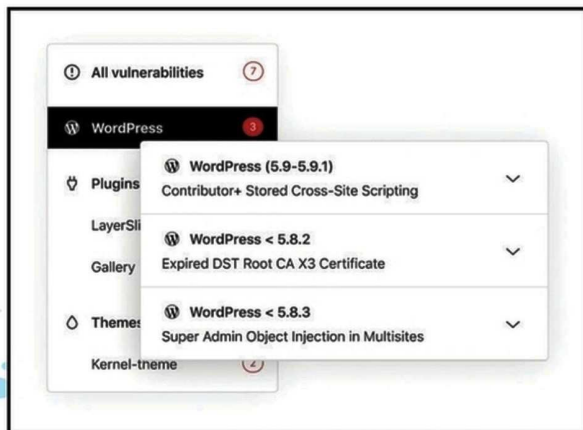
> CIBLE WORDPRESS

WPScan, conçu spécifiquement pour WordPress, contient une vaste base de données de vulnérabilités et de faiblesses connues. Ses capacités d'analyse incluent la détection des noms d'utilisateur, des mots de passe faibles, des versions de plugins non sécurisées et des thèmes vulnérables.

WPScan est un outil de ligne de commande doté d'un

potentiel d'automatisation utilisant des scripts pour des tests à grande échelle. Il est régulièrement mis à jour pour inclure les dernières vulnérabilités connues.

Lien : wpscan.com/wordpress-security-scanner

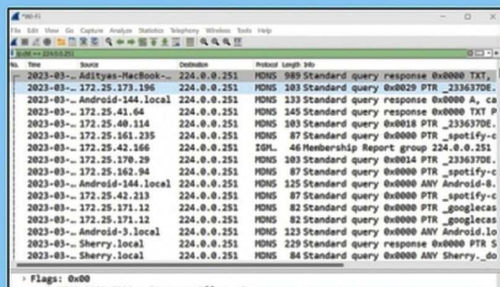




WIRESHARK > ANALYSE LES VULNÉRABILITÉS D'UN RÉSEAU

Wireshark est un analyseur de protocole réseau open source populaire. Il peut être utilisé sur plusieurs systèmes d'exploitation pour capturer et analyser le trafic réseau. Les capacités d'inspection et de filtrage des paquets réseau en temps réel facilitent l'investigation ciblée d'un trafic réseau spécifique.

Lien : www.wireshark.org

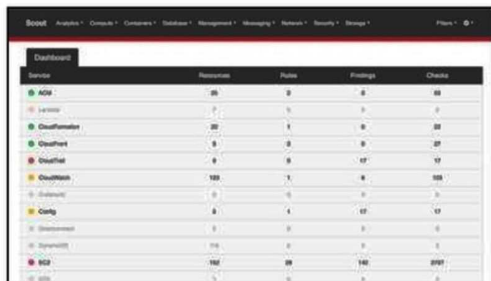


SCOUTSUITE

> POUR LE CLOUD

ScoutSuite est un outil populaire qui analyse les environnements cloud à la recherche de vulnérabilités et de mauvaises configurations. L'outil fonctionne sur AWS, Azure et GCP. Il fournit une analyse détaillée des ressources cloud, telles que les machines virtuelles, les bases de données et les compartiments de stockage. Il évalue également leur conformité aux meilleures pratiques de sécurité standards du secteur.

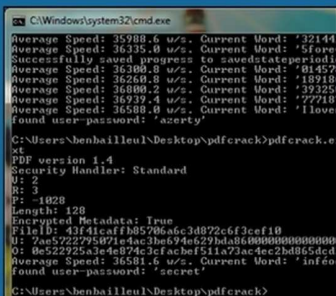
Lien : sourceforge.net/projects/scout-suite.mirror



PDFCRACK > 100%PDF

PDFCrack est un logiciel destiné à fonctionner sur système Linux, mais il existe une version pour Windows. Il permet de tirer profit des processeurs multicœurs et de la puissance de plusieurs ordinateurs (cluster) pour attaquer les mots de passe d'ouverture et d'autorisation du format PDF.

Lien : <http://andi.flowrider.ch/research/pdfcrack.html>



NMAP > ANALYSE LES VULNÉRABILITÉS D'UN RÉSEAU

Nmap, communément appelé mappeur de réseau, « cartographie » un réseau en analysant les réponses reçues des paquets envoyés au réseau cible. Avec Nmap, les utilisateurs peuvent déterminer quels hôtes et services sont disponibles. Nmap permet également aux testeurs d'identifier les détails du système d'exploitation, les ports ouverts, les numéros de version des services en cours d'exécution, les pare-feu et les vulnérabilités potentielles du réseau. Nmap peut être utilisé sur divers systèmes d'exploitation, notamment Linux, Windows et macOS. Il prend également en charge différents types d'analyse, depuis les analyses de ports simples jusqu'aux analyses avancées qui détectent des vulnérabilités spécifiques. Il peut être utilisé avec d'autres outils comme Metasploit pour une exploitation automatisée des vulnérabilités.

Lien : github.com/nmap/nmap

```
Nmap scan report for 10.0.0.71
Host is up (0.0095s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vnc?
2869/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: B0:6E:BF:30:AD:33 (ASUSTek Computer)
Service Info: OS: Windows; CPE: o:microsoft:windows

Nmap scan report for 10.0.0.89
Host is up (0.14s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
7000/tcp   open  rtsp           iTunes rtspd 377.40.00
MAC Address: 10:3D:0A:90:A1:B5 (Hui Zhou Gaoshengda Technology)

Nmap scan report for 10.0.0.138
Host is up (0.17s latency).
All 1000 scanned ports on 10.0.0.138 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 44:61:32:52:EA:8D (ecobee)
```

AIRCRACK-NG > CIBLE LES RÉSEAUX WI-FI

Aircrack-ng fournit une suite complète d'outils pour surveiller et analyser le trafic réseau. Il prend également en charge le piratage des mots de passe pour les réseaux wifi qui utilisent des méthodes de cryptage faibles. Il est open source et peut aider à identifier les points d'accès vulnérables, à surveiller le trafic réseau et à tester la sécurité du réseau.

Lien : www.aircrack-ng.org

```
Aircrack-ng 0.9

[00:03:06] Tested 674449 keys (got 96610 IVs)

KB  depth  byte(vote)
0  0/ 9  12( 15) F9( 15) 47( 12) F7( 12) FE( 12) 1B( 5) 77( 5) A5( 3) F6( 3) 03( 0)
1  0/ 8  34( 61) E8( 27) E0( 24) 06( 18) 30( 16) 4E( 15) E1( 15) 2D( 13) 09( 12) E4( 12)
2  0/ 2  56( 87) A6( 63) 15( 17) 02( 15) 68( 15) E0( 15) A8( 13) 0E( 10) 17( 10) 27( 10)
3  1/ 5  78( 43) 1A( 20) 98( 20) 4B( 17) 4A( 16) 2B( 15) 4D( 15) 50( 15) 6A( 15) 7C( 15)

KEY FOUND! [ 12:34:56:78:90 ]

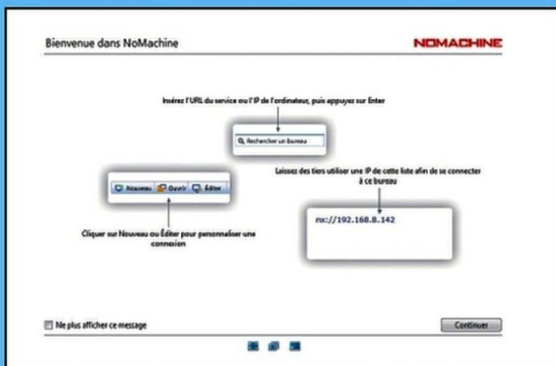
Probability: 100%
```



NO MACHINE > PRISE DE CONTRÔLE À DISTANCE

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

Lien : www.nomachine.com



OSFORENSIC

> INTRUSION MATÉRIELLE

Ce puissant outil de recherche et d'investigation est utilisé par la police, les services de renseignement et les professionnels de restauration de fichiers. OSForensics va scanner votre ordinateur (ou celui que vous voudrez) en vue d'extraire les informations pertinentes : mot de passe (site ou documents), activité récente, fichiers supprimés ou avec une extension ne correspondant pas, etc. En plus de toutes ces fonctionnalités, le logiciel permet de créer un index des fichiers et des e-mails pour retrouver en un instant les éléments en rapport avec tel ou tel sujet. Il analyse le contenu du disque par secteur et fouille même dans la mémoire. Notons aussi la possibilité de faire un cliché des partitions du disque pour observer les changements dans le temps ou créer une image du disque pour l'exporter et l'analyser tranquillement plus tard. La version 8 dispose d'un essai gratuit mais de plus anciennes versions sont, elles, disponibles gratuitement.

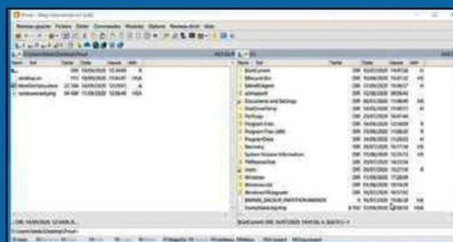
Lien : www.osforensics.com



ALTAP SALAMANDER > RÉVÉLER L'INVISIBLE

Vous avez masqué, un peu trop consciencieusement, des fichiers sensibles sur votre partition Windows (avec par exemple les commandes attrib +s +h) et vous ne vous souvenez plus où ils se trouvent ? L'utilitaire gratuit Altap Salamander va vous aider à les dénicher. Il suffit de lui indiquer l'emplacement qu'il doit scruter et, au bout de quelques minutes, les fichiers cachés ressurgissent. À garder sous la main.

Lien : altap.cz/salamander/downloads



PROXMARK3

> INTRUSION MATÉRIELLE

Proxmark3 est un outil matériel opensource utilisé pour la recherche et les tests RFID. Il peut lire et émuler différents types de cartes et d'étiquettes RFID, effectuer des analyses sans fil et cloner des appareils RFID. Cet outil permet aux pentesters de simuler diverses attaques, telles que des attaques par rejeu et des attaques de type man-in-the-middle, sur les systèmes RFID afin d'évaluer leur niveau de sécurité.

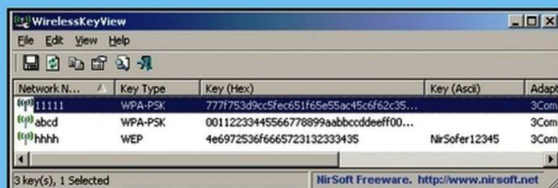
Lien : proxmark.com



WIRELESSKEYVIEW > CIBLE LES RÉSEAUX WI-FI

Cette fois-ci, ce logiciel se spécialise uniquement dans la récupération des identifiants de votre réseau Wi-Fi. Installé sur votre PC, il va analyser le signal et tentera de vous livrer le nom du réseau (SSID), le type de protection (WEP/WPA), le mot de passe complet (Hex, Ascii) et le nom du routeur Wi-Fi.

Lien : www.nirsoft.net

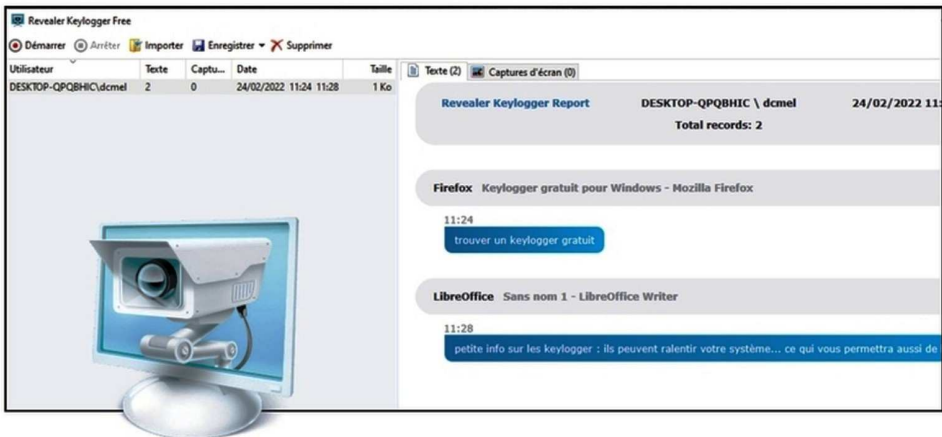




REVEALER KEYLOGGER > ENREGISTREUR DE FRAPPES

Un outil précieux pour surveiller tout ce qui est écrit sur votre PC, sur un document ou une messagerie : tout ce qui est frappé sur le clavier est enregistré. Dans sa version gratuite, Revealer Keylogger ne peut être masqué à l'insu d'un utilisateur curieux, ce qui le réserve heureusement à des usages légaux. L'ergonomie du logiciel permet la consultation des journaux très clairs et bien organisés, contrairement à d'autres concurrents.

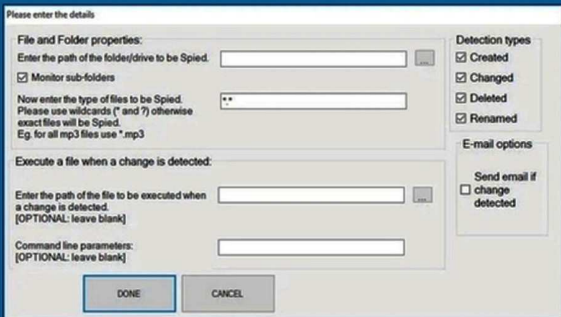
Lien : logixoft.com



THE FOLDER SPY > MONITORING POUR TOUT SURVEILLER

Cet outil de monitoring peut se transporter sur une clé USB et s'installer en mode incognito sur un appareil. Très léger, il surveille toutes les modifications de fichiers et dossiers et est entièrement automatisé. Une fois en place, vous n'avez plus qu'à regarder les journaux pour savoir ce qu'il s'est passé en votre absence.

Lien : bit.ly/3KhMQZI



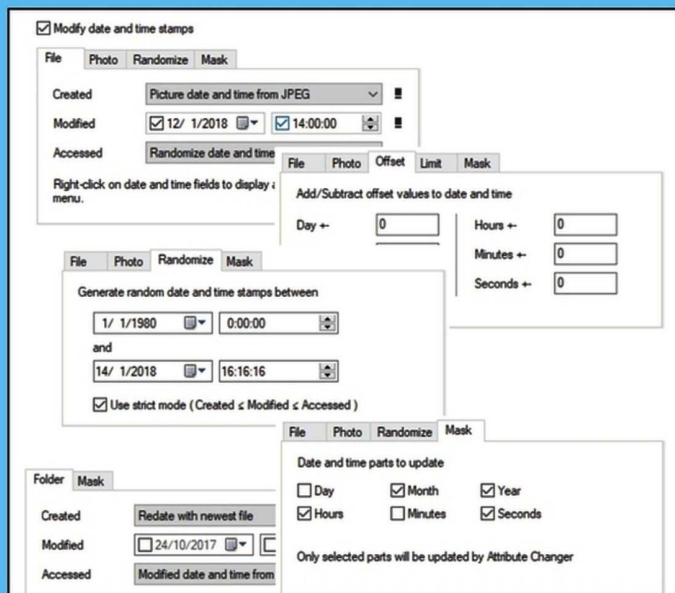
ATTRIBUTE CHANGER

> CHANGER LES ATTRIBUT D'UN FICHIER

Attribute Changer vous donne la main sur les attributs d'un fichier ou d'un dossier (date et heure de création ou modification, lecture seule, système, caché, archive et indexé, etc.). Il vous permet de les modifier et donc de leur donner une nouvelle identité pour, par exemple, masquer

ses origines. Une fois Attribute Changer installé, ce programme gratuit sera accessible via le clic droit de votre souris sur le fichier ou dossier cible. Vous avez la possibilité de modifier les attributs de fichiers un par un ou par lot. Un mode **Simulation** vous permet de vérifier le résultat avant toute modification.

Lien : www.petges.lu



OFFICE2JOHN

> UN PUISSANT CRACKER DE DOCS

Les documents Word, Excel ou PowerPoint peuvent aussi profiter d'une protection par mot de passe. Si votre mémoire vous joue des tours, pas de panique. Office2John va vous donner un sérieux coup de main. Ce programme gratuit, écrit en Python, se charge d'extraire le hash du fichier issu de diverses versions d'Office (de 97 à 2013). Le hash en main, ne reste plus qu'à se remettre à Johnny ou Hashcat pour révéler le sésame. Vous pouvez pour cela suivre ce tutoriel en anglais mais très détaillé : tinyurl.com/y4n6cvws.

Lien : tinyurl.com/y5as3b87



NIRSOFT > LA TROUSSE À OUTILS

Pour ceux qui ne le connaissent pas, Nirsoft est un site web qui propose une collection unique de petits utilitaires freeware utiles, tous développés par Nir Sofer. Vous y trouverez des outils de récupération de mot de passe, de surveillance réseau, de ligne de commande, pour retrouver des clés de licence, etc. Certains outils sont un peu datés mais d'autres continuent d'être mis à jour.

Lien : www.nirsoft.net

NirSoft

- Main Page
- Blog
- Search
- FAQ
- TOP 10
- PDF Files
- Contact
- About...
- Donate
- All Utilities
- System Tools
- Network Tools
- Programmer Tools
- Outlook/Office
- 64-bit Download
- Panel
- Forensics
- Pre-Release Tools
- Articles

Ads by Google

Stop seeing this ad Why this ad?

Windows Password Recovery Tools

See Also:

- Windows Password Recovery Software From Stellar Phoenix - Reset Windows password, recover FTP passwords, and more...

NirSoft Web site provides free password recovery tools for variety of Windows programs, including Chrome Web browser, Firefox Web browser, Microsoft Edge, Internet Explorer, Microsoft Outlook, Network passwords of Windows, Wireless network keys, Display entries of Windows, and more...

If you want to download a package of all Windows password recovery tools in one zip file, [click here](#). The password to extract the files is [nirsoft123!](#) (Click the password to copy it to the clipboard)

Be aware that some Antivirus programs might detect that these password recovery tools are infected with Virus/Trojan. All these Trojan/virus alerts are "False Positive" issues. [Click here](#) to read more false alerts in Antivirus programs.

As you may know, I removed the command-line options that exports the passwords to a file from all major password-recovery tools. You can find the reason for removing the command-line option [Blog post](#). If you need to use the command-line options of these password-recovery tools (For legal purposes only!), you can download a package of all major password-recovery tools with command support, by following the instructions below:

1. Click [this download link](#).
2. Enter "download" as the user name, and "nirsoft123!" as the password.
3. After downloading the package, extract the files from it using the following password: [nirsoft123!](#)

If you want to get more information about the locations in the Registry or in the file system that the passwords are stored, you can read this: [Password Storage Locations For Popular Windows Apps](#)

The following table describes the most popular password recovery utilities for Windows in NirSoft Web site:

IE PassView	IE PassView is a small utility that reveals the passwords stored by Internet Explorer browser. It supports the new Internet Explorer 7.0 and 8.0, as well as older versions of Internet Explorer, v4.0 - v6.0
Dialupass	Password recovery tool that reveals all passwords stored in dial-up entries of Windows (Internet and VPN connections). This tool works in all versions of Windows including Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003/2008, Windows 8, and Windows 10.
BulletsPassView	BulletsPassView is a password recovery tool that reveals the passwords stored behind the bullets in the standard password text-box of Windows operating system Internet Explorer Web browser. After revealing the passwords, you can easily copy them to the clipboard or save them into text/html/csv/xml file. You can use this tool to recover the passwords of many Windows applications, like CuteFTP, Filezilla, VNC, and more...
Network Password Recovery	Recover network shares passwords stored by Windows XP, Windows Vista, Windows 7, and Windows Server 2003/2008.
RouterPassView	Windows utility that can recover lost passwords from configuration file saved by a router. This utility only works if your router save the configuration file in a format RouterPassView can detect and decrypt.

SOCIAL ENGINEER TOOLKIT

> BOÎTE À ARNAQUES

Le Social Engineer Toolkit (SET) est un outil open source utilisé pour générer diverses attaques d'ingénierie sociale telles que le phishing et la récolte d'informations d'identification. De plus, il inclut des fonctionnalités d'usurpation d'e-mails, d'usurpation de SMS et d'usurpation de géolocalisation. Il peut même s'intégrer au framework Metasploit pour permettre aux testeurs de fournir des charges utiles et d'exploiter les vulnérabilités.

Lien : www.trustedsec.com/tools/the-social-engineer-toolkit-set





HACKING

10111010011010111101010101101010101010101010101

TOP 5

CRACK DE MOTS DE PASSE



LOGIN

PASSWORD



JOHN THE RIPPER

John the Ripper est un outil largement utilisé pour déchiffrer les mots de passe cryptés avec des algorithmes de cryptage populaires tels que MD5 et SHA. Il peut également effectuer des attaques par dictionnaire et tester la force des mots de passe.

Lien : www.openwall.com/john/

John The Ripper Modes



Single Crack



Wordlist



Incremental

VARONIS

```

hashcat (v6.2.1) starting...
CUDA API (CUDA 11.3)
*****
* Device #1: NVIDIA GeForce RTX 2080 Ti, 10137/11264 MB, 68MCU

Hashes: 1 digests; 1 unique digests; 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepend-Salt
* Single-Hash
* Single-Salt
* Brute-Force
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 1100 MB
e983672a03adcc9767b24584338eb378:00:hashcat

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Solarwinds Serv-U
Hash.Target.....: e983672a03adcc9767b24584338eb378:00
Time.Started.....: Sun May 23 21:43:13 2021 (1 sec)

```

HASHCAT

Hashcat est un outil populaire capable de déchiffrer plus de 300 types de hachage différents à l'aide d'attaques par dictionnaire, par force brute et hybrides. Il prend en charge le cracking distribué afin que plusieurs ordinateurs puissent travailler ensemble pour cracker un mot de passe lors d'enquêtes forensics.

Lien : hashcat.net

HYDRA

Hydra est un outil populaire de piratage de mots de passe qui effectue des attaques par force brute sur divers protocoles et services tels que SSH, FTP et Telnet. Il prend en charge les mécanismes d'authentification tels que HTTP, FTP et SMB, ce qui en fait un outil polyvalent.

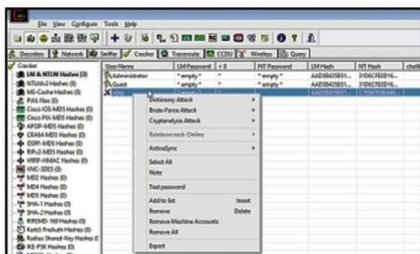
Lien : github.com/vanhauser-thc/thc-hydra



CAIN & ABEL

Connu pour sa capacité à cracker des mots de passe, Cain & Abel possède dans sa besace de nombreux autres outils d'analyse et de sniff. L'interface est riche et « assez » intuitive si vous n'êtes pas rebuté par les dizaines de sous-menus disponibles. Il prend en charge les attaques par rainbow tables, comme les attaques plus classiques (brute, dictionnaire, etc.), que ce soit en local ou en ligne. Gratuit, Cain & Abel ne fournit cependant pas son code source.

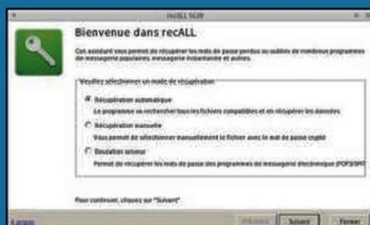
Lien : tinyurl.com/y3zb2tqv



RECALL

Vous devrez installer recALL sur le PC cible et laisser le programme travailler pour vous. Il n'est pas là pour cracker un fichier ou un service en ligne mais pour chercher des mots de passe, des codes d'accès ou des numéros de licence dans des endroits de votre Windows dont vous ne soupçonniez même pas l'existence (dossier d'installation, base de registre, etc.). Ces emplacements sont préenregistrés et toutes sortes de logiciels sont passés au crible : Windows, Office, antivirus, client mail, navigateurs, client FTP, messagerie instantanée, logiciels commerciaux, jeux vidéo, etc. Avec presque 3 000 références, ce serait bien le diable si recALL ne trouvait pas ce que vous cherchez.

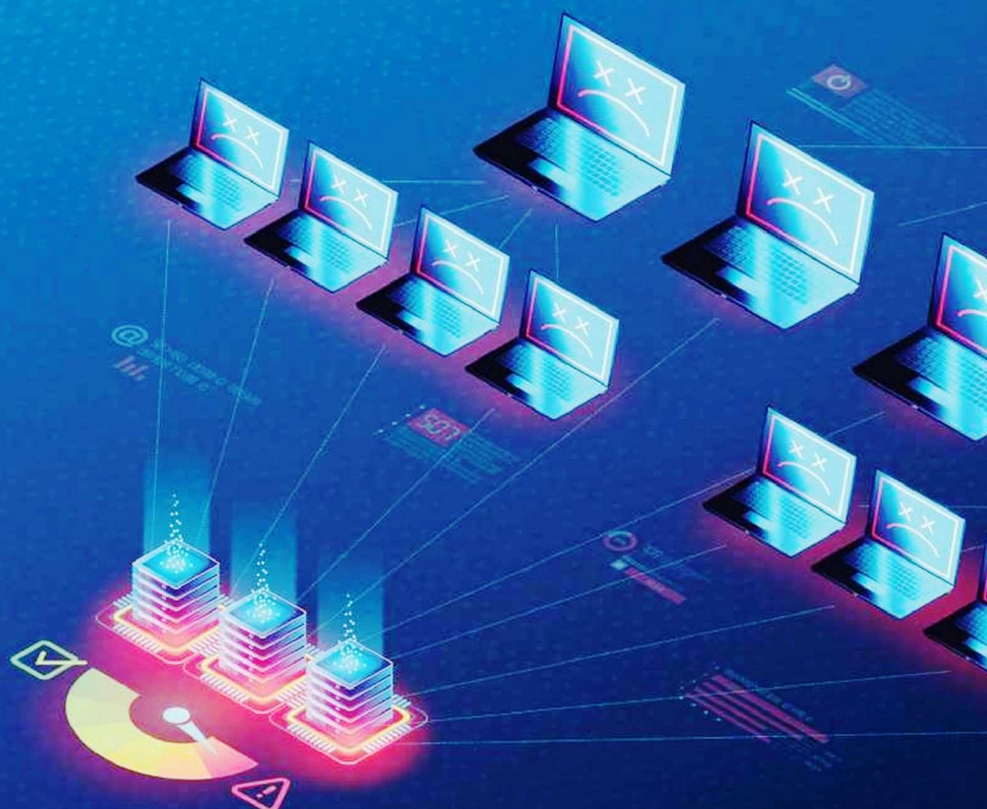
Lien : keit.co/p/recall



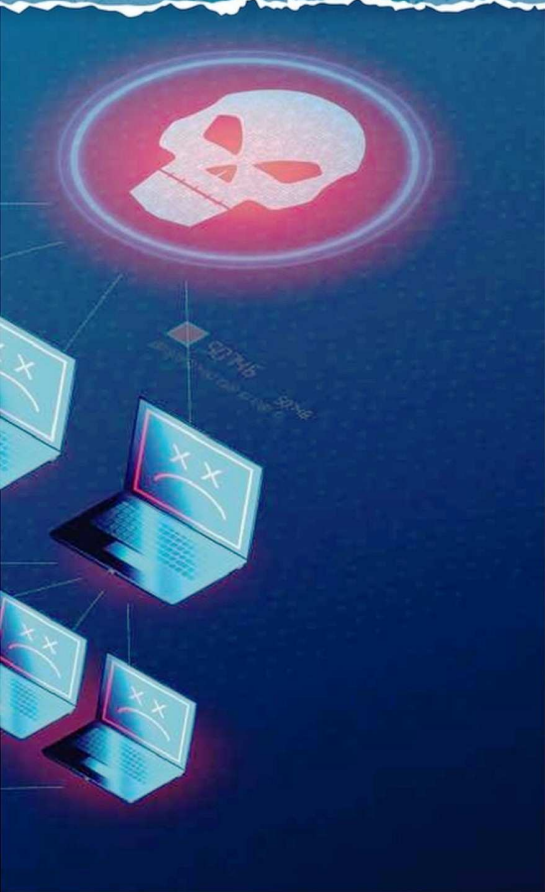


HACKING

11010011010111101010101101010101010101000



COMMENT FONT LES PIRATES POUR LANCER LEURS ATTAQUES DDOS



Les attaquants utilisent différentes méthodes pour lancer une attaque DDoS. Une stratégie commune est la création d'un «botnet», un réseau de machines infectées par des logiciels malveillants, contrôlées à distance par l'attaquant. Ces machines, souvent des ordinateurs



personnels ou des appareils IoT compromis, sont utilisées pour envoyer un grand nombre de requêtes simultanées à la cible, la submergeant de trafic.



POUR MENER UNE ATTAQUE PAR DÉNI DE SERVICE, UN PIRATE UTILISERA UN RÉSEAU DE PC ZOMBIES. UN PC ZOMBIE EST UN PC INFECTÉ SANS QUE SON PROPRIÉTAIRE LE SACHE. MAIS SES RESSOURCES ET SA CONNEXION À INTERNET SERONT UTILISÉES PAR UN HACKER POUR ENVOYER DES REQUÊTES SUR SA CIBLE FINALE. IL FAUT DES CENTAINES VOIRE DES MILLIERS DE PC ZOMBIES POUR MENER UNE ATTAQUE DDOS. UN TEL RÉSEAU EST APPELÉ BOTNET.



Une autre stratégie est l'exploitation des vulnérabilités des serveurs ou des réseaux pour amplifier le trafic. Par exemple, un attaquant peut utiliser un petit nombre de requêtes pour générer une grande quantité de réponses de la part du serveur cible. Cette technique utilise des protocoles comme NTP (Network Time Protocol) ou DNS (Domain Name System) pour amplifier l'attaque.

QUELLES RESSOURCES NÉCESSAIRES ?

Pour mener une attaque DDoS, les pirates ont besoin de ressources telles que des ordinateurs ou des appareils compromis pour former un botnet. Ils

peuvent également avoir besoin de logiciels spécifiques pour automatiser et orchestrer l'attaque, ainsi que d'une connexion Internet stable et rapide pour gérer le trafic généré.

Les attaquants passent par des forums spécialisés pour acquérir des outils et des compétences, ou des services de location de botnets («DDoS-for-hire») pour faciliter l'attaque sans nécessiter une infrastructure propre. Les protocoles couramment exploités incluent HTTP pour le trafic web, UDP (User Datagram Protocol) pour les services comme le streaming vidéo, et ICMP (Internet Control Message Protocol) pour les messages d'erreur et de contrôle du réseau.

TROIS TECHNIQUES POUR TROIS FAILLES

- **UDP Flood** : Cette technique utilise le protocole UDP (User Datagram Protocol) pour envoyer un grand nombre de paquets UDP à des ports aléatoires sur un serveur distant, provoquant une surcharge du serveur.

- **SYN Flood** : Une attaque qui exploite le protocole TCP. Elle envoie des demandes de connexion (SYN) rapides et continues sans compléter le processus de connexion, ce qui épuise les ressources du serveur.

- **Ping of Death** : Exploite les faiblesses du protocole ICMP en envoyant des paquets malformés ou de très grande taille qui peuvent provoquer un crash ou un redémarrage du système cible.

```
// UDP Flood initiation..
286 function udpFlood($host,$port,$time,$packetsize) {
287     $this->privmsg($this->config['chan'], "[*]UDP Flood Started[*]");
288     $packetsize = 1;
289     for($i=0;$i<$packetsize;$i++) { $packet = chr(rand(1,256)); }
290     Send = time() + $time;
291     $multitarget = false;

// Supporting Multiple Hosts Attacks..
298 if($multitarget) {
299     {
300         $fp = array();
301         foreach($host as $shost) $fp[] = fsockopen("udp://", $shost, $port);

// The UDP Packet attack logic (payloads)..
306 fwrite($fp[$i % $count], $packet);
307 fflush($fp[$i % $count]);
308 if($i % 100 == 0) {
309     {
310         if($Send < time()) break;
311     }
312     $i++;
}
```


TOP 5



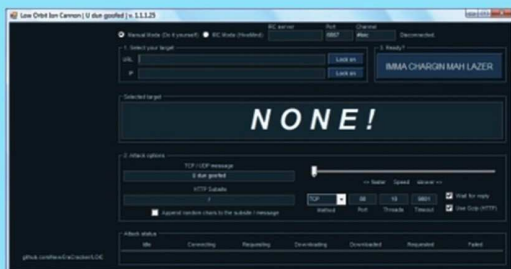
LOGICIELS POUR LANCER UNE ATTAQUE DDOS

» LOIC (Low Orbit Ion Cannon)

> POUR LES DÉBUTANTS ET LES TESTS DE SÉCURITÉ

Toujours utilisé mais plutôt destiné aux débutants grâce à son interface accessible) et aux cibles mal protégées. LOIC a été conçu avec l'intention de permettre aux administrateurs de réseau de tester la résistance de leur propre infrastructure aux attaques DDos. L'idée était de fournir un moyen simple et accessible pour simuler

des attaques réalistes, permettant ainsi d'identifier et de renforcer les points faibles. Cependant, en raison de sa facilité d'utilisation et de sa disponibilité en open-source, LOIC a rapidement été adopté par des hackers et des collectifs tels que Anonymous. Mais il se trouve aujourd'hui de plus en plus délaissé au profit d'alternatives plus puissantes. Car les attaques menées avec LOIC sont relativement faciles à détecter et à atténuer par les défenseurs modernes de cybersécurité. Les systèmes de protection contre les DDos ont évolué pour identifier et filtrer le trafic malveillant généré par des outils comme LOIC. Le programme n'offre qui plus est pas d'anonymat pour ses utilisateurs, rendant les attaquants facilement traçables par les autorités. L'utilisation de VPN ou autre solution de routage proxy s'impose donc.



Lien : sourceforge.net/projects/loic/



ET POUR LES RÉSEAUX DE BOTNETS ?

Pour l'utilisation de PC zombies et de botnets, voici les principaux malwares utilisés :

- **Mirai** : Comme indiqué ci-contre, Mirai est un tout-en-un qui peut préparer et lancer une attaque DDoS en ayant la capacité à mobiliser son réseau de botnets infectés pour se faire.

- **Trickbot** : Originellement un cheval de Troie bancaire, Trickbot a évolué pour inclure des fonctionnalités permettant la création de botnets. Il est souvent distribué via des campagnes de phishing.

- **Emotet** : Bien qu'il soit principalement un logiciel malveillant de vol

d'informations, Emotet a été utilisé pour distribuer d'autres types de malwares, y compris ceux qui créent des botnets.

- **Qbot (ou Qakbot)** : Ce malware polymorphe est connu pour sa capacité à infecter des réseaux d'entreprises et à recruter des machines infectées dans des botnets.

- **DDoS-for-hire Services** : Ces services, également connus sous le nom de «booters» ou «stressers», offrent à des individus la capacité de lancer des attaques DDoS sans avoir besoin de créer leur propre botnet. Ils louent l'accès à des réseaux de machines infectées.

Cyberbooter.eu Home How It Works Pricing Telegram Support Sign In

Advanced IP Booter Panel With Guaranteed Attack Power

Made by a highly skilled developers, We have our own dedicated servers and everything is custom coded by us: beautiful panel, advanced attack methods and more...

- 11+ Attack Methods
- 10+ Active Servers
- 134735+ Total Attacks

Cyberbooter is a professional IP Stresser services used in a booter panel that will let you simulate DDoS attacks against your server/website/ip. We have amazing custom panel, easy to use and the most advanced bypass attack methods on the market so you can enjoy a really powerful and affordable IP Stresser.

Les hackers en herbe trouve facilement des sites leur proposant pour quelques dizaines d'euros par moi des services « DDoS-for-hire ». C'est-à-dire que programmes d'attaques et botnets sont fournis pour automatiser au maximum les attaques.

» HOIC (High Orbit Ion Cannon)

> LOIC... MAIS EN MIEUX.

À la différence de LOIC, qui se concentre sur une seule cible à la fois, HOIC peut attaquer plusieurs cibles simultanément grâce à sa capacité à gérer jusqu'à 256 adresses URL ou IP différentes en une seule instance. Il utilise des scripts personnalisables, appelés «boosters», pour varier le type de trafic généré, rendant ainsi les attaques plus difficiles à détecter et à bloquer par les mécanismes de défense traditionnels. Ces scripts permettent également d'imiter les comportements des utilisateurs légitimes, augmentant d'autant plus la complexité de la détection des attaques.

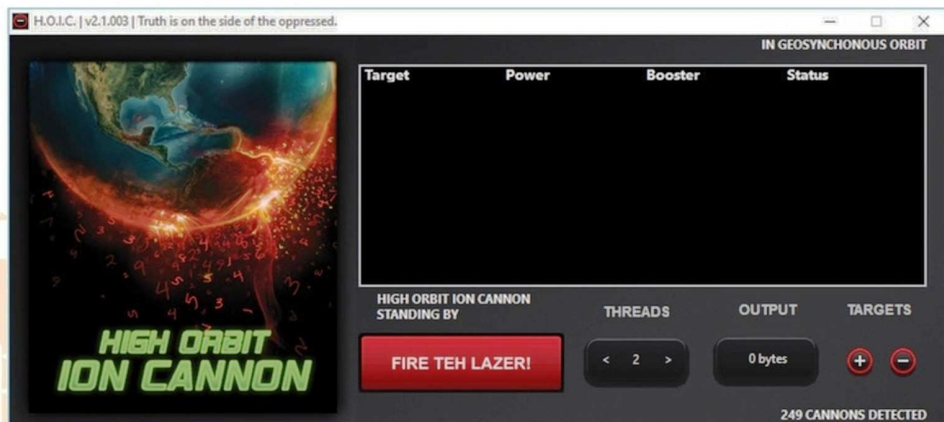
Comme LOIC, HOIC présente une interface utilisateur graphique (GUI) simple, rendant les attaques DDoS accessibles même aux utilisateurs ayant des connaissances techniques limitées.

Bien que l'utilisation de HOIC puisse



être tracée jusqu'à l'IP de l'attaquant si des précautions supplémentaires ne sont pas prises, l'outil est souvent utilisé en conjonction avec des réseaux privés virtuels (VPN) ou des réseaux de botnets pour masquer l'identité de l'attaquant.

Lien : sourceforge.net/projects/high-orbit-ion-cannon



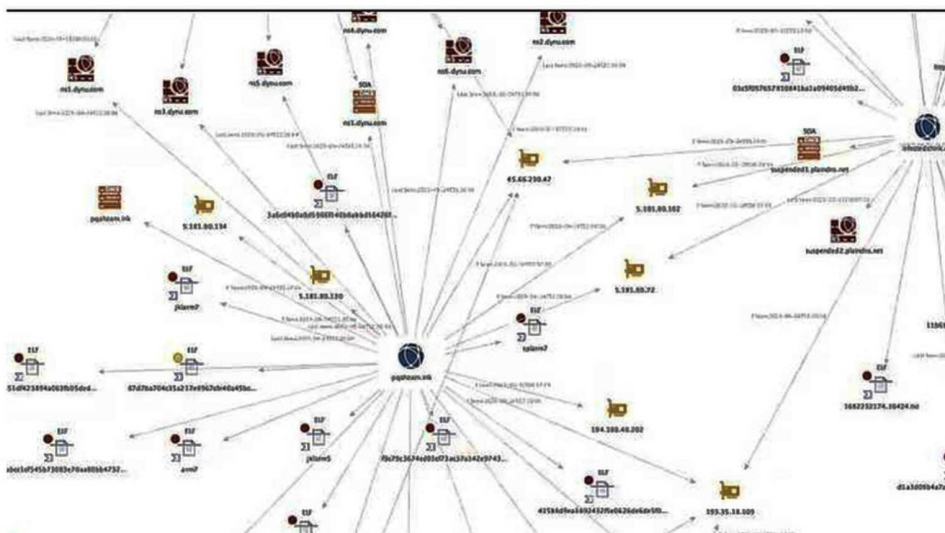


» Mirai Botnet

> MYRIADES D'OBJETS CONNECTÉS

Bien que plus connu comme un botnet, Mirai est également associé à un outil pour lancer des attaques DDoS. Mirai fonctionne en infectant des appareils IoT vulnérables, tels que des caméras IP, des

nouveaux appareils vulnérables à infecter, augmentant rapidement la taille de son botnet. Le botnet Mirai peut être utilisé pour lancer plusieurs types d'attaques DDoS, y compris les attaques par



routeurs et d'autres dispositifs connectés, en utilisant une table de mots de passe par défaut largement répandus et rarement modifiés par les utilisateurs finaux. Une fois un appareil infecté, il est ajouté à un réseau de bots (botnet) contrôlé à distance par l'attaquant. Ce réseau peut ensuite être utilisé pour lancer des attaques DDoS. Mirai peut automatiquement scanner Internet à la recherche de

inondation SYN, UDP, et DNS, rendant ses attaques difficiles à atténuer.

L'impact et la facilité d'utilisation de Mirai ont rapidement conduit à sa notoriété. Après l'attaque contre Dyn, le code source de Mirai a été publié en ligne, permettant à d'autres cybercriminels de créer leurs propres variantes du botnet. Le dernier en date ayant impressionné les spécialistes en cybersécurité est baptisé « V3G4 de Mirai ».

L'INFORMATIQUE FACILE POUR TOUS !



**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**

LES DOSSIERS DU
Pirate



JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON
MARCHAND DE JOURNAUX

Direct Éditeurs

ANONYMAT & PROTECTION





TOP 5



NAVIGATEURS QUI PROTÈGENT VOS DONNÉES

BRAVE > LE CHAMPION

Brave se démarque en bloquant par défaut les traceurs et les publicités intrusives. Basé sur le projet open source Chromium, il offre une expérience de navigation rapide tout en mettant l'accent sur la sécurité. De plus, avec son système innovant de récompense en cryptomonnaie, Brave redéfinit la relation entre les annonceurs, les créateurs de contenu et les utilisateurs.

Lien : brave.com



TOR > VERS L'ANONYMAT ET AU-DELÀ

En faisant rebondir le trafic des utilisateurs à travers un réseau mondial de relais, Tor garantit un niveau d'anonymat inégalé. Conçu pour accéder au Dark Web, il est aussi compatible avec le protocole Internet que nous utilisons tous au quotidien. Mais ces vitesses sont moindres que ces concurrents, du fait de son architecture.

Lien : www.torproject.org

FIREFOX

> TOUJOURS PLUS DE FONCTIONS

Depuis sa création en 2002, Firefox a toujours été à la pointe de la navigation web. Développé par la Mozilla Foundation, il est reconnu pour sa vitesse, sa sécurité, ses nombreux réglages et ses extensions. Avec des initiatives comme le projet Quantum, Firefox continue d'innover tout en restant fidèle à sa mission de protéger la vie privée des utilisateurs.

Lien : www.mozilla.org/fr/firefox/



LIBREWOLF > LE LOUP LIBRE

Dérivé de Firefox, LibreWolf est le navigateur pour ceux qui veulent encore plus de confidentialité. Sans collecte et avec uBlock Origin préinstallé, il offre une



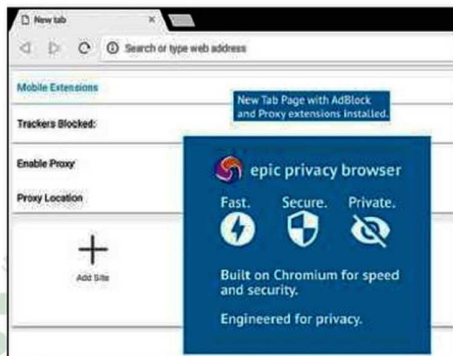
expérience de navigation sécurisée tout en restant fidèle à l'esprit open source.

Lien : librewolf-community.gitlab.io

EPIC > FUTUR CHALLENGER ?

Lui aussi basé sur Chromium, Epic fonctionne par défaut en mode privé, garantissant ainsi qu'aucune information de navigation n'est conservée une fois la session terminée. Epic est équipé d'un petit VPN. Il bloque bien sûr les publicités, les trackers et d'autres méthodes utilisées pour suivre les utilisateurs à leur insu.

Lien : www.epicbrowser.com





TOP 3



MESSAGERIES VRAIMENT SÉCURISÉES

**SIGNAL**

> LE MEILLEUR RAPPORT

QUALITÉ/SÉCURITÉ

Considérée comme l'une des applications de messagerie les plus sûres du marché, Signal protège vos communications par un chiffrement de bout en bout des appels et des messages. Son protocole de chiffrement est si sûr que d'autres applications de premier plan (telles que WhatsApp et Facebook Messenger), l'utilisent également. Comme d'autres applications, Signal propose des fonctions de messagerie, appel, chat vidéo et partage de fichiers/photos. Elle permet également de faire disparaître les messages pour plus de confidentialité. Vous avez besoin d'un numéro de téléphone pour vous inscrire et nous vous recommandons de sécuriser l'application avec un mot de passe. Pour les amateurs de sécurité, toutes vos données sont stockées localement sur votre appareil, et non sur des serveurs distants. Enfin, des dizaines de fonctions et paramètres vous permettront de personnaliser votre usage et d'ajouter encore plus de confidentialité !



Signal n'est pas la propriété d'une grande entreprise technologique. Il s'agit d'un logiciel open source financé par des subventions et des dons. Contrairement à d'autres applications de messagerie privée, Signal ne contient pas de publicités, d'affiliés ni de suivi secret — nul besoin de s'embarasser d'une option « Ne pas suivre ». De plus, grâce à son statut de logiciel open source, l'application fait l'objet d'audits de sécurité continus afin de la rendre encore plus sûre.

Lien : signal.org/fr



OLVID > LA NOUVELLE MESSAGERIE DU GOUVERNEMENT

Si vous nous lisez régulièrement, vous connaissez déjà Olvid, la messagerie ultra-sécurisée développée par une start-up française et qui séduit les spécialistes de la protection des données. Mais elle a aussi connu un gros coup de projecteur ces derniers mois avec l'annonce de son adoption par l'exécutif français : le gouvernement a rendu obligatoire l'utilisation d'Olvid pour ses ministres et employés gouvernementaux, se détournant d'applications plus populaires comme WhatsApp, Telegram et Signal. Ce changement, effectif à partir du 8 décembre 2023, fait partie d'un effort pour améliorer la sécurité des communications sensibles. Créée en juin 2019. Elle ne recueille bien sûr aucune donnée personnelle, même lors de l'inscription, chiffre les échanges de bout en bout et même les métadonnées. Contrairement à ce qui se passe pour la plupart des messageries, chaque conversation établit

un lien direct avec le ou les destinataires, sans passer par un serveur central. Comme Threema, Olvid ne nécessite pas de numéro de téléphone pour l'inscription, l'ajout de contacts se fait via QR codes, en raison de l'absence d'un annuaire centralisé.

Olvid a reçu d'importantes certifications de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France, étant la première et unique application de messagerie instantanée à recevoir une telle reconnaissance. L'application est disponible gratuitement sur diverses plateformes, y compris Android, iPhone et ordinateurs. Cependant, l'absence de fonctions de base comme l'appel audio, la synchronisation sur plusieurs appareils, etc. en version gratuite l'empêcheront de devenir une application populaire. Dommage.

Lien : olvid.io/fr



THREEMA > LE MODÈLE IDÉAL ?

Threema est une application de messagerie open source, totalement chiffrée de bout en bout, et dont le siège social se trouve en Suisse. Elle est basée sur les principes du privacy-by-design, à savoir l'intégration des principes du respect de la vie privée des usagers dès sa conception. Threema propose des messages, des appels vocaux/vidéo et des chats de groupe. L'utilisation de Threema n'exige ni numéro de téléphone ni adresse électronique, un nouveau standard qui se retrouve chez les plus sécurisées de ses concurrentes. L'inconvénient de la puissante sécurité offerte

par Threema est qu'elle n'est pas gratuite. Son téléchargement coûte 5,99 € sur le PlayStore : donc pas d'abonnement à la clé, mais un paiement unique, plutôt sain et accessible pour franchir le pas. Ce business model lui permet de collecter très peu de données : l'application permet à ses utilisateurs de rester complètement anonymes, elle supprime définitivement un message de ses serveurs après transmission. Pour limiter les écoutes, Threema préfère gérer les informations localement sur les appareils des utilisateurs plutôt que sur des serveurs. Selon le quotidien suisse Le Temps, l'app comptait 6 millions d'utilisateurs en 2023.

Lien : threema.ch/fr/home



TOP 10

EXTENSIONS

POUR FIREFOX

Avec Brave, Firefox est l'un des navigateurs préférés des internautes soucieux de garder le contrôle de leurs données et de leur vie numérique. Il dispose également de nombreuses extensions qui viennent renforcer voire étendre le champ de ses possibilités en matière de sécurité, de protection de la vie privée et de confidentialité.



UMATRIX > TOUR DE CONTRÔLE

UMatrix permet un contrôle complet des connexions, des téléchargements et de l'exécution des scripts par le navigateur. Il est recommandé pour les utilisateurs avancés, car il nécessite de nombreux réglages.

UMatrix fonctionne en bloquant par défaut tous les scripts, iframes, et autres éléments potentiellement dangereux, tout en permettant à l'utilisateur de créer des règles personnalisées pour les autoriser sur des sites de confiance. Sa spécificité réside dans sa capacité à décomposer les sites web en composants individuels et à donner un contrôle complet sur ce qui est chargé et ce qui est bloqué. Cela permet de réduire considérablement les risques de malwares, de publicités intrusives et de trackers. L'extension est particulièrement appréciée pour sa flexibilité, mais elle peut être complexe à configurer pour les débutants.



DUCKDUCKGO PRIVACY ESSENTIALS

> LE CANARD MASQUÉ

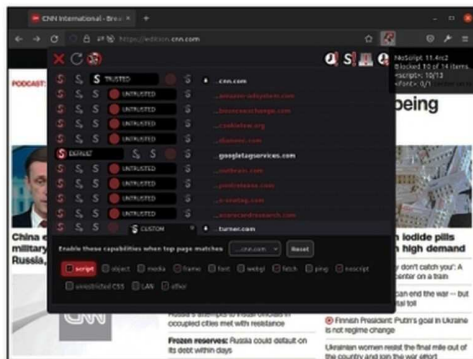
Cette extension offre une expérience de navigation sans suivi, notant les sites en fonction de leurs pratiques de confidentialité. Elle est facile à utiliser et s'intègre bien aux applications courantes. L'extension évalue et note les sites web en fonction de leur utilisation de méthodes de suivi et de la transparence de leur politique de confidentialité. Elle intègre également le moteur de recherche DuckDuckGo par défaut dans le navigateur, permettant ainsi des recherches anonymes sans suivi. Une caractéristique clé est la fonctionnalité de «Protection de la vie privée», qui force les sites à utiliser des connexions cryptées HTTPS lorsque cela est possible, renforçant ainsi la sécurité des données transmises. L'extension est conçue pour être conviviale, avec une interface simple et des explications claires sur les notes de confidentialité des sites. Elle est particulièrement adaptée aux utilisateurs qui veulent une protection de la vie privée sans avoir à configurer de multiples paramètres ou extensions.



NOSCRIPT

> ANTI-SCRIPTS MALICIEUX

NoScript Security Suite est une extension essentielle pour les utilisateurs de Firefox qui veulent se protéger contre les scripts malveillants et les attaques de type cross-site scripting (XSS). Elle fonctionne en bloquant par défaut tous les scripts JavaScript, Java, Flash et autres types de scripts intégrés dans les pages web. L'utilisateur a la possibilité de permettre ces scripts temporairement ou de manière permanente sur des sites de confiance. Une des particularités de NoScript est sa capacité à offrir une protection même contre les menaces inconnues, grâce à son approche préventive. Bien que très efficace, NoScript peut rendre la navigation plus difficile sur certains sites jusqu'à ce que l'utilisateur configure correctement les autorisations. L'extension est idéale pour les utilisateurs qui privilégient la sécurité et sont prêts à consacrer du temps à la configuration des paramètres pour chaque site.





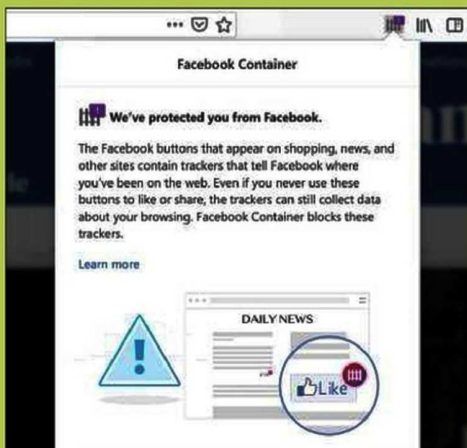
FACEBOOK CONTAINER

> FACEBOOK, PAS BOUGER !

Facebook Container est une extension développée par Mozilla pour limiter la capacité de Facebook à suivre votre activité en ligne en dehors de sa plateforme.

L'extension fonctionne en isolant votre identité Facebook dans un «conteneur» séparé, empêchant ainsi Facebook de suivre vos visites sur d'autres sites via des cookies tiers. Lorsque vous utilisez Facebook, l'extension ouvre le site dans un onglet bleu spécial, indiquant qu'il s'agit d'un conteneur isolé. Tout lien non-Facebook ouvert dans cet onglet sera chargé en dehors du conteneur, empêchant Facebook de lier vos activités sur ces sites à votre identité Facebook.

Cette extension est particulièrement utile pour les utilisateurs qui veulent continuer à utiliser Facebook tout en limitant son influence sur leur vie privée en ligne. Elle est simple à utiliser et ne nécessite pas de configuration complexe, ce qui la rend accessible à tous les utilisateurs, indépendamment de leur niveau de compétence technique.



COOKIE AUTODELETE > SUPPRIMER

Cookie Autodelete gère automatiquement les cookies de votre navigateur. Inspirée par l'extension «Self-Destructing Cookies», elle supprime les cookies des onglets fermés après un certain délai, empêchant ainsi les entreprises de suivre votre navigation sur plusieurs sessions.

L'extension offre une fonctionnalité «Auto-clean» qui doit être activée

pour que les cookies soient effacés automatiquement. Les utilisateurs peuvent également créer une liste blanche de sites pour lesquels ils souhaitent conserver les cookies, garantissant ainsi que les préférences et les sessions de connexion restent intactes pour les sites de confiance. L'extension est facile à utiliser avec une interface simple qui permet une gestion efficace des cookies sans expertise technique approfondie.



OPEN IN TOR BROWSER

> TU ME VOIS, TU ME VOIS PLUS

En activant le bouton Tor, les utilisateurs peuvent diriger leur trafic Internet à travers le réseau Tor, rendant ainsi leur navigation beaucoup plus difficile à suivre pour les annonceurs, les fournisseurs de services Internet et les gouvernements. L'extension est particulièrement utile pour les utilisateurs qui nécessitent un haut niveau d'anonymat en ligne, comme les journalistes travaillant dans des environnements répressifs, les militants, ou toute personne soucieuse de la confidentialité.

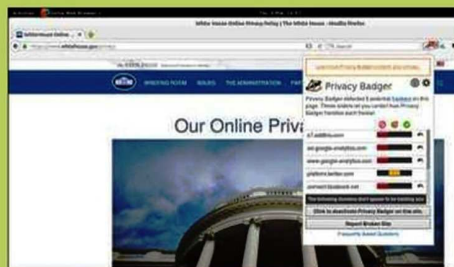
Le bouton Tor permet de basculer facilement entre une navigation normale et une navigation via le réseau Tor, offrant flexibilité et commodité. Il est important de noter que l'utilisation de Tor peut ralentir la navigation en raison de la manière dont le trafic est acheminé à travers différents relais pour atteindre son anonymat.



PRIVACY BADGER > PUBS ET TRACKERS

Privacy Badger est une extension développée par l'Electronic Frontier Foundation (EFF) pour bloquer les publicités et les trackers qui ne respectent pas les préférences de Do Not Track de l'utilisateur. Contrairement aux bloqueurs de publicités traditionnels, Privacy Badger se concentre sur le blocage des trackers invisibles qui collectent des données sur votre comportement en ligne sans votre consentement. L'extension utilise

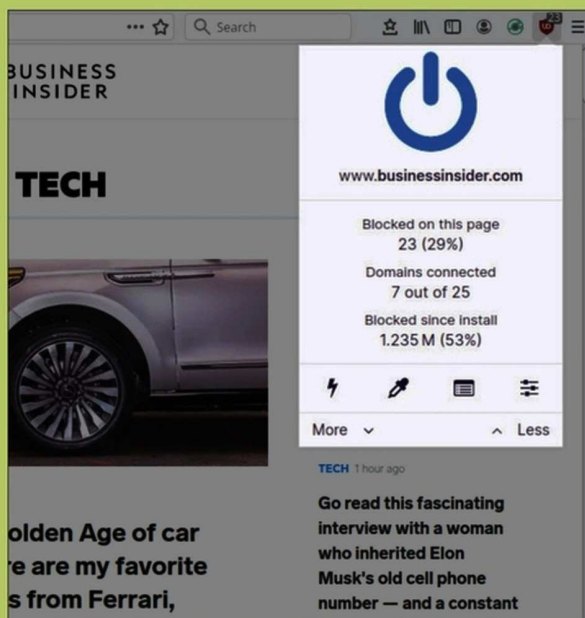
un algorithme d'apprentissage pour détecter et bloquer de nouveaux trackers, ce qui signifie qu'elle s'améliore avec le temps en fonction de votre utilisation. Une caractéristique unique de Privacy Badger est qu'elle ne maintient pas de liste de blocage prédéfinie, mais apprend plutôt quels domaines suivent votre navigation et les bloque en conséquence. Cela rend l'extension efficace contre les trackers récemment apparus et les méthodes de suivi moins connues. Privacy Badger est une excellente option pour les utilisateurs qui cherchent une protection contre le suivi en ligne sans avoir besoin de configurer des listes de blocage ou de filtres complexes.





UBLOCKORIGIN > LE MEILLEUR BLOQUEUR DE PUBS

Très recommandée, UBlockOrigin bloque les publicités intrusives et les traceurs. Elle utilise des listes de filtrage pour bloquer les publicités, les traceurs, et potentiellement les scripts malveillants. Les utilisateurs peuvent personnaliser le filtrage et ajouter ou supprimer des sites de la liste blanche. Ce qui distingue UBlockOrigin, c'est sa légèreté en termes d'utilisation des ressources du système par rapport à d'autres bloqueurs de publicités. Elle offre également une interface utilisateur avancée pour ceux qui souhaitent personnaliser leurs filtres.



DR.WEB LINK CHECKER

> VÉRIFICATEUR DE LIENS

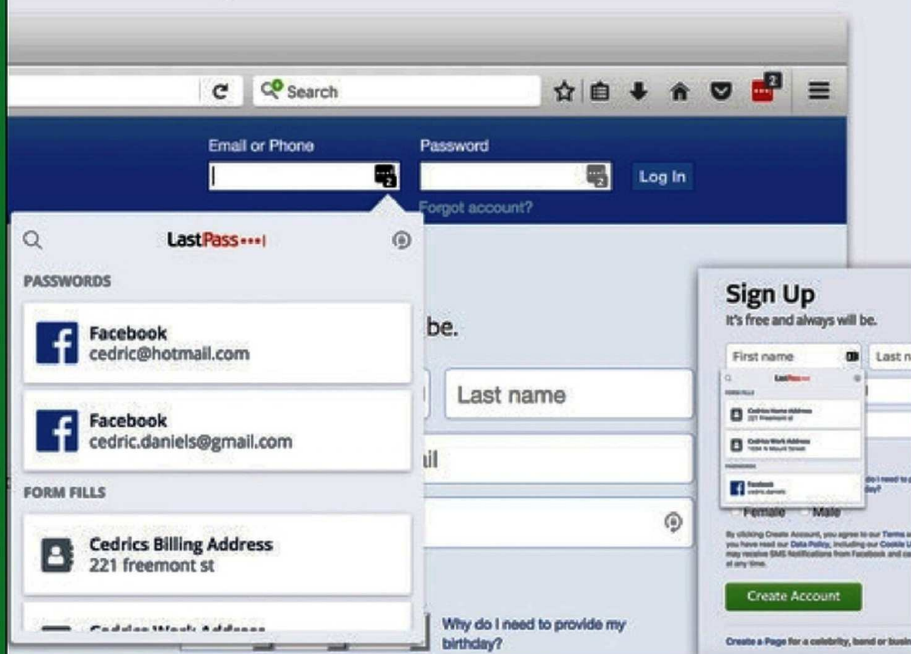
Cette extension utilise le moteur antivirus de Dr.Web pour analyser les hyperliens sur les pages Web, permettant à l'utilisateur de vérifier les liens avant de cliquer, réduisant ainsi le risque d'infection. L'extension utilise le moteur antivirus de Dr.Web pour scanner les liens et les fichiers téléchargés, fournissant ainsi une évaluation rapide du risque potentiel et évitant, en temps réel, de lancer par mégarde un programme malveillant.



LASTPASS > GESTION DE MOTS DE PASSE

LastPass est un gestionnaire de mots de passe conçu pour stocker et gérer en toute sécurité les identifiants de connexion et les mots de passe. Il stocke ces derniers dans un coffre-fort crypté, sécurisé par un mot de passe principal. Cela signifie que vous n'avez besoin de mémoriser qu'un seul mot de passe fort. Il peut générer des mots de passe forts et uniques pour chaque compte puis s'occuper du remplissage automatique de vos identifiants de connexion. En plus des mots de passe, LastPass peut stocker de manière sécurisée d'autres informations sensibles, telles que les notes sécurisées, les informations de carte de crédit et les pièces d'identité.

stantly autofill passwords and forms to all your saved websites





TOP 5

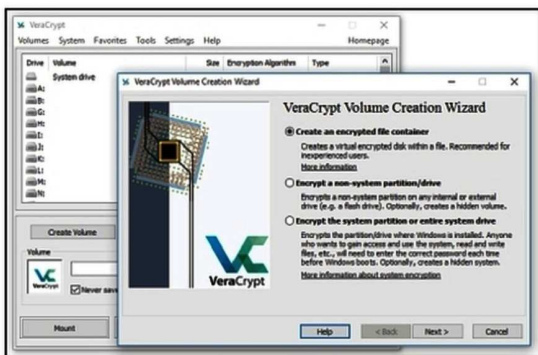


LOGICIELS DE CHIFFREMENT

VERACRYPT > LE NUMÉRO 1

Logiciel open source en français, il offre un chiffrement de qualité professionnelle. VeraCrypt chiffre vos données, partitions de disque et même son chiffrement intégral. Il est compatible avec les périphériques de stockage externes. Par contre, on notera son absence de partage ou d'intégration cloud.

Lien : www.veracrypt.fr



AXCRYPT > LIMITÉ MAIS INTUITIF

Programme open source disponible pour Windows, macOS, Android et iOS. Chiffre, déchiffre et supprime des fichiers et dossiers. La version payante est compatible avec Google Drive et Dropbox. Multilingue avec un gestionnaire de mots de passe. La version gratuite a des fonctionnalités restreintes et un chiffrement 128 bits. Certains réglages par défaut nécessitent une activation manuelle.

Lien : axcrypt.net

BITLOCKER

> TU L'AS OU TU L'AS PAS ?

Outil de chiffrement propriétaire de Windows pour le chiffrement intégral du disque. Il n'est malheureusement pas intégré dans toutes les versions de Windows (vérifier en recherchant **Chiffrement du disque** dans vos **Paramètres**). Avec un chiffrement automatique AES 256 bits, il est facile à configurer et à utiliser, il propose même une protection en cas de vol du disque dur.

Récupération BitLocker

Entrer la clé de récupération de ce lecteur :

Utilisez les touches numériques ou les touches de fonction F1 à F10 (utilisez F10 pour 0).
ID de clé de récupération (pour identifier votre clé) :

BitLocker a besoin de votre clé de récupération pour déverrouiller votre disque car la stratégie de démarrage sécurisé a été modifiée de façon inattendue.

Voici comment trouver votre clé :

- Essayez votre compte Microsoft sur : aka.ms/myrecoverykey
- Pour plus d'informations, accédez à : aka.ms/recoverykeyfaq

Appuyez sur Entrée pour continuer

Appuyez sur Échap pour obtenir d'autres options de récupération

Appuyez sur F11 pour choisir un autre système d'exploitation

ROHOS MINI DRIVE

> POUR VOS CLÉS USB

Rohos crée une partition sécurisée protégée par mot de passe sur votre clé. Ainsi, l'autre partie, non chiffrée, peut encore servir à d'autres usages. Le chiffrement est en AES 256 bits. La zone cryptée est paramétrable, mais ne peut pas dépasser 2 Go dans la version d'essai. Rohos est portable, c'est l'une de ses forces.

Lien : rohos.com

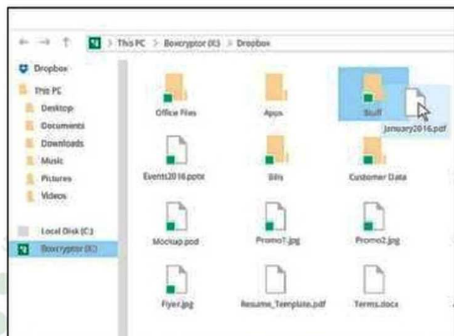


BOXCRYPTOR

> POUR LE CLOUD

Ce programme est spécialisé dans le chiffrement de bout en bout pour le stockage cloud. Il utilise un chiffrement AES 256 bits et RSA et est compatible avec plus de 30 fournisseurs de stockage cloud dont Dropbox, Google Drive et Microsoft OneDrive. La version gratuite est restreinte à deux appareils et à un fournisseur cloud.

Lien : www.boxcryptor.com





ANONYMAT & PROTECTION 1010101010

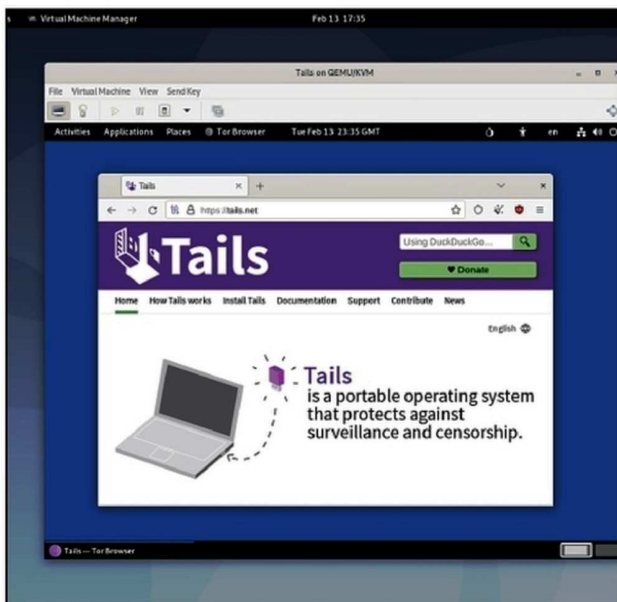


TAILS

ANONYMISE VOTRE PC

Tails, "The Amnesic Incognito Live System", est un système d'exploitation dédié à la sécurité et à la protection de la vie privée. Il s'agit d'un système live, ce qui signifie qu'il peut être démarré à partir d'une clé USB ou d'un DVD sans laisser de traces sur l'ordinateur utilisé après son redémarrage.

Quel que soit votre ordinateur et son système d'exploitation (Windows, Mac, Linux...), vous pouvez avoir besoin de lancer une session vraiment sécurisée sans craindre la présence d'un espion installé sur votre terminal ou qui surveille vos données transitant sur le Web. C'est la promesse de Tails, un système d'opération qui se lance à la demande via un port USB et qui fonctionne comme un container inviolable. Cet OS se base sur Debian GNU/Linux et route l'ensemble du trafic Internet à travers le réseau Tor, masquant ainsi l'identité et la localisation de l'utilisateur.



UN SYSTÈME ENTIER SUR UN SIMPLE SUPPORT USB QUI FONCTIONNE COMME UN CONTAINER INVOLABLE. TAILS EST UTILISABLE À LA DEMANDE, AVEC N'IMPORTE QUEL PC

UN OUTIL ANTI-SURVEILLANCE OU MAFIEUX ?

Tails continue de faire l'actualité, avec des mises à jour régulières qui améliorent ses fonctionnalités et sa sécurité. Toutefois, comme tout outil de protection de la vie privée, Tails fait l'objet de controverses. Certains gouvernements et organisations le voient d'un mauvais œil, arguant qu'il pourrait faciliter des activités illégales en offrant un anonymat presque parfait. Ces critiques sont régulièrement balayées par la communauté Tails, qui souligne l'importance de la vie privée et de la liberté d'expression dans un monde numérique.



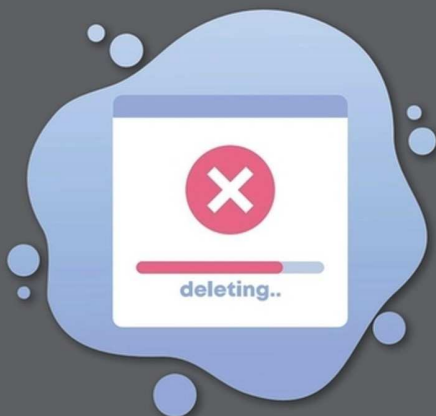
La nouvelle version 6.0 de Tails est sortie en février dernier.

MODE LIVE AVEC AMNÉSIE

Tails est principalement conçu pour être utilisé comme un système live, ce qui signifie qu'il peut être démarré à partir d'une clé USB ou d'un DVD sans avoir à être installé sur l'ordinateur. Plus important encore, il ne laisse aucune trace sur l'ordinateur une fois qu'il est éteint, grâce à sa fonctionnalité d'amnésie. Cela empêche la récupération de l'activité ou des données après utilisation.

CHIFFRER CE QUI DOIT ÊTRE CONSERVÉ

Pour ceux qui souhaitent conserver des documents ou des réglages entre différentes sessions d'utilisation, Tails offre la possibilité de créer un volume chiffré persistant sur la clé USB. Ce volume est chiffré avec une forte cryptographie, protégeant les données en cas de perte ou de vol de la clé USB.



Depuis son lancement en 2009, Tails a constamment évolué, intégrant de nouvelles technologies de chiffrement et de sécurité pour rester à la pointe de la protection des données. Son but premier est de permettre à ses utilisateurs de contrer la surveillance de masse et les attaques informatiques, offrant ainsi un havre de paix dans un monde numérique de plus en plus sous surveillance.

OBJECTIF ANONYMAT !

Tails s'appuie donc sur le réseau Tor pour chiffrer et anonymiser l'ensemble du trafic Internet de ses utilisateurs, rendant ainsi leur navigation véritablement privée. Outre l'accès à un Internet anonyme, Tails comprend une suite d'outils de sécurité préinstallés, parmi laquelle figurent des applications de messagerie chiffrée, de gestion de mots de passe et de cryptage

TAILS : UN PACK « TOUT-EN-UN »

Voici une liste non exhaustive de certaines des fonctionnalités et programmes préinstallés sur Tails. Ces programmes permettent aux utilisateurs de naviguer sur Internet, de communiquer, de gérer des fichiers et d'effectuer des tâches bureautiques tout en minimisant les risques de surveillance et d'analyse de leur activité en ligne.

- **Tor Browser** : un navigateur web modifié à partir de Mozilla Firefox, conçu pour une navigation anonyme via le réseau Tor.

- **Thunderbird** : un client de messagerie électronique pour envoyer et recevoir des emails de manière sécurisée.

- **KeePassXC** : un gestionnaire de mots de passe pour stocker de manière sécurisée tous vos mots de passe.

- **LibreOffice** : une suite bureautique complète pour créer et éditer des documents texte, des feuilles de calcul, des présentations, etc.

- **GIMP** : un programme de manipulation d'images pour l'édition et la création d'images numériques.

- **Audacity** : un logiciel d'édition audio permettant d'enregistrer et de modifier des fichiers audio.

- **Electrum** : un portefeuille Bitcoin pour effectuer des transactions en Bitcoin de manière anonyme.

- **OnionShare** : un outil pour partager des fichiers de manière anonyme et sécurisée à travers le réseau Tor.

- **GNOME Sound Recorder** : un enregistreur de son simple pour enregistrer de l'audio avec un microphone.

- **Pidgin** : un client de messagerie instantanée qui supporte plusieurs protocoles, configuré pour une utilisation anonyme avec OTR (Off-the-Record Messaging) pour le chiffrement des conversations.

- **MAT (Metadata Anonymisation Toolkit)** : un outil pour supprimer les métadonnées des fichiers, réduisant ainsi les risques de fuites d'informations personnelles.

- **Tails Installer** : un outil pour installer Tails sur une clé USB ou un disque dur externe.



PEUT-ON INSTALLER CE QUE L'ON VEUT SUR TAILS ?

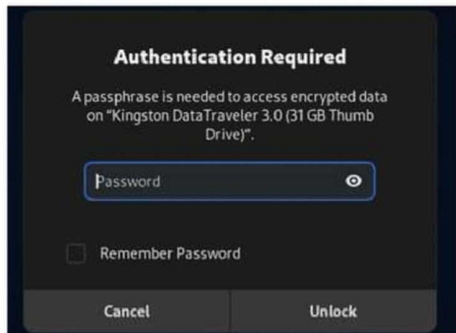
Tails est basé sur Debian GNU/Linux, ce qui signifie que les applications doivent être compatibles avec Linux pour fonctionner. De nombreux programmes populaires sur Windows ou macOS, comme Microsoft Office ou les logiciels Adobe, n'ont pas de versions natives pour Linux. Bien qu'il existe des alternatives Linux pour presque toutes les applications Windows, l'installation de logiciels non pris en charge nativement par Tails peut compromettre les fonctionnalités de sécurité intégrées de Tails. Par exemple, installer et utiliser Google Chrome au lieu du Tor Browser serait une erreur critique : autant jeter Tails à la poubelle !

de fichiers. Tails ne laisse aucune trace sur l'ordinateur utilisé après redémarrage, grâce à son système d'exploitation amnésique, assurant ainsi une couche supplémentaire de sécurité.

SÉCURITÉ PAR DÉFAUT

Tails est conçu avec une approche de sécurité par défaut. Cela inclut l'utilisation de logiciels open source largement audités, la désactivation de composants logiciels potentiellement vulnérables et la configuration par défaut de ses applications pour maximiser la confidentialité et la sécurité. De plus, étant basé sur Debian GNU/Linux, il bénéficie des mises à jour de sécurité régulières et des pratiques de sécurisation du système d'exploitation Linux. En utilisant des outils et des

configurations qui minimisent l'empreinte numérique, Tails rend plus difficile pour les sites web et les services en ligne de suivre ou d'identifier ses utilisateurs.



Vos dossiers chiffrés sont accessibles via mots de passe.

Quel support USB choisir ?

La taille de l'image ISO de Tails varie légèrement avec chaque version, mais elle est généralement autour de 1.1 à 1.2 Go. Cette taille est importante, car elle doit être prise en compte lors du choix du média sur lequel Tails sera installé ou gravé.

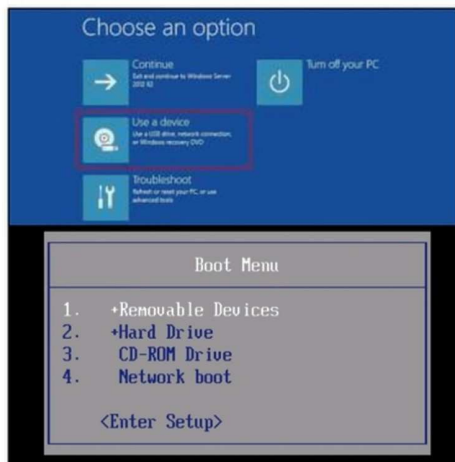
Pour installer Tails sur une clé USB ou un disque dur externe, il est recommandé d'utiliser un périphérique d'au moins 8 Go de capacité. Cette recommandation prend en compte non seulement l'espace nécessaire pour l'image ISO elle-même, mais aussi pour le volume de persistance optionnel qui permet de sauvegarder des données entre les sessions d'utilisation. Un périphérique de plus grande capacité pourrait être nécessaire si vous prévoyez de stocker une grande quantité de données de manière persistante.

Comment lancer Tails ?

TUTO

01 > BOOT USB

Pour démarrer Tails, insérez la clé USB dans un port USB de l'ordinateur, puis redémarrez-le. Vous devrez peut-être accéder au menu de démarrage de l'ordinateur ou modifier l'ordre de démarrage dans le BIOS/UEFI pour permettre le démarrage depuis la clé USB.



02 > CONFIGURER

Une fois que Tails démarre, vous serez accueilli par un écran de bienvenue où vous pouvez configurer des options telles que la langue et le clavier avant d'entrer dans l'environnement de bureau.



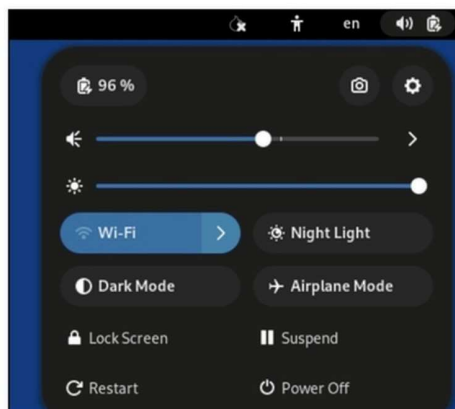
03 > INTERNET

Vous serez bien sûr amené à configurer votre accès Internet et votre connexion à Tor.



04 > ÉTEINDRE

Pour éteindre Tails, cliquez sur le menu d'application en haut à gauche, sélectionnez le bouton d'arrêt, puis choisissez **Éteindre**. Tails se fermera et vous indiquera quand il est sûr de retirer la clé USB.



Il est crucial de suivre cette procédure pour s'assurer que toutes les données temporaires sont effacées et que le volume de persistance (si utilisé) est correctement démonté, préservant l'intégrité des données et la sécurité du système.



TOP 5

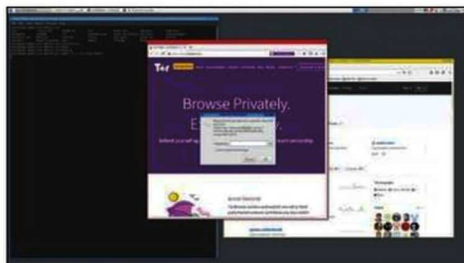
ALTERNATIVES À TAILS

Plusieurs systèmes d'exploitation alternatifs à Tails offrent des niveaux élevés de sécurité informatique, de protection de la vie privée, et d'anonymat. Chacun a ses propres caractéristiques et cas d'utilisation spécifiques. Voici quelques-unes des alternatives les plus notables :

QUBES OS > JE CLOISONNE !

Qubes OS base sa résistance aux intrusions et à la surveillance sur la virtualisation. Il partitionne les différentes parties de l'activité quotidienne de l'utilisateur, comme naviguer sur Internet, travailler sur des documents, ou vérifier les emails, en domaines isolés exécutés dans des machines virtuelles séparées. Cette séparation permet de limiter les dommages potentiels en cas d'attaque logicielle.

Lien : www.qubes-os.org



WHONIX > IP À DOUBLE TOUR

Whonix est un système d'exploitation axé sur l'anonymat, qui utilise également Tor pour tout le trafic Internet et fonctionne sur le principe de la sécurité par l'isolement. Il se compose de deux parties : une «Workstation» où l'utilisateur effectue toutes ses activités, qui est isolée et ne peut pas voir l'IP réelle de l'utilisateur, et une «Gateway» qui route tout le trafic à travers le réseau Tor.

Lien : www.whonix.org

KODACHI LINUX

> INTERNET BLINDÉ

Linux Kodachi route également tout le trafic Internet à travers le réseau Tor et utilise un VPN et des DNS sécurisés pour une couche supplémentaire de protection en ligne. Convient aux utilisateurs qui cherchent une solution tout-en-un pour la navigation sécurisée et anonyme sur Internet.

Lien : sourceforge.net/projects/linuxkodachi/



SUBGRAPH OS

> TOUT TERRAIN

Subgraph OS est un système d'exploitation conçu pour être résistant aux attaques logicielles et à la surveillance en ligne. Il intègre des technologies de sécurité avancées comme le sandboxing des applications, le système de fichiers chiffré, et la communication anonyme via Tor.

Lien : subgraph.com

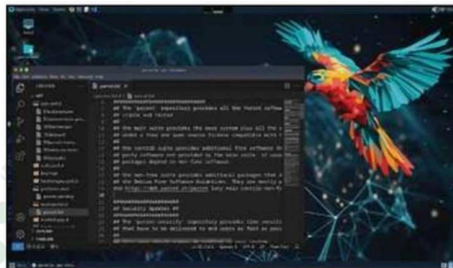


PARROT SECURITY OS

> PRO ET ACCESSIBLE

Parrot Security OS est une distribution basée sur Debian conçue pour les tests de sécurité, l'analyse médico-légale numérique, le piratage éthique, et la protection de la vie privée. Tout en offrant des dizaines d'outils pour les professionnels de la sécurité et les hackers, Parrot OS propose également une édition Home pour une utilisation quotidienne avec un accent sur la confidentialité.

Lien : www.parrotsec.org





TOP 5

ANTIMALWARES
POUR ANDROIDBITDEFENDER
ANTIVIRUS FREE

> GARDIEN SILENCIEUX

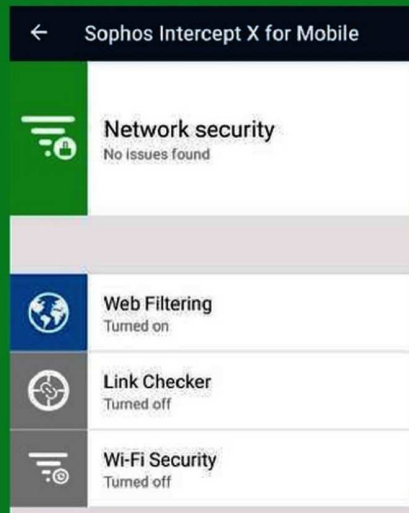
Cette application gratuite brille par sa légèreté, avec son scanner antivirus à un clic. Elle se distingue par son approche de cloud-scanning, offrant une détection avancée des menaces sans alourdir le système. La solution de Bitdefender sait se faire discrète, protégeant sans interrompre l'utilisateur.



SOPHOS INTERCEPT X

> HIGHWAY TO WEB

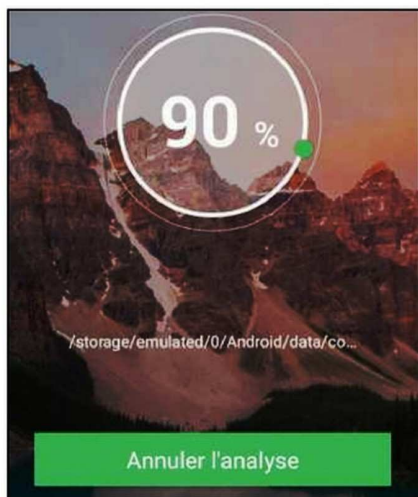
Sa fonctionnalité de scans programmés assure une surveillance continue, tandis que sa protection web exceptionnelle bloque efficacement les sites dangereux. L'appli de Sophos met notamment l'accent sur la protection anti-phishing.



PANDA DOME FREE ANTIVIRUS

> ULTRA-CONNECTÉ

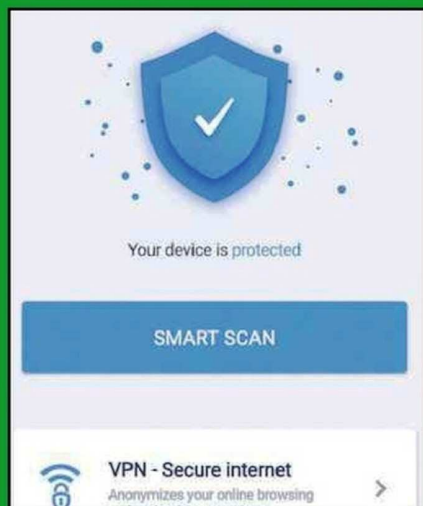
Compatible avec les smartwatches, Panda peut opérer à distance via une montre, pour rester informé des menaces en temps réel. L'application détecte la plupart des malwares, avec un accent sur la protection contre les ransomwares et les spywares.



AVIRA ANTIVIRUS SECURITY

> PROTECTEUR COMPLET

Une solution de sécurité complète : moteur de détection de virus, analyse approfondie des applications, protection des données personnelles, VPN intégré, surveillance Web, etc. Une plateforme à découvrir et à apprivoiser.



KASPERSKY FREE

> SIMPLICITÉ ET PUISSANT

Ses fonctionnalités gratuites se concentrent sur l'essentiel : détection efficace de malwares et protection en temps réel, qui empêche le téléchargement de fichiers nuisibles. Vous pouvez aussi initier des scans depuis une smartwatch (intégration moins avancée que celle de Panda).



Le chat a neuf vies. Le papier en a cinq. (Pour le papier, c'est prouvé.)

Tous les papiers ont droit à plusieurs vies.



journaux - magazines



publicités - prospectus



enveloppes - papiers



catalogues - annuaires



courriers - lettres



livres - cahiers

recyclons-les-papiers.fr



MULTIMÉDIA





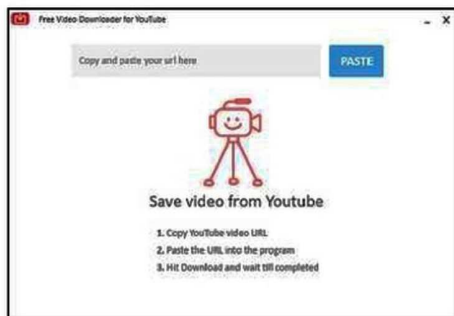
TOP 5

TÉLÉCHARGER
SUR YOUTUBENOTMP3 FREE VIDEO
DOWNLOADER

> POUR LES PURS

Ce logiciel gratuit est à l'aise avec la vidéo comme avec l'audio. Il permet des téléchargements illimités depuis des milliers de sites, offrant ainsi une grande flexibilité et est apprécié pour son efficacité sans chichi et sans pub ! Disponible uniquement pour les utilisateurs Windows.

Lien : notmp3.com

FREEMAKE VIDEO
DOWNLOADER

> TOUT TERRAIN

Freemake Video Downloader est un logiciel de téléchargement vidéo hautement intuitif, adapté pour télécharger des vidéos non seulement de YouTube mais aussi de Facebook, Dailymotion ou Vimeo. Il peut convertir les vidéos dans plusieurs formats et extraire l'audio des fichiers vidéo.

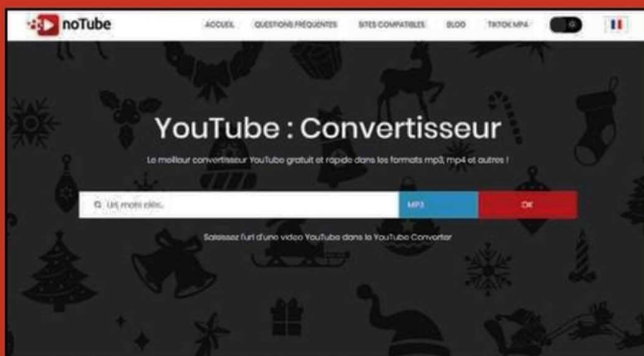
Lien : www.freemake.com



NOTUBE > RAPIDE ET EFFICACE

noTube est un service en ligne sans inscription dédié à la conversion de vidéos YouTube en formats MP3 et MP4. Simple, ergonomie réussie et téléchargement d'un clic ! Pas de limite dans le nombre de vidéos à convertir. Attention, la qualité HD n'est pas sélectionnée par défaut.

Lien : notube.lol



MP3 YOUTUBE

> QUALITÉ DU SON

MP3 YouTube, connu sous le nom de MP3Y, offre une expérience utilisateur épurée pour la conversion de vidéos YouTube



en MP3. Il promet des fichiers de qualité sonore maximale, bien qu'il ne propose pas de réglages de qualité. Son interface sommaire est fonctionnelle et compatible avec plusieurs sites de streaming vidéo.

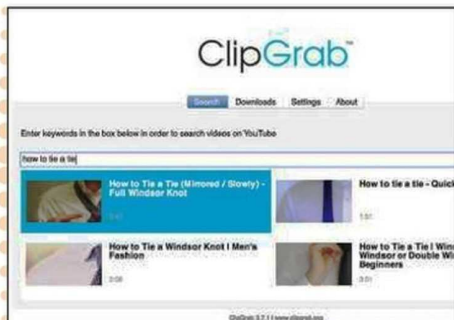
Lien : www.mp3y.org

CLIPGRAB

> RECHERCHE INTÉGRÉE

ClipGrab est compatible avec YouTube, Vimeo et Dailymotion. Un des points forts de ClipGrab est sa barre de recherche intégrée, permettant de trouver des vidéos sans ouvrir un navigateur. L'installateur de ClipGrab propose des logiciels publicitaires, donc une vigilance est nécessaire lors de l'installation.

Lien : clipgrab.de





TOP 3



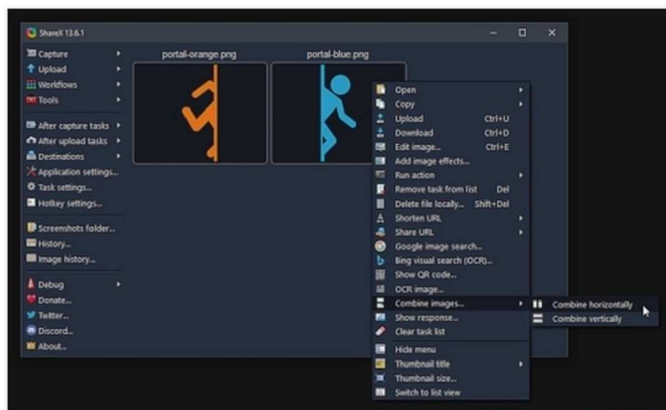
CAPTUREZ DU STREAM EN DIRECT

SHAREX

> PETIT, SIMPLE
MAIS COSTAUD

ShareX est un logiciel de capture d'écran et de capture vidéo polyvalent et léger. Il propose de nombreuses fonctionnalités pratiques pour capturer et enregistrer votre écran. ShareX permet de capturer des régions spécifiques de l'écran, des fenêtres, des objets ou même des pages Web entières. Vous pouvez également enregistrer des vidéos avec audio, capturer des GIF animés, ajouter des annotations et des effets spéciaux, et partager facilement vos captures via divers services en ligne. ShareX est hautement personnalisable et dispose d'une interface conviviale.

Lien : getsharex.com



OBS STUDIO

> LA RÉFÉRENCE
OPEN SOURCE !

OBS Studio (Open Broadcaster Software) est un logiciel de capture vidéo et de streaming en direct très populaire, utilisé par de nombreux streamers et créateurs de contenu. Il

offre une grande flexibilité et de nombreuses fonctionnalités avancées. Vous pouvez capturer des écrans multiples, enregistrer des sources audio et vidéo, créer des scènes personnalisées avec des transitions fluides, et même ajouter des filtres et des effets en temps réel. OBS Studio prend en charge les principaux systèmes d'exploitation (Windows, macOS et Linux) et offre une configuration et une personnalisation poussées.



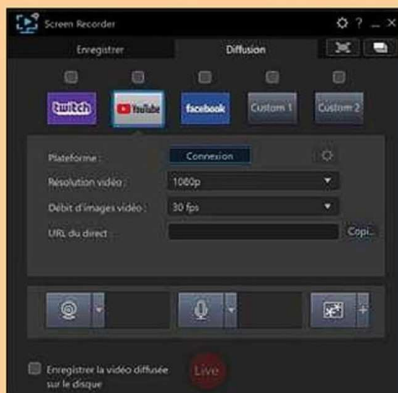
VOIR
NOTRE TUTO
PAGE
SUIVANTE



SCREEN RECORDER 4 ESSENTIAL > PRO ET CONVIVIAL

Avec OBS, il se partage le plébiscite des streamers. Mais il n'est disponible que sur Windows, pas sur Mac. Il se distingue par une pléthore de fonctionnalités et d'options de personnalisation, tout en restant étonnamment convivial, même pour les novices. Lui aussi vous permet de diffuser en direct sur plusieurs plateformes (Twitch, YouTube, Facebook, ...). Grâce à son utilisation efficace des ressources système, il minimise la charge sur le CPU, garantissant ainsi une expérience de jeu fluide et sans interruption. De plus, vous avez le contrôle total sur la résolution vidéo et la fréquence d'images, ce qui vous permet de gérer les ressources nécessaires. Il propose enfin d'autres fonctions avancées pour intégrer une interaction en temps réel avec votre public, utiliser un fond vert ou ajouter une image dans l'image.

Lien : fr.cyberlink.com





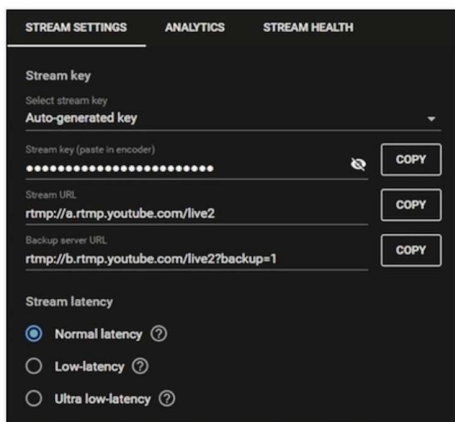
INFOS [OBS STUDIO]

Où le trouver ? [obsproject.com] Difficulté : ☠ ☠ ☠

TUTO

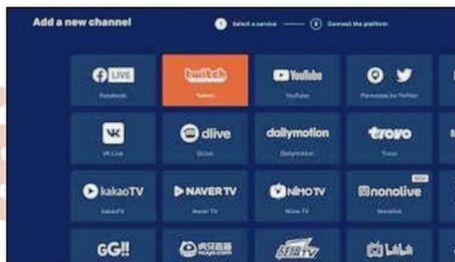
01 > CLÉ DE DIFFUSION

Configurez votre compte de diffusion en direct sur la plateforme de votre choix (YouTube, Twitch, etc.) et récupérez la clé de diffusion (stream key) nécessaire (ici sur Youtube après avoir créé le projet de stream).



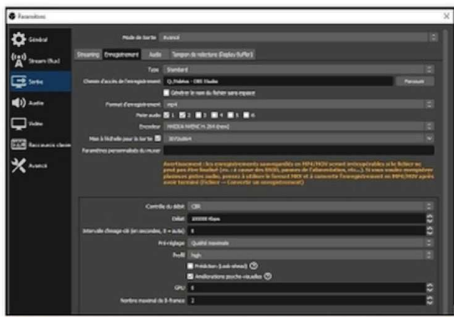
02 > PLATEFORME

Dans OBS Studio, allez dans les paramètres et sélectionnez l'onglet **Streaming**. Choisissez la plateforme de diffusion en direct que vous souhaitez utiliser dans la liste présentée, puis collez votre clé de diffusion dans le champ approprié.



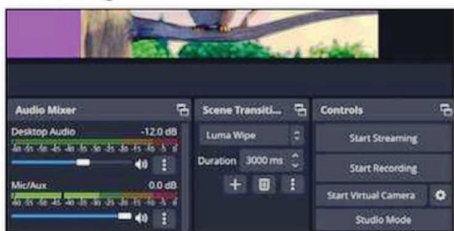
03 > RÉGLAGES

Configurez d'autres options telles que la résolution de la diffusion, le débit binaire, les sources vidéo et audio, etc.



04 > C'EST PARTI!

Une fois que vous avez configuré les paramètres, vous pouvez démarrer la diffusion en direct en appuyant sur le bouton **Start Streaming**.



À SAVOIR

OBS Studio vous permet également de personnaliser votre diffusion en ajoutant des scènes, des transitions, des superpositions, et bien plus encore. Il offre une grande flexibilité pour créer des diffusions en direct professionnelles et de haute qualité.

TOP 3 CLIENTS TORRENT



µTORRENT > LÉGER ET ADAPTABLE

Si vous cherchez un client léger, µTorrent a toute sa place chez vous. Les néophytes préféreront la version web, qui s'intègre dans le navigateur et permet un visionnage direct. La version Windows comporte plus de fonctionnalités (ajouter des torrents à distance, les programmer ou optimiser la bande passante). Il existe également en version mobile.

Lien : utorrent.com/intl/fr

QBITORRENT > L'OPEN SOURCE

qBittorrent est open source et cela lui confère un avantage en terme de transparence et de sécurité. Il est équipé d'un moteur de recherche et d'un lecteur multimédia intégré. Régulièrement mis à jour, il reste léger et simple à utiliser. Son interface ressemble d'ailleurs beaucoup à celle de µTorrent, avec des fonctions similaires.

Lien : qbittorrent.org



WEBTORRENT

> LE PLUS ESTHÉTIQUE

À l'origine, WebTorrent était conçu uniquement pour les navigateurs et rédigé en JavaScript. Il a cependant été développé aussi pour les ordinateurs. Rapide, agréable à l'œil, il permet de visionner les vidéos en streaming. Très léger, il ne consomme qu'une petite fraction de la puissance de calcul de votre ordinateur!

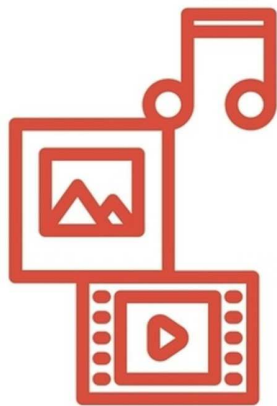
Lien : webtorrent.io





TOP 5

MEDIA CENTERS



KODI > ULTRA-PUISSANT

Kodi est un logiciel open source est connu pour sa flexibilité et sa personnalisation, avec de nombreux add-ons et skins disponibles. Il est compatible avec une large gamme de plateformes, y compris les ordinateurs, les appareils mobiles, les téléviseurs intelligents et les boîtiers de streaming.

Lien : kodi.tv



MEDIAPORTAL

> TOUT-TERRAIN POUR LA TV

MediaPortal est apprécié pour sa prise en charge de la télévision en direct et de l'enregistrement de programmes TV, son intégration de services de streaming et une interface utilisateur personnalisable avec une grande variété de plug-ins et d'extensions.

Lien :

www.team-mediaportal.com

PLEX > L'ERGONOMIE EN PLUS

Plex permet lui aussi de diffuser du contenu multimédia sur différents appareils, y compris les téléviseurs intelligents, les ordinateurs et les smartphones. Il offre également des fonctionnalités de sauvegarde et de synchronisation, ainsi que des options pour gérer et organiser votre bibliothèque multimédia. Plex est reconnu pour sa facilité d'utilisation et son interface utilisateur intuitive.

Lien : www.plex.tv

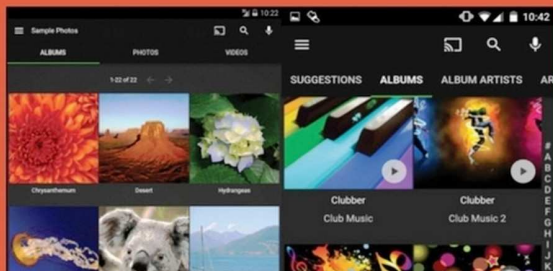


EMBY

> L'EXPÉRIENCE MULTI-UTILISATEURS

Emby, moins populaire, offre cependant des fonctionnalités proches de ses concurrents. Il est apprécié pour sa prise en charge de plusieurs utilisateurs, ainsi que pour ses fonctionnalités de transcodage en temps réel pour une meilleure compatibilité avec différents appareils.

Lien : emby.media



LIBREELEC

> LINUX ET RASPBERRY PI

LibreELEC est une distribution Linux légère liée à la team Kodi, qui peut être installée sur un Raspberry Pi ou un PC. Elle est connue pour sa facilité d'installation et d'utilisation.

Lien : libreelec.tv



TOP 5

TROUVER DE LA MUSIQUE LIBRE DE DROIT



FREE MUSIC ARCHIVE

> GÉNÉRALISTE

Une bibliothèque de musique en ligne avec une grande variété de genres musicaux gratuits, tels que le jazz, le classique, le rock, l'ambient, la musique électronique, etc.

Lien : freemusicarchive.org



SOUNDCLOUD > LA COMMUNAUTÉ

Une plateforme de partage de musique qui permet aux artistes d'uploader leur musique gratuitement et de la partager avec le public. Il existe également des sections dédiées aux remixes et aux playlists d'artistes populaires. La meilleure communauté et une plateforme aux services et à l'ergonomie bluffants !

Lien : soundcloud.com



JAMENDO

> MÉDIATHÈQUE GÉANTE

Une plateforme de musique en ligne qui offre des milliers de morceaux de musique gratuits, sous licence Creative Commons. Les artistes peuvent également commercialiser leur musique sur la plateforme, à destination des particuliers, mais surtout des professionnels.

Lien : www.jamendo.com



Popular



MUSOPEN

> LA PASSION EN PARTAGE

Une bibliothèque de musique classique gratuite, qui offre également des partitions, des enregistrements et des ressources pédagogiques.

Lien : musopen.org/music

CCMIXTER > POUR LES CRÉATEURS

Une communauté en ligne de remixeurs, qui permet de télécharger des chansons, des samples et des pistes instrumentales pour créer de la musique.

Lien : ccmixter.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

CITEO

Le nouveau nom
d'Eco-Emballages et Ecofolio

TROUSSE À OUTILS





TOP 3

SERVICES GRATUITS DE RECONNAISSANCE FACIALE



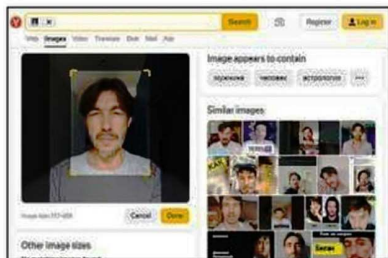
Retrouver une personne, ses publications Internet et ses comptes sociaux non pas à partir d'un nom, mais à partir d'une photo : c'est le principe de la recherche inversée basée sur la reconnaissance faciale. Quels sont les meilleurs services gratuits ?

YANDEX > MEILLEUR QUE GOOGLE IMAGES

La recherche inversée proposée par le moteur de recherche russe fournit d'excellents résultats avec les visages. On sent que les technologies de reconnaissance faciale ont reçu d'importants subsides de la part de l'État russe. Rendez-vous sur la version internationale de Yandex, passez par **Images** et uploadez la photo de votre choix via l'icône caméra. Utilisez l'outil de recadrage pour vous focaliser sur le visage à rechercher. Un petit curseur à positionner vous permet même de retrouver un vêtement ou un objet présent sur l'image.

Bien sûr, les résultats sont proposés par similarité avec, à droite, un diaporama de portraits pouvant correspondre et, en bas à gauche, une liste de liens URL pour retrouver la source. Le problème de Yandex : son indexation du Web étant surinvestie sur le monde russophone, de nombreux résultats y font référence. Mais avouez que c'est amusant de se trouver un sosie de l'autre côté de l'Oural.

Lien : yandex.com



FACECHECK.ID

> ES-TU UN CRIMINEL ?

Un service entièrement consacré à la recherche de personnes parmi plus de 500 millions de visages répertoriés sur le Web. Vous pouvez uploader plusieurs visages pour plus de précision dans les résultats. Ces derniers vous renvoient vers des portraits avec un taux de similarité proposé par ordre décroissant après recherche sur les réseaux sociaux, blogs, vidéos ou encore sites d'actualités. FaceCheck développe aussi sa base à partir de photos de personnes ayant défrayé la chronique judiciaire (en ciblant par exemple les délinquants sexuels). Au cas où vous voudriez vérifier le pedigree de votre dernier match... À la fois malin... et inquiétant. Le service est gratuit, mais un temps d'attente de quelques minutes est nécessaire à chaque nouvelle recherche.

Lien : facecheck.id



VOIR
NOTRE TUTO
PAGE
SUIVANTE



EAGLEEYE

> Go LINUX !

EagleEye est spécialisé dans la recherche de personnes via les photos publiées sur les réseaux sociaux, pros ou grand public. Tout ce dont vous avez besoin est d'au moins une image de la personne que vous recherchez et un nom

ou un petit indice sur le nom de cette personne. Lorsque vous saisissez ces données dans EagleEye, il essaiera de trouver les profils et les comptes Facebook, YouTube, Twitter et Instagram liés à la personne recherchée. Disponible sur Linux, il faudra être familiarisé aux commandes pour exploiter cette solution open source.

Lien : github.com/ThoughtfulDev/EagleEye

```
root@kali:~# EagleEye# python3 eagle-eye.py

EAGLE EYE
Version 0.1
root, you have been activated

==> Enter the persons name to find on FB: Antoon
==> How many jitters, higher is better [max 100]: 100
==> Opening Webdriver
-> Collecting Image URLs...(Page 1)
-> Collecting Images URLs...(Page 2)

:: Starting Face Recognition
...
```




INFOS [FACECHECK]

Où le trouver ? [facecheck.id] Difficulté :

TUTO

01 > UPLOADEZ VOTRE OU VOS PHOTOS

Vous pouvez uploader une ou plusieurs photos via **Browse** ou directement en glisser-déposer dans l'espace concerné. Si vos photos sont trop différentes, vous risquez de perturber l'algorithme. Cependant, des images assez ressemblantes avec des conditions d'exposition similaires sont idéales pour aider FaceCheck.



02 > FILE D'ATTENTE

Cliquez ensuite sur **Search Internet by Face**. Vous êtes placés dans une file d'attente selon l'heure d'affluence du service. Comptez entre 1 et 5 minutes pour que le scan ne démarre automatiquement une fois cette liste purgée.



03 > SCAN

La recherche est lancée, elle prend en moyenne moins de 15 secondes.



04 > À QUI JE RESSEMBLE ?

Les résultats apparaissent par ordre de calcul de similarité selon FaceCheck. C'est le pourcentage que vous avez en haut à droite de chaque portrait. Ici, nous commençons à 60% ce qui est un très mauvais score. Mais rien de plus normal : la personne qui nous a prêté sa photo n'est sur aucun réseau social ni site Web à sa connaissance !



À SAVOIR

FaceCheck dispose d'une extension Chrome. Une fois installée, vous pouvez cliquer avec le bouton droit sur n'importe quelle image de n'importe quel site Web et sélectionner **Find Person with FaceCheck.ID** dans le menu contextuel.

TOP 3 SITES

POUR TROUVER DES PROGRAMMES OPEN SOURCE

GITHUB > LA RÉFÉRENCE POUR LES EXPERTS

GitHub est la plus grande plateforme de collaboration pour le développement de logiciels dans le monde, permettant aux développeurs de stocker, gérer, suivre et collaborer sur des projets. Une mine d'informations et de logiciels à tester ! Bien qu'il ne soit pas le plus intuitif pour les utilisateurs novices, c'est le lieu de prédilection pour trouver de nouveaux logiciels incroyables mais aussi les dernières mises à jour et tutos de certains programmes stars.

Lien : github.com

SOURCEFORGE

> LE LIBRE POUR TOUS !

À la fois destiné aux utilisateurs et aux développeurs, Sourceforge est plus accessible que GitHub. Cette plateforme de distribution de logiciels libres et open source offre une grande variété de logiciels pour différents systèmes d'exploitation et des index de recherche qui facilitent grandement la vie.

Lien : sourceforge.net



FOSSHUB

> VÉRIFIÉS SANS MALWARES

Ce site propose un téléchargement sécurisé de logiciels gratuits et open source, couvrant une large gamme de catégories logicielles. Il est connu pour son engagement envers la sécurité des programmes qu'il héberge. FossHub s'engage à offrir des téléchargements sans logiciels malveillants, adwares, ou spywares.

Lien : www.fosshub.com





TOP 5

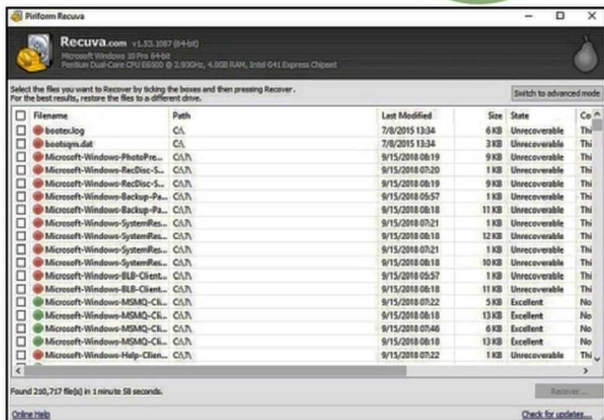
RÉCUPÉRATEURS
DE FICHIERS
EFFICACES

RECUVA

> LE PLUS POPULAIRE

Recuva est un logiciel de récupération de fichiers convivial qui peut récupérer des données supprimées à partir de divers supports de stockage. Il prend en charge la récupération de fichiers dans des situations telles que la suppression accidentelle, la corbeille vidée et les erreurs de formatage.

Lien : www.ccleaner.com/recuva



TESTDISK > EN PROFONDEUR

TestDisk est un logiciel open source conçu pour récupérer des partitions perdues et réparer les secteurs de démarrage endommagés. Il est capable de récupérer des partitions non amorçables et de restaurer la table de partition corrompue.

Lien : www.cgsecurity.org/wiki/TestDisk



MINITOOL POWER DATA RECOVERY FREE EDITION

> LE PLUS POLYVALENT

MiniTool Power Data Recovery Free Edition est un logiciel de récupération de données sous-terrains qui permet de récupérer des fichiers supprimés, ainsi que des partitions perdues ou endommagées. Il prend en charge différents types de fichiers et différents types de supports de stockage.

Lien : <https://urlz.fr/mDKf>



PHOTOREC

> SPÉCIALISTE DES PHOTOS ET VIDÉOS

PhotoRec est un logiciel gratuit de récupération de données axé sur la récupération de fichiers multimédias, tels que les photos, les vidéos et les documents. Il peut récupérer des fichiers à partir de supports de stockage tels que les disques durs, les cartes mémoire et les clés USB.

Lien : www.cgsecurity.org/wiki/PhotoRec



GLARY UNDELETE

Glary Undelete propose lui aussi une interface utilisateur intuitive, propose une recherche rapide ou approfondie ainsi qu'un aperçu des fichiers récupérables. Il offre des options de filtrage des résultats de recherche en fonction du nom, de la taille, de la date de modification, etc., pour vous aider à localiser plus facilement les fichiers recherchés.

Lien : www.glarysoft.com/file-recovery-free/





LES MEILLEURS LOGICIELS ET SERVICES INCLASSABLES...



MAIS INDISPENSABLES !

ANONADDY > SE CACHER DERRIÈRE UN ALIAS !

AnonAddy est spécialisé dans la création d'alias email. Attention, pas d'un email jetable, mais bien d'un alias que vous pourrez piloter depuis votre adresse principale. Un outil puissant et gratuit pour réduire les risques de spam, de phishing et d'autres formes de cyberattaques. Dans sa version gratuite, Anonaddy permet la création d'un domaine avec autant d'alias que nécessaire, redirection automatique des emails vers une adresse principale enregistrée, possibilité de répondre aux emails sans révéler l'adresse principale...

Lien : addy.io



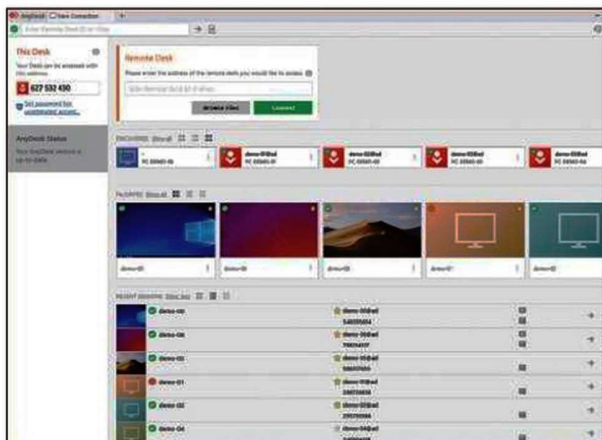
ANYDESK

> PRISE DE CONTRÔLE

À DISTANCE

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

Lien : <https://anydesk.com/fr>



READYBOOST

> BOOSTER SON PC

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





CPU-Z

> QUELLES SONT
LES PERFORMANCES
DE VOTRE PC ?

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

Lien : www.cpuid.com

CPU		Caches	Mainboard	Memory	SPD	Graphics	About
Processor							
Name		AMD FX					
Code Name		Zambezi	Max TDP	125 W			
Package		Socket AM3+ (942)					
Technology		32 nm	Core Voltage	1.312 V			
Specification		AMD FX(tm)-8350 Eight-Core Processor					
Family		F	Model	2	Stepping	0	
Ext. Family		15	Ext. Model	2	Revision	OR-C0	
Instructions		MMX(+), SSE (1, 2, 3, 3S, 4.1, 4.2, 4A), x86-64, AMD-V, AES, AVX, XOP					
Clocks (Core #0)							
Core Speed		4100.16 MHz					
Multiplier		x 20.5					
Bus Speed		200.01 MHz					
Rated FSB							
Cache							
L1 Data		8 x 16 KBytes			4-way		
L1 Inst.		4 x 64 KBytes			2-way		
Level 2		4 x 2048 KBytes			16-way		
Level 3		8 MBytes			64-way		
Selection Processor #1 Cores 8 Threads 8							

XBOOT > MULTI-BOOT ET LIVE CD

Vous utilisez souvent des Live CD pour réparer Windows, faire découvrir Linux ou tester la sécurité d'un réseau ? Avec XBoot il vous sera possible de placer plusieurs ISO sur un CD/DVD ou une clé USB pour choisir la distribution à utiliser lors du boot.

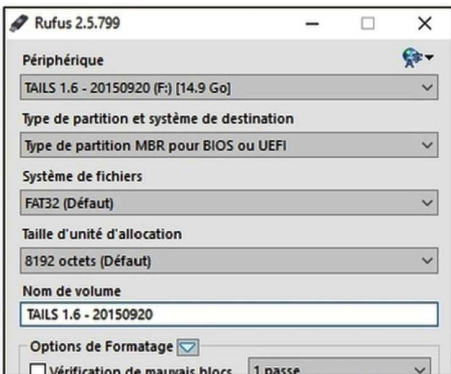
Lien : <http://goo.gl/WnzKd>



RUFUS > CRÉER DES CLÉS USB DÉMARRABLES

Rufus permet de formater et créer des médias USB bootables (clés USB, mémoire flash, etc.) sous Windows. Le logiciel est aussi compatible avec une tripotée de distribution Linux...

Lien : <http://rufus.akeo.ie>





LALA.AI > SÉPARER VOIX ET MUSIQUE

Un service 100 % en ligne et ultra-complet. Cet outil de suppression de voix et de séparation de sources musicales utilise ses propres algorithmes et propose les options les plus nombreuses : supprimez les pistes vocales, instrumentales, de batterie, de basse, de piano, de guitare électrique, de guitare acoustique et même de synthétiseur sans perte de qualité.

Lien : lala.ai



USB CAPTURE > COPIE LE CONTENU D'UNE CLÉ

USB Capture propose très simplement de récupérer tous les fichiers contenus dans une clé «intruse». Vous pourrez donc voir ce qu'un potentiel pirate avait dans la tête lorsqu'il a branché sa clé sur votre précieux poste.

Lien : www.novirusthanks.org/products/usb-capture

Gestionnaire des tâches				
Fichier Options Affichage				
Processus	Performance	Historique des applications	Démarrage	Utilisateurs
Détails	Services			
Nom	PID	Description	Statut	Groupe
USBCaptureSvc	6416	USBCaptureSvc Service	En cours d'exécution	
Avira.ServiceHost	16212	Avira Service Host	En cours d'exécution	
xbgm		Xbox Game Monitoring	Arrêté	
WSearch	1668	Windows Search	En cours d'exécution	
WMPNetworkSvc		Service Partage réseau du Lecteur Wi...	Arrêté	
wmiApSrv		Carte de performance WMI	Arrêté	
WinDefend		Service antivirus Windows Defender	Arrêté	
WdNisSvc		Service Inspection du réseau de l'ant...	Arrêté	
wbengine		Service de moteur de sauvegarde en ...	Arrêté	
VSS		Cliché instantané des volumes	Arrêté	
vds	5360	Disque virtuel	En cours d'exécution	
VaultSvc	936	Gestionnaire d'informations d'identi...	En cours d'exécution	
UioDetect		Détection de services interactifs	Arrêté	
TrustedInstaller		Programme d'installation pour les m...	Arrêté	
TieringEngineService		Gestion des niveaux de stockage	Arrêté	
Steam Client Service		Steam Client Service	Arrêté	

PRIVACY BADGER

> CONTRE LES TRAQUEURS

Cette extension ne fonctionne pas sur une liste de filtrage contrairement à la plupart des bloqueurs. Lorsqu'on consulte un site, Privacy Badger recense les sites tiers (souvent à l'origine des publicités). Si au cours de la navigation, ces sites semblent pister l'utilisateur, Privacy Badger demande au navigateur de les bloquer. Pour ces sites, c'est comme si l'utilisateur avait disparu. L'avantage c'est qu'il n'y a pas de risque de pression de la part des publicitaires pour être retirés des listes de filtrage.

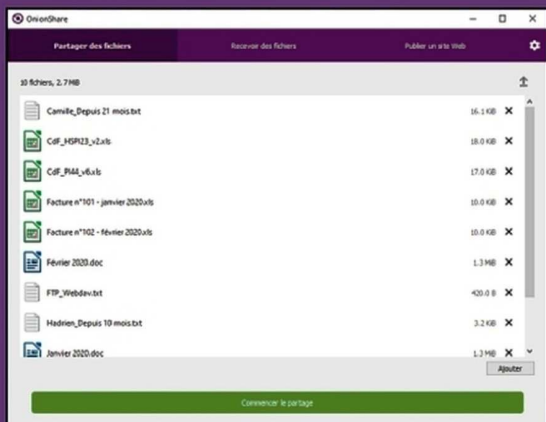
Lien : privacybadger.org



ONIONSHARE > PARTAGEZ DES FICHIERS INCOGNITO

OnionShare va créer un serveur temporaire sur votre ordinateur. Il va générer une URL en .onion uniquement accessible via Tor. La sécurité est de mise puisqu'en plus de cette URL, le logiciel va aussi lui adjoindre une clé unique qui servira à authentifier votre correspondant. Il faudra juste que votre machine reste allumée le temps du transfert. Il est même possible de fermer le serveur lorsque les fichiers seront transférés. Cerise sur le gâteau, votre correspondant n'aura même pas à installer OnionShare pour réceptionner les fichiers puisqu'une simple connexion à Tor depuis son navigateur suffit pour accéder à l'URL de votre service caché.

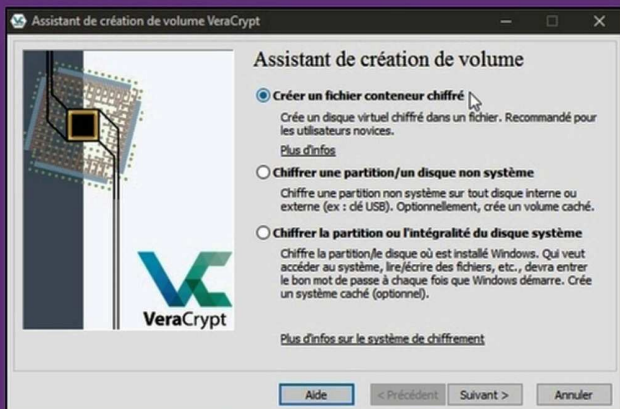
Lien : <https://onionshare.org>



**VERACRYPT** > TU ME VOIS, TU ME VOIS PLUS

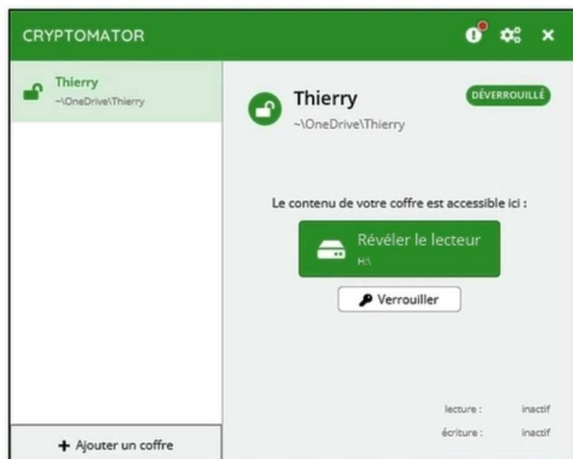
Ce logiciel est open source et développé par une société française, IDRIX (cocorico). VeraCrypt crée un fichier appelé conteneur dans lequel il insère un volume ou un disque virtuel chiffré avec l'algorithme AES-256. Un léger inconvénient de VeraCrypt est que lors de la création de ce disque virtuel il faut spécifier la taille. Les dossiers protégés ne pourront pas dépasser ce poids. Il suffit ensuite de monter le disque virtuel comme un disque réel pour accéder au dossier et à ses documents. C'est cette étape qui est protégée par un mot de passe, il ne faut donc pas oublier de démonter le disque lorsqu'on a fini de travailler ! Il est aussi possible de créer un volume VeraCrypt chiffré sur un support externe (clé USB, ...).

Lien : www.veracrypt.fr

**CRYPTOMATOR**

> LE CLOUD COMME HORIZON

Même si ce logiciel peut sécuriser les dossiers de votre ordinateur, il est spécialisé pour crypter les données que vous mettez sur un cloud, comme Dropbox ou OneDrive. Grâce à l'algorithme AES, vos fichiers sont à l'abri des regards même sur Internet. Il fonctionne sur un principe similaire à VeraCrypt. Cependant, lorsque vous démontez le disque virtuel, Cryptomator ne synchronise avec le cloud que les fichiers que vous avez modifiés, ce qui apporte un gain de temps précieux.

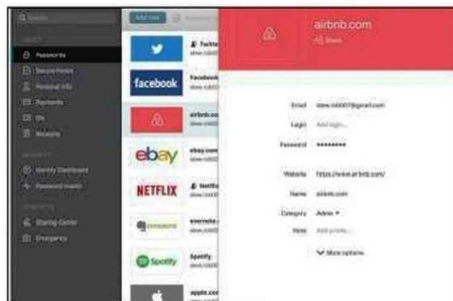


DASHLANE

> LA TENTATION PC

Le très bon et très complet Dashlane (gestionnaire, formulaires, moyens de paiement, notifications, ...) propose ses services gratuitement sur 1 seul poste... ce qui vous poussera peut-être à la version Premium pour vos autres terminaux.

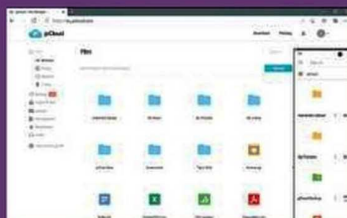
Lien : www.dashlane.com



PCLOUD > JUSQU'À 10 Go DE CLOUD GRATUIT

2 Go gratuits tout de suite et 10 Go rapidement sous forme de récompenses ludiques. Basée en Suisse (et donc protégée par la loi helvétique), pCloud se veut la solution de stockage en ligne « la plus sécurisée d'Europe ». Via votre navigateur, un espace virtuel dédié sur votre PC ou une application mobile : accédez facilement à tous vos fichiers et dossiers, avec les mêmes fonctionnalités que les versions premium, ce qui est assez rare.

Lien : www.pcloud.com



PROGRAM BLOCKER

> BLOQUEZ L'ACCÈS

À CERTAINS PROGRAMMES

Vous souhaitez conserver un usage exclusif d'un ou plusieurs logiciels sur votre PC ? Installez l'outil gratuit Program Blocker (tinyurl.com/y5zewapx). Lancez-le et définissez le sésame que vous voulez. Cliquez ensuite sur **Block Applications**. Dans la fenêtre qui s'affiche, sélectionnez le programme à verrouiller et activez la flèche pointant vers la droite. Validez Par **Save** et fermez Program Blocker. Tentez d'ouvrir le logiciel verrouillé. Saisissez votre mot de passe et cliquez sur **Continue** pour y accéder.





TOP 5

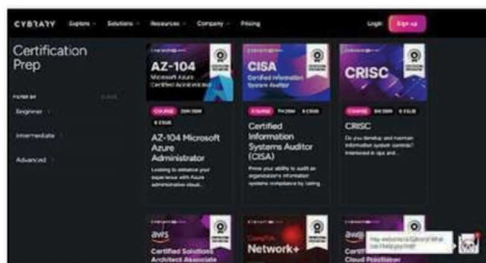


SE FORMER EN CYBERSÉCURITÉ ET HACKING

CYBRARY > TESTEZ UN SPÉCIALISTE

Cybrary est une plateforme en ligne axée sur la sécurité informatique et la cybersécurité. Ils proposent plus de 50 cours gratuits, dont certains avec certification, sur des sujets tels que l'éthique du hacking, la sécurité des réseaux, la gestion des incidents de sécurité, la sécurité des applications, et bien plus encore.

Lien : www.cybrary.it



FRANCE UNIVERSITÉ NUMÉRIQUE

> VIVE L'ACADÉMIE !

FUN est une plateforme française qui propose des MOOC gratuits créés par des établissements d'enseignement supérieur et des organismes de recherche. Bien qu'ils ne soient pas exclusivement axés sur la sécurité informatique, vous pouvez trouver des cours spécifiques sur des sujets liés à la cybersécurité, tels que la protection des données, la sécurité des réseaux, et d'autres domaines connexes. La plateforme est ouverte à tous et propose des cours de différents niveaux de difficulté.

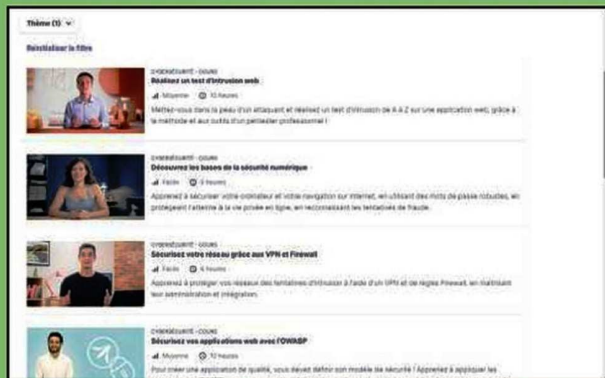
Lien : www.fun-mooc.fr



OPENCLASSROOMS > LE PLUS GÉNÉRALISTE

OpenClassrooms est une plateforme d'apprentissage en ligne qui propose une large gamme de cours gratuits et de parcours payants. Ils couvrent divers domaines, y compris la cybersécurité. Vous pouvez trouver des cours sur des sujets tels que la sécurité des systèmes d'information, le pentesting, la cryptographie, et d'autres aspects de la sécurité informatique.

Lien : openclassrooms.com

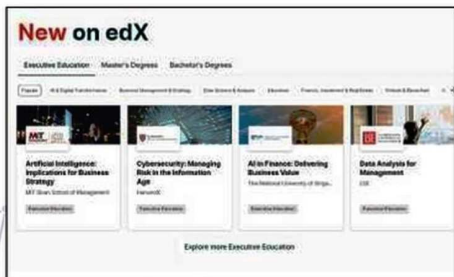


EDX > RÉFÉRENCE

ANGLO-SAXONNE

edX est une plateforme de cours en ligne fondée par Harvard et le MIT. Elle propose une vaste gamme de cours gratuits en informatique, y compris en cybersécurité, programmation et développement web. Les cours sont créés par des universités et des institutions académiques de premier plan.

Lien : www.edx.org



SECNUMACADEMIE

> POUR LE GRAND PUBLIC

Pilotée par l'Agence nationale de la sécurité des systèmes d'information



(ANSSI), cette plateforme ambitionne de former le grand public (chez soi ou en entreprise) aux principaux enjeux cyber et de s'y initier gratuitement grâce à plusieurs modules assez complets.

Lien : secnumacademie.gouv.fr



**FREE JULIAN
ASSANGE**

BONUS

JEUX VIDÉO





BONUS 0101110100110101111010101011010101010101010



RECALBOX > SUR PC ET RASPBERRY PI

[illegible]

Lien : www.recalbox.com/fr

DOSBOX > ÉMULER DU PC SUR PC POUR LES JOUEURS PC

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



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

EMUCONTROLCENTER > ORGANISEZ VOS ROMs

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



Lien : <https://phoenixinteractivenl.github.io/emuControlCenter>



BONUS

01011101001101011110101010110101010101010

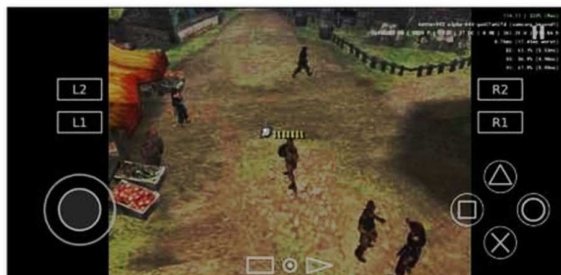
ROMSTATION

> NE PARTEZ PLUS À LA PÊCHE AUX ROMs

Pour jouer à de vieux jeux, il fallait jusqu'à présent télécharger un émulateur, des ROMs ou des ISOs (les jeux au format numérique) et lancer le tout sur votre ordinateur. Il fallait faire la même chose pour chaque système que vous vouliez émuler en cherchant des jeux sur Internet. Avec RomStation, tout va changer ! Depuis la même interface, vous choisissez, téléchargez et jouez à des milliers de jeux sans chercher, décompresser ou bidouiller quoi que ce soit. Il suffit de cliquer

sur un bouton et cela fonctionne puisque tous les émulateurs ainsi que les BIOS nécessaires au fonctionnement sont intégrés dans les 188 Mo du programme. Attention, n'espérez pas émuler de la Wii avec un PC vieux de 5 ans tout de même... Une des fonctionnalités intéressantes du logiciel, c'est la possibilité de mettre en relation d'autres utilisateurs pour jouer à des jeux qui normalement ne permettent le multijoueur qu'en local. Il est donc possible de jouer à *GoldenEye 64*, *Mario 64* ou *Monster Hunter* avec des joueurs distants.

Lien : www.romstation.fr



PCSX2 > PLAYSTATION 2

L'émulateur de référence pour la PlayStation 2, permettant une vaste compatibilité avec les jeux de la console et la possibilité d'augmenter les résolutions graphiques. Avec des mises à jour régulières, PCSX2 s'est amélioré au fil des ans, augmentant sa compatibilité avec un large éventail de jeux et peaufinant l'expérience utilisateur pour offrir une immersion sans précédent. PCSX2 se distingue par sa capacité à exécuter des jeux PS2 en HD, une prouesse qui transforme visuellement l'expérience de jeu. Cet émulateur utilise un système de plugins qui permet une grande flexibilité dans la configuration graphique, sonore, et de contrôle, rendant ainsi possible l'optimisation selon les spécificités du matériel de l'utilisateur. Les fonctionnalités avancées, telles que l'enregistrement de l'état du jeu, le mappage des touches, et le support pour les contrôleurs, sont également au rendez-vous, assurant une expérience de jeu personnalisée et enrichissante.

Lien : pcsx2.net

EPSXE > PLAYSTATION

Pour tous les fans de la PlayStation qui n'ont plus forcément un ancien modèle en état de marche ! Ce logiciel vous permettra de retrouver tous vos jeux préférés sur PC. Ce dernier doit cependant posséder un lecteur CD/DVD. Cet émulateur est compatible avec les systèmes Windows, Mac et Linux. La version pour terminaux Android est, elle, payante.

Lien : www.epsxe.com



ON AIME AUSSI !

DOLPHIN EMULATOR

> WII ET GAMECUBE

Considéré comme l'un des meilleurs émulateurs de Wii et GameCube, Dolphin est capable d'émuler les commandes de mouvement de la manette Wii sans nécessiter de manettes Wiimote.

Lien : fr.dolphin-emu.org/download

PPSSPP

> PSP SUR ANDROID ET PC

Un émulateur spécifiquement pour PSP sur Android et sur PC, qui



est disponible en version gratuite et payante, offrant déjà des fonctionnalités complètes dans sa version gratuite.

Lien : www.ppsspp.org

RETROBAT

> STATION DE GESTION

RetroBat est hautement personnalisable et permet de télécharger, mettre à jour, et configurer les émulateurs les plus renommés directement depuis son interface.

Lien : www.retrobat.org



BONUS

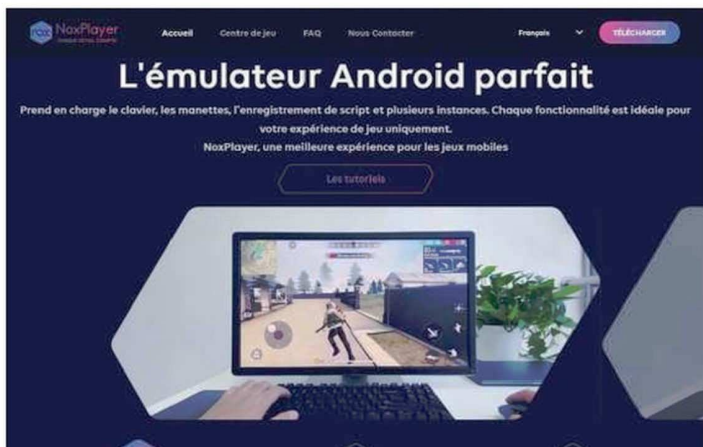
01011101001101011110101010110101010101010

NOXPLAYER

> POUR LES JEUX ANDROID

Retrouvez votre environnement Android sur votre PC. Un accès direct au Playstore vous permet de télécharger et d'ouvrir directement vos jeux. Pour une expérience optimale, configurez manettes, claviers, souris, raccourcis, etc. Vous pouvez enfin opter pour un affichage horizontal ou vertical selon le jeu lancé. Un must qui concurrence déjà BlueStacks et qui le devance sur de nombreux points !

Lien : www.bignox.com



M.A.M.E > LE MEILLEUR DU JEU D'ARCADE !

Multi Arcade Machine Emulator est le plus connu et le plus plébiscité des émulateurs de jeux pour bornes d'arcade. Lui aussi compatible Windows, MAC et GNU/Linux, il met à la disposition des joueurs plus de 40000 titres. Autant dire que vous retrouverez les meilleurs et les pires jeux n'ayant jamais existé ! La configuration manette demande de la précision, mais sachez que Mame peut s'associer à la très populaire manette X-Arcade.

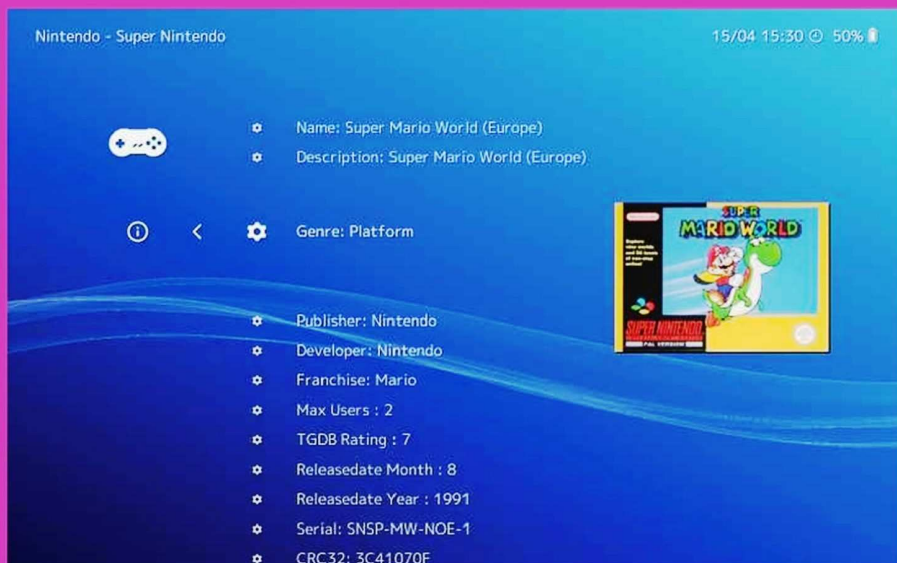
Lien : www.mamedev.org



RETROARCH > MULTI CONSOLES

RetroArch est un émulateur open source qui vous permettra de retrouver sur PC l'expérience de nombreuses consoles et jeux vintage. Gratuit et toujours mis à jour, il est lui aussi multiplateforme et bénéficie même de versions pour Android.

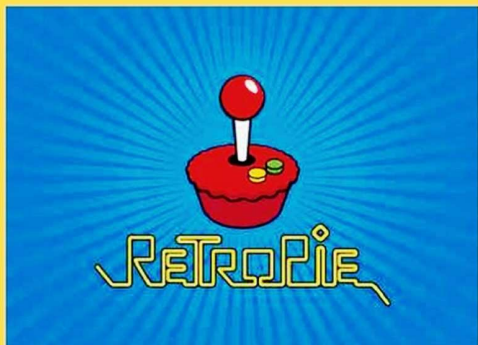
Lien : www.retroarch.com



RETROPIE > VOTRE RASPBERRY DEVIENT BORNE DE JEU !

Cet ensemble d'outils et programmes vous permet d'utiliser votre Raspberry Pi comme émulateur de consoles rétro. Ce kit se base sur le célèbre EmulationStation pour proposer l'une des offres gratuites les plus complètes du marché de l'émulation. Les ressources de ROM libres sont légion, faites-vous plaisir !

Lien : retropie.org.uk



**BONUS**

1010001011101001101011110110110101010101

**TOP 5**

ÉMULATEURS ANDROID

BLUESTACKS 5 > LE LEADER

BlueStacks 5 est l'émulateur à la fois le plus léger et complet du marché. Il fonctionne sur Windows et Mac ; son ergonomie est appréciée des geeks comme des joueurs occasionnels. Les utilisateurs saluent notamment l'accès au Playstore, l'outil de mappage de touches ainsi que le fait de pouvoir exécuter plusieurs jeux simultanément.

Lien : www.bluestacks.com/fr



NOX APP PLAYER

> LE CHALLENGER

Team Nox ou team BlueStacks ? Le combat fait rage. Lui aussi en français, il propose des réglages fins pour optimiser les ressources de votre PC afin d'obtenir la meilleure expérience d'émulation Android. Et, comme avec BlueStacks, le résultat est bluffant et pro, le tout gratuitement et sans pub.

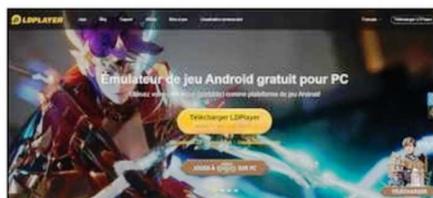
Lien : fr.bignox.com



LDPLAYER

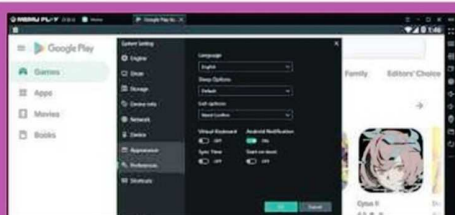
> LA GUERRE DES CLONES

LDPlayer reprend quasiment toutes les bonnes recettes de BlueStacks et on ne le lui reprochera pas. Les ressemblance graphiques, « librement inspirées », en



énervent cependant plus d'un. Sous Android 7.1, il propose la gamme habituelle de fonctionnalités orientées joueur avec un FPS élevé.

Lien : fr.ldplayer.net



MEMU > LES VRAIS SAVENT

À condition d'avoir un PC puissant, MeMu séduit avant tout par ses performances et la fluidité de sa prise en charge. Et comme l'équipe de développeurs travaille à un rythme de dingue, il rattrape petit à petit ses concurrents en terme de fonctionnalités et d'ergonomie. Hier plébiscité par les gamers purs et durs sur mobile, il séduit aujourd'hui le grand public.

Lien : www.memuplay.com

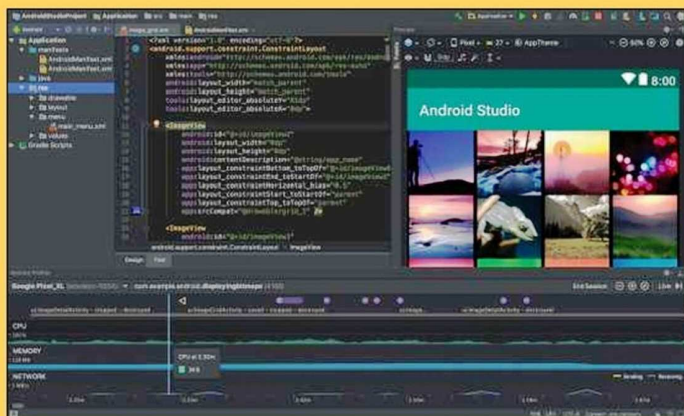
ANDROID STUDIO

> À LA SOURCE!

Android Studio est une console de développement indispensable aux créateurs d'applis pour Android. Elle intègre un émulateur efficace pour tester votre application ou

votre jeu depuis un environnement PC. Pas simple à configurer, Android Studio s'avère très complet pour émuler tout type d'applis du Playstore, personnaliser vos contrôles, etc.

Lien : developer.android.com/studio



**BONUS**

1000101110100110101111010101011010101010101

L'ARSENAL DES TRICHEURS :

11 TECHNIQUES AU CRIBLE

Quelles sont les techniques de triche utilisées en 2024 ? Tour d'horizon des méthodes et hacks utilisés pour doper artificiellement son gameplay.

LES CHEAT CODES

Présents depuis les tout débuts du jeu vidéo, les cheat codes auréolent le joueur qui les utilise d'une certaine aura. Les connaître c'est s'afficher comme un initié auprès de ceux qui les ignorent. Ils se présentent souvent sous la forme de mots à saisir ou de touches à presser dans un ordre précis. À la clé, des bonus comme de l'argent, de l'énergie ou des vies supplémentaires, des munitions inépuisables ou l'accès à l'immortalité. Il peut aussi s'agir de révéler un niveau caché ou un personnage original. Cerise sur le gâteau, les codes de triche n'ont rien de répréhensible. Ils font en effet partie intégrante du jeu, dévoilés sciemment ou non par les développeurs ou les éditeurs eux-mêmes. Pourquoi ? Parce qu'ils apportent du fun tout en étant maîtrisés par l'éditeur. Impossible donc de s'en servir en compétition ou contre d'autres joueurs à leur insu. Très populaires dans les années 90-2000, ils demeurent présents aujourd'hui dans de nombreux jeux, souvent complétés par des « easter eggs » (œufs de Pâques) présentant un clin d'œil humoristique ou un délire du développeur. Pour les dénicher, les sites Web spécialisés comme **supercheats.com** ou **cheatcodes.com** ont pris la relève des magazines d'antan.



Qui a dit que les cheat codes avaient disparu ? Ici, dans les Sims 4 (Maxis/Electronic Arts), un simple mot entré dans la console offre de faire le plein de Simflouz.

LE CHEAT ENGINE

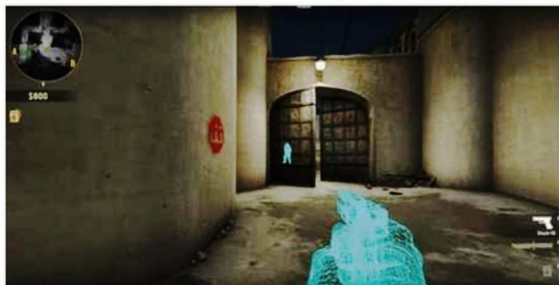
Les codes de triche peuvent aussi prendre des allures beaucoup plus techniques. Le joueur peut intervenir directement sur le fichier de sauvegarde du jeu à l'aide d'un logiciel tel que le Cheat Engine. La méthode, appelée Trainer, n'est pas nouvelle (elle était déjà en vigueur à la fin des années 80 pour modifier des jeux sur Atari ST ou Amiga) mais le Web la rend plus accessible. Les forums des sites spécialisés dans les jeux vidéo regorgent de cheat codes à appliquer en modifiant les codes hexadécimaux (Hex) de la sauvegarde d'un jeu. Le hack touche aussi bien les titres sur PC que sur console, à l'instar de la Nintendo Switch où il suffit d'installer une app particulière (que l'on ne trouve évidemment pas sur la boutique en ligne de l'éditeur) pour procéder aux modifications. Il devient possible de s'octroyer quelques bonus dans *Animal Crossing*, *Pokemon Sword & Shield* ou encore *Fire Emblem*. Si, dans un jeu solo, la manipulation ne satisfait que le plaisir personnel du joueur, dans un jeu multijoueurs, l'altération des fichiers lui procure de sérieux atouts vis-à-vis des autres (en faisant par exemple grimper artificiellement ses points d'expérience) et se trouve sévèrement punie.



Quelques modifications dans le fichier de sauvegarde et le jeu Mario Odyssey (Nintendo) sur Switch devient tout de suite plus facile à finir.

LE WALLHACK

Comme le aimbot (ils fonctionnent d'ailleurs souvent en duo), le Wallhack est un petit programme de triche niché dans le répertoire du jeu. Son but : permettre au joueur de voir à travers les murs et donc de détecter les adversaires qui s'estiment normalement à l'abri des tirs. De plus, le Wallhack couplé à l'aimbot donne la possibilité de tirer à travers les murs, quelle que soit leur nature mais aussi la distance. Un avantage indéniable sur les adversaires, lui aussi sévèrement sanctionné si l'on se fait pincer.



Qui n'a pas rêvé de voir à travers les murs. C'est le principe du Wallhack, très prisé dans les MMO comme ici avec Counter Strike : Global Offensive (Valve).



LES AIMBOT

Voilà une invention redoutable contre laquelle s'énervent les joueurs honnêtes et qui est généralement sanctionnée par un bannissement à vie si elle est détectée. L'Aimbot est un petit programme qui vient se greffer à un jeu de type FPS MMO. Comme son nom l'indique (aim pour visée et bot pour robot) il s'agit de doter son personnage d'un système de visée automatique. Sitôt qu'un joueur adverse entre dans le champ de vision, il est instantanément détecté, verrouillé et éliminé par un tir automatique en pleine tête pour cumuler plus de points sans qu'il ne soit nécessaire d'effectuer la moindre action. Pratique non ? À chaque jeu son aimbot et certains sont personnalisables. Ils offrent de choisir d'effectuer un tir sur une autre partie du corps ou de retarder le coup pour ne pas se faire détecter. Sur les consoles, la mise en place d'un aimbot passe par l'ajout d'une manette « moddée » c'est à dire modifiée pour ajouter des actions automatiques à certains boutons. Attention : les aimbots ne sont pas gratuits. Ils peuvent être proposés sous forme d'abonnement accompagnés d'autres outils de triche. On trouve ainsi des packs valables 3 mois pour une quarantaine d'euros quand les plus perfectionnés peuvent se négocier autour de 150 € ! Reste que ces outils, contrairement à ce qu'annoncent leurs concepteurs, ne sont pas tous indétectables par les logiciels anti-triche nichés dans les jeux ou sur les serveurs. Le propriétaire d'un tel arsenal, s'il est démasqué, se trouve banni à vie du jeu et perd du même coup son investissement.



Ne jamais rater un seul tir, c'est le but des aimbots, ces programmes de triche les plus répandus dans les MMO comme dans Call of Duty Warzone (Infinity Ward/Activision).

LE GHOSTING

C'est bien connu, à deux, on est plus fort. Ce principe peut être mis en œuvre dans les MMO mais de façon sournoise. Ici, un joueur parcourt le terrain tandis qu'un complice, sur une autre machine, l'assiste en tant que spectateur de la partie (il peut même observer à travers le regard d'un adversaire). Facile dès lors de l'informer à la volée des positions ennemies sur la carte, des emplacements de points de ravitaillement, etc.

Un peu comme si au poker, un ami invisible vous indiquait au creux de l'oreille les cartes de vos adversaires. Une technique de triche difficilement décelable sur le coup mais qui implique un vrai travail d'équipe. Au Ghosting s'ajoute le Boosting. Il s'agit là de compter sur la bonne volonté d'un complice acceptant de voir son avatar se faire tuer encore et encore par son partenaire pour que ce dernier augmente artificiellement son score.



Avec l'aide d'un comparse qui surveille le jeu comme spectateur, il devient tout de suite plus simple d'anticiper la présence des ennemis sur le terrain comme ici dans Counter Strike : Global Offensive (Valve).

L'ESP

L'Extra Sensory Perception (pour perception extra sensorielle) est un module bien pratique dans les MMO. Il agit tel un agent de renseignement en localisant les joueurs adverses, leur état de santé, leur inventaire, etc. mais aussi tous les

points de ravitaillement pour refaire le plein de munitions et d'armes. Une sorte de troisième œil qui se fiche pas mal des obstacles, du terrain et des distances. L'ESP fait souvent partie d'un pack de hacks avec l'aimbot et le Wallhack.



Bien pratique l'ESP pour repérer sur la carte les ennemis mais aussi les points de ravitaillement comme ici avec le jeu Apex Legends.

**BONUS**

1000101110100110101111010101011010101010101

CRONUS ZEN, L'ACCESSOIRE AU BANC DES ACCUSÉS

Il existe de nombreux périphériques destinés à améliorer ses performances sur PC et consoles. Certains joueurs considèrent que ces matériels améliorent le game play et le fun tandis que d'autres (la majorité) estiment que ces boîtiers vendus plusieurs dizaines d'euros sont des hacks favorisant les tricheurs au détriment des joueurs véritables.

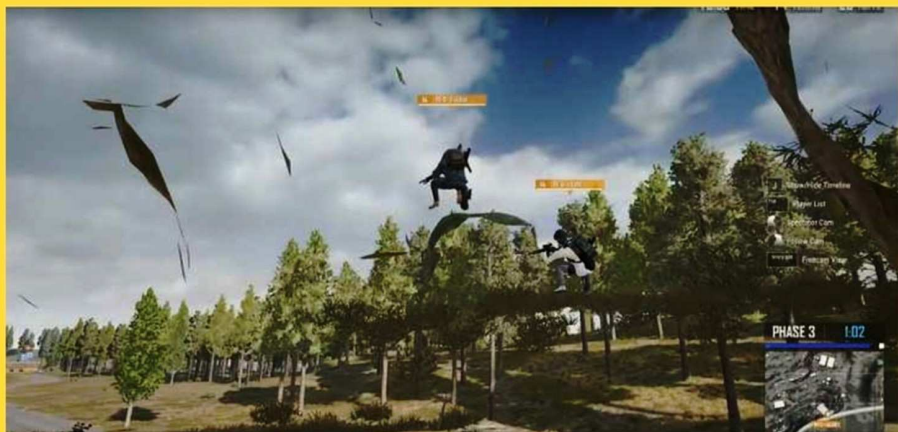
L'un des périphériques les plus connus est le Cronus Zen, un accessoire controversé utilisé par certains joueurs pour tricher dans des jeux vidéo, notamment sur PS5. Il permet de connecter presque n'importe quel contrôleur à n'importe quelle console, personnaliser les commandes et automatiser certaines actions dans les jeux, donnant un avantage jugé injuste par les autres joueurs. Récemment, une mise à

jour de la PS5 a bloqué l'utilisation du Cronus Zen, ce qui a été salué par la communauté qui cherche à préserver l'équité dans les jeux en ligne. Sony a également pris des mesures pour exclure définitivement les joueurs PC utilisant des outils similaires pour tricher sur PS5.



LE GLITCHING

Aucun jeu n'est exempt de bugs d'affichage ou de comportement, ce que l'on appelle les glitch. Ceux-ci peuvent être mis à profit dans bien des situations. Dans un MMO par exemple, ils peuvent permettre de se cacher dans un mur ou un rocher et préparer une embuscade parfaite. Associé à la technique du Bunny Hopping qui consiste à sauter en permanence pour aller plus vite, il est possible de se servir d'un objet pour sauter dessus à répétition et prendre beaucoup d'altitude. Ce mode de triche est généralement puni d'une exclusion temporaire ou permanente du jeu en cas de récidive.



Difficile de trouver une bonne cachette. Sauf à profiter des bugs d'affichage du jeu comme ces deux tricheurs dans Fortnite d'Epic Games.

LE SWITCH LAG

Technique de triche assez bien élaborée mais également interdite, le Switch lag consiste à manipuler la connexion réseau de son PC. En bloquant temporairement les données sortantes de la machine mais en conservant un flux normal de données entrantes, on provoque ainsi un lag (ralentissement de l'affichage) chez les autres joueurs. L'avatar n'apparaît plus que par intermittence sur leurs écrans. Mais du côté du tricheur, les adversaires demeurent bel et bien visibles et on peut donc les éliminer plus facilement.



BONUS

11000101110100110101111010101011010101010101

LE TEXTURE HACK

Difficile de bien distinguer les ennemis qui vadrouillent sur le terrain vêtus d'une combinaison de camouflage. En modifiant la texture de leurs vêtements, il devient nettement plus aisé de les identifier et de les éliminer. C'est ce que propose le Texture Hack. Les adversaires se parent d'une couleur rouge vif qui ruine leur discrétion. Elle peut même virer au jaune canari sitôt qu'ils épaulent leur fusil de sniper. Une technique de triche punie d'un bannissement permanent du jeu.



Lorsque l'on peut faire briller ses ennemis de mille feux, c'est plus facile de les repérer sur le terrain comme ici dans Call of Duty Warzone (Infinity Ward/Activision).

LE SCRIPTING

Dans les jeux vidéo, la rapidité d'exécution reste un atout majeur pour gagner. Et lorsqu'il faut effectuer successivement plusieurs manipulations, ne pas s'emmêler les doigts sur les touches ou les boutons devient un vrai défi. La parade ? Enregistrer ces étapes dans un script qu'il suffira de lancer en pressant une unique touche. Des scripts prêts à l'emploi sont disponibles pour bon nombre de jeux sur le Web et compatibles avec un large éventail de manettes. Mais là aussi, le Scripting est souvent mentionné comme outil de triche dans les conditions d'utilisation des jeux. Il est généralement sanctionné d'une expulsion temporaire.



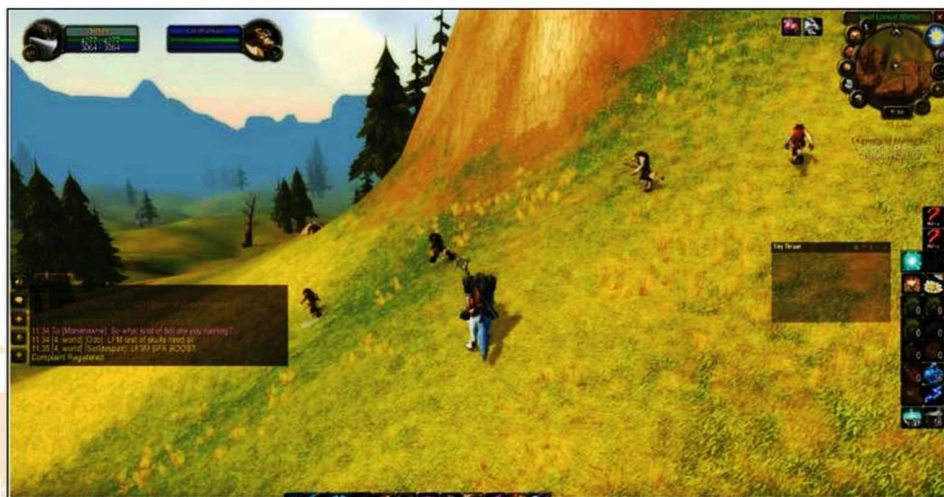
Lorsqu'il s'agit d'enchaîner les actions, mieux vaut faire preuve de dextérité avec la manette sauf à enregistrer un script comme ici dans Pro Evolution Soccer de Konami.

LES FARMING BOT

Pour progresser dans certains jeux, il faut en passer par des phases barbant et longues durant lesquelles on doit procéder à des tâches répétitives. Accomplir ces « quêtes » permet par exemple de récolter de la monnaie virtuelle pour ensuite, améliorer son équipement ou ses installations. Plutôt que de passer ses journées devant l'écran, il est possible de confier ces épreuves à un bot (robot) et ainsi d'automatiser le travail. On peut ainsi laisser tourner le jeu et vaquer à d'autres occupations. Une méthode qui a poussé Blizzard à suspendre plus de 70 000 comptes dans *World of Warcraft Classic* l'été dernier. Aux Farming bots s'ajoutent les Anti-AFK (Away from keyboard). Des petits programmes prennent le contrôle des gardes qui surveillent par exemple votre camp ou votre village lorsque vous n'êtes plus devant votre écran. Ils empêchent ainsi les tentatives d'invasion pendant votre absence. L'utilisation de tels robots est formellement interdite.



IL EXISTE AUTANT DE TECHNIQUES DE TRICHE QUE DE STYLES DE JOUEURS. POUR LE FUN OU POUR LA GAGNE SANS SCRUPULE, CHOISI TON CAMP.



Dans les jeux de stratégie comme *World of Warcraft Classic* (Blizzard), confier les tâches de surveillance à des personnages dirigés par un programme de triche permet de quitter l'écran du jeu sereinement.



**LES JEUNES,
ON LEUR FABRIQUE
DES VÊTEMENTS
PAS CHERS ET
AU LIEU DE DIRE
MERCI, ILS LUTTENT
CONTRE LE TRAVAIL
DES ENFANTS.**

BIENVENUE AUX IDÉALISTES.

**ON SE BAT ENSEMBLE.
ON GAGNE ENSEMBLE.**

**AMNESTY
INTERNATIONAL**



Casser les codes et décrypter l'info

JE M'ABONNE à **PIRATE** INFORMATIQUE

LIVRAISON
SOUS PLI
DISCRET

OFFRE ABONNEMENT

1 AN POUR 17 €

(au lieu de ~~19,60 €~~)

2 ANS POUR 29,40 €

(au lieu de ~~39,20 €~~)



À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À RENVOYER SOUS ENVELOPPE AFFRANCHIE À :

BII - SERVICE ABONNEMENT - 15, RUE DE MERY - 60420 MÈNÉVILLERS

- ☐ Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 17,00 €
- ☐ Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 29,40 €

☐ **OUI, JE M'ABONNE :**

Nom _____

Prénom _____

Adresse _____

Code Postal _____

Ville _____

E-Mail _____

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

Offre valable en France métropolitaine
uniquement.

POUR NOUS CONTACTER :
abonnement@idpresse.com



Signature obligatoire :

Offre valable jusqu'au 31 décembre 2024. Les délais
d'acheminement de La Poste varient selon les régions et
pays. Conformément à la loi Informatique et Libertés du
6/1/1978, vous disposez d'un droit d'accès et de rectification
quant aux informations vous concernant, que vous pouvez
exercer librement auprès de ID PRESSE - IMPASSE DE
L'ESPÉRON - VILLA MIRAMAR - 13960 SAUSSET LES PINS



BEST-OF 2024

l'adresse



L 14376 - 38 - F: 3,90 € - RD



BEL/LUX : 5,00 € - CH : 6,50 CHF - PORT. CONT.
5,20 € - DOM : 5,10 € - POL/S : 700 XPF - N
CAL/S : 700 XPF - MAROC : 45 DH - TUNISIE :
6,50 TND - CAN : 7,50 CAD