Améliorer la sécurité, la confidentialité et l’anonymat de votre smartphone

Michel NALLINO

Nice, France, 2025-09-20 – Révision 4

Liens internes au document

1. Introduction

Les smartphones ont envahi nos vies, au point qu'ils apparaissent parfois comme absolument nécessaires. Cependant, bien que pratiques, ils sont souvent perçus comme des « espions dans la poche », au point que certaines personnes refusent de les utiliser.

L'objectif de ce petit guide est de montrer comment améliorer la sécurité, la confidentialité et l'anonymat de votre smartphone, quel que soit le type de votre appareil, de votre smartphone Android ou de votre iPhone Apple.

Quelques chiffres : Il y a aujourd'hui 8,6 milliards de smartphones utilisés dans le monde par 7,3 milliards d'utilisateurs. Les smartphones Android actifs sont de 5,4 à 5,6 milliards, et les iPhones actifs représentent plus d'un milliard.

2. Résolveurs DNS filtrants

Les résolveurs DNS filtrants sont des outils communs aux smartphones Android et aux iPhones pour augmenter leur sécurité et leur confidentialité.

Ainsi, ce chapitre est valable pour les deux types d'appareils, et la façon de les utiliser sera expliquée dans les chapitres dédiés correspondants.

2.1) Cloudflare avec filtrage des maliciels :

Adresse IPV4 du serveur primaire : 1.1.1.2

Adresse IPV4 du serveur secondaire : 1.0.0.2

Adresse IPV6 du serveur primaire : 2606:4700:4700::1112

Adresse IPV6 du serveur secondaire : 2606:4700:4700::1002

DNS over HTTPS: https://security.cloudflare-dns.com/dns-query

DNS over TLS: security.cloudflare-dns.com

2.2) Cloudflare avec filtrage des maliciels et du contenu pour adultes :

Adresse IPV4 du serveur primaire : 1.1.1.3

Adresse IPV4 du serveur secondaire : 1.0.0.3

Adresse IPV6 du serveur primaire : 2606:4700:4700::1113

Adresse IPV6 du serveur secondaire : 2606:4700:4700::1003

DNS over HTTPS: https://family.cloudflare-dns.com/dns-query

DNS over TLS: family.cloudflare-dns.com

2.3) OpenDNS Protection familiale :

Adresse IPV4 du serveur primaire : 208.67.222.123

Adresse IPV4 du serveur secondaire : 208.67.220.123

Adresse IPV6 du serveur primaire : 2620:119:35::123

Adresse IPV6 du serveur secondaire 2620:119:53::123

DNS over HTTPS: https://doh.familyshield.opendns.com/dns-query

DNS over TLS: familyshield.opendns.com

NB: Cisco a arrêté les activités d'OpenDNS en France, en vigueur depuis le 28 juin 2024. Voir :

https://support.opendns.com/hc/en-us/articles/27951404269204-OpenDNS-Service-Not-Available-To-Users-In-France-and-Portugal (le service a depuis été réactivé au Portugal).

2.4) Résolveur DNS configurable de Rethink :

Rethink propose, gratuitement pour le moment, un résolveur DNS filtrant que l'utilisateur peut configurer.
Il y a deux façons de le faire:

* configuration « avancée », sur https://rethinkdns.com/configure, vous sélectionnez les filtres que vous voulez dans une liste de plus de 190 ;

* Configuration « simple », à partir de la page Web précédente, vous cliquez sur le bouton « Simple », et vous sélectionnez des catégories complètes de filtres (Adult, Piracy, Gambling, Dating, Social Media, Security Full, Security Extra, Privacy Lite, Privacy Aggressive, Privacy Extreme) ;

Dans les deux cas, une fois votre sélection terminée, vous obtenez un nom de résolveur DNS en tant que DNS over TLS (DoT) ou DNS over HTTPS (DoH).

Exemple : après avoir sélectionné parmi la page de configuration simple Security Full et Privacy Aggressive, vous obtenez le nom de résolveur DNS suivant, en tant que DoT :

« 1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com ».

2.5) Résolveurs DNS de Mullvad :

Mullvad a ouvert à tout le monde ses serveurs DNS, utilisés avec Mullvad VPN, en tant que service gratuit.

Noms d'hôte et bloqueurs de contenu

Le tableau ci-dessous montre les différentes options de noms d'hôte et leurs bloqueurs de contenu. Reportez-vous-y lors de la configuration du DNS en suivant les instructions ci-dessous.

Nom d'hôte	Publicités	Pisteurs	Malware	Adultes	Paris
dns.mullvad.net					
adblock.dns.mullvad.net	✅	✅			
base.dns.mullvad.net	✅	✅	✅		
extended.dns.mullvad.net	✅	✅	✅		
family.dns.mullvad.net	✅	✅	✅	✅	✅
all.dns.mullvad.net	✅	✅	✅	✅	✅

Adresses IP et ports

Le tableau ci-dessous indique les adresses IPV4 et IPV6 des différents noms d'hôtes.

Nom d'hôte	Adresse IPV4	Adresse IPV6	Port DoH	Port DoT
dns.mullvad.net	194.242.2.2	2a07:e340::2	443	853
adblock.dns.mullvad.net	194.242.2.3	2a07:e340::3	443	853
base.dns.mullvad.net	194.242.2.4	2a07:e340::4	443	853
extended.dns.mullvad.net	194.242.2.5	2a07:e340::5	443	853
family.dns.mullvad.net	194.242.2.6	2a07:e340::6	443	853
all.dns.mullvad.net	194.242.2.9	2a07:e340::9	443	853

Noms en mode DNS over HTTPS:

https://dns.mullvad.net/dns-query

https://adblock.dns.mullvad.net/dns-query

https://base.dns.mullvad.net/dns-query

https://extended.dns.mullvad.net/dns-query

https://family.dns.mullvad.net/dns-query

https://all.dns.mullvad.net/dns-query

Les résolveurs DNS de Mullvad n'utilisent que les modes chiffrés DoH ou DoT, et non pas le mode non chiffré UDP / 53. Les listes de filtres utilisés par les résolveurs DNS de Mullvad sont disponibles ici : https://github.com/mullvad/dns-blocklists.

Plus d'informations sur les résolveurs DNS de Mullvad ici: https://mullvad.net/en/help/dns-over-https-and-dns-over-tls.

2.6) Résolveurs DNS souverains et conformes au RGPD pour les citoyens de l'UE:

Il y a deux initiatives de résolveurs DNS souverains, conformes au RGPD :

- « Souverain » : les serveurs sont à l'intérieur de l'UE, et il y a au moins un serveur dans chacun des 27 pays de l'UE,

- « Conforme au RGPD »: offrant la meilleure protection contre la confidentialité à ses utilisateurs, conformément à la réglementation générale de la protection des données de l'UE, voir https://gdpr-info.eu/,

- « Compatible DNSSEC »: les réponses DNS sont signées par les serveurs.

* DNS4EU, financé par l'UE, voir https://www.joindns4.eu/. Ce résolveur DNS existe en cinq versions :

Nom d'hôte	Publicité	Pisteurs	Maliciels	Adultes
unfiltered.joindns4.eu				
protective.joindns4.eu			✅	
noads.joindns4.eu	✅	✅	✅	
child.joindns4.eu			✅	✅
child-noads.joindns4.eu	✅	✅	✅	✅

Résolveur DNS non filtrant :

Adresse IPV4 du serveur primaire : 86.54.11.100

Adresse IPV4 du serveur secondaire : 86.54.11.200

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:100

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:200

DNS over HTTPS: https://unfiltered.joindns4.eu/dns-query

DNS over TLS: unfiltered.joindns4.eu

Résolveur DNS protecteur :

Ce résolveur DNS est durci, orienté sécurité.

Adresse IPV4 du serveur primaire : 86.54.11.1

Adresse IPV4 du serveur secondaire : 86.54.11.201

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:1

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:201

DNS over HTTPS: https://protective.joindns4.eu/dns-query

DNS over TLS: protective.joindns4.eu

Résolveur DNS protecteur et filtrant la publicité :

Adresse IPV4 du serveur primaire : 86.54.11.13

Adresse IPV4 du serveur secondaire : 86.54.11.213

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:13

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:213

DNS over HTTPS: https://noads.joindns4.eu/dns-query

DNS over TLS: noads.joindns4.eu

Résolveur DNS protecteur avec filtrage du contenu pour adultes :

Adresse IPV4 du serveur primaire : 86.54.11.12

Adresse IPV4 du serveur secondaire : 86.54.11.212

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:12

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:212

DNS over HTTPS: https://child.joindns4.eu/dns-query

DNS over TLS: child.joindns4.eu

Résolveur DNS protecteur avec filtrage du contenu pour adultes et de la publicité :

Adresse IPV4 du serveur primaire : 86.54.11.11

Adresse IPV4 du serveur secondaire : 86.54.11.211

Adresse IPV6 du serveur primaire : 2a13:1001::86:54:11:11

Adresse IPV6 du serveur secondaire : 2a13:1001::86:54:11:211

DNS over HTTPS: https:/child-noads.joindns4.eu/dns-query/

DNS over TLS: child-noads.joindns4.eu

* DNS0.EU, sur fonds privés. Ce résolveur DNS existe en trois versions.

Résolveur DNS non filtrant :

Voir https://www.dns0.eu

Adresse IPV4 du serveur primaire : 193.110.81.0

Adresse IPV4 du serveur secondaire : 185.253.5.0

Adresse IPV6 du serveur primaire : 2a0f:fc80::

Adresse IPV6 du serveur secondaire : 2a0f:fc81::

DNS over HTTPS: https://dns0.eu

DNS over TLS: dns0.eu

Résolveur DNS protecteur Zero :

Ce DNS est durci, orienté vers la sécurité, utilisant le filtrage humain et heuristique, voir les détails ici : https://www.dns0.eu/zero

Adresse IPV4 du serveur primaire : 193.110.81.9

Adresse IPV4 du serveur secondaire : 185.253.5.9

Adresse IPV6 du serveur primaire : 2a0f:fc80::9

Adresse IPV6 du serveur secondaire : 2a0f:fc81::9

DNS over HTTPS: https://zero.dns0.eu

DNS over TLS: zero.dns0.eu

Résolveur DNS filtrant le contenu pour adultes :

Ce résolveur DNS protège les enfants du contenu pour adultes, voir : https://www.dns0.eu/kids

Adresse IPV4 du serveur primaire : 193.110.81.1

Adresse IPV4 du serveur secondaire : 185.253.5.1

Adresse IPV6 du serveur primaire : 2a0f:fc80::1

Adresse IPV6 du serveur secondaire : 2a0f:fc81::1

DNS over HTTPS: https://kids.dns0.eu

DNS over TLS: kids.dns0.eu

3. Smartphones Android

3.1) Introduction à Android

Les appareils Android incluent un système d'exploitation avec plusieurs couches :

– un noyau Linux, personnalisé pour Android,

– une couche d'Open Source Android, AOSP, voir https://source.android.com/.

– dans la plupart des cas, une couche Google (avec Google Play, Google Play Service, Google Assistant ou Gemini, Android Auto, Google Chrome, Gmail, Google Maps, etc.),

– des pilotes et des réglages spécifiques au fabricant,

– dans certains cas, une couche de fabricant supplémentaire (exemple, Samsung) sur celle de Google ou remplaçant partiellement certaines applications Google,

– des applications du magasin Play Store de Google, ou de magasins alternatifs tels que F-Droid, ou installées à partir d'un fichier APK.

La sécurité d'Android est basée sur l'utilisation de Selinux (Security Enhanced Linux), qui fournit une isolation complète des applications dans les bacs à sable les plus forts. Certains mécanismes permettent de partager des données et des fichiers entre les applications en bacs à sables.

Les failles de sécurité viennent essentiellement de l'installation et de l'usage de maliciels.

Les logiciels malveillants sont contrôlés par Google dans son Play Store et par Google Security sur l'appareil. Le contrôle des logiciels malveillants pas Google n'est pas parfait, régulièrement des maliciels sont rendus disponibles dans Play Store. Le risque de télécharger et d'installer des logiciels malveillants est plus élevé lors de l'utilisation du magasin alternatif ou lors de l'installation à partir d'un fichier APK.

Il est recommandé d'arrêter et de redémarrer périodiquement les périphériques Android, pour supprimer les maliciels persistant en mémoire.

Comme pour tout système d'exploitation, il est recommandé de le mettre à jour le plus souvent possible (système et applications), pour les corrections de bogues et les correctifs de sécurité.

Le principal problème avec Android est le pistage : vous êtes traqué par Google et par toutes les applications « gratuites » (non payantes) installées sur l'appareil (et même par certaines applications payantes).

Les publicités sont un autre problème, affichées si agressivement à l'intérieur des applications qu'elles empêchent leur utilisation normale.

3.2) Utilisation de distributions alternatives

Certains utilisateurs peuvent installer des distributions alternatives à la place celles livrées avec leur smartphone Android, afin d'être complètement libérés de Google.

Cela nécessite une compétence de l'utilisateur, et ce n'est pas disponible pour tous les appareils.

L'installation d'une distribution alternative est risquée : une mauvaise manipulation pourrait rendre inutilisable le smartphone. Ce risque est annulé lorsque l'utilisateur achète un smartphone avec l'une de ces distributions préinstallées.

Enfin, sans compte Google, la sauvegarde Google Cloud n'est pas possible ; l'utilisateur doit configurer une autre solution de sauvegarde et restauration. Certains utilisateurs choisissent une sauvegarde RSYNC en mode racine, mais certaines applications telles que Netflix ne fonctionneront pas une fois le smartphone en mode racine.

→ **Pour toutes ces raisons, c'est une utilisation de niche.**

Voici quelques distributions alternatives :

Distributions Linux :

* Ubuntu Touch

https://www.ubuntu-touch.io/

« Une expérience complète d'un système d'exploitation mobile, qui est le vôtre ».

Ubuntu Touch est un système d'exploitation Linux, dédié aux smartphones, remplaçant totalement Android.

Il est compatible avec la liste des appareils suivants : https://devices.ubuntu-touch.io/. il est possible de l'obtenir préinstallé sur certains appareils (Volla, Pine64 and FXP).

Il utilise ses propres applications. Certaines applications Android peuvent être exécutées sur Ubuntu Touch en utilisant des applications qui permettent d'exécuter des applications Android en conteneur sur les systèmes Linux sans avoir besoin d'un système d'exploitation Android complet.

Il y aurait environ 200 000 à 300 000 utilisateurs d'Ubuntu Touch.

* Sailfish OS

https://sailfishos.org/

« Sailfish OS est une alternative européenne basée sur Linux aux systèmes d'exploitation mobiles dominants, et le seul système d'exploitation mobile offrant un modèle de licence exclusif pour les implémentations locales ».

Il est compatible avec les appareils suivants : https://docs.sailfishos.org/Support/Supported_Devices/.

Il utilise son propre magasin d'applications, Jolla Store.

Il y aurait environ 80 000 à 120 000 utilisateurs, essentiellement des développeurs.

* PostmarketOS

https://postmarketos.org/

« PostmarketOS développe des logiciels gratuits et open-source pour prolonger la vie de l'électronique grand public. En permettant aux gens d'avoir le plein contrôle de leurs appareils, nous faisons la promotion d'une société plus saine et plus durable »

Il est compatible avec les appareils suivants : https://wiki.postmarketos.org/wiki/Devices.

Il y aurait environ 1 000 utilisateurs.

* Mobian

https://mobian-project.org/

« Un dérivé de Debian pour les appareils mobiles ».

Il est compatible avec les appareils suivants : https://wiki.debian.org/Mobian/Devices, surtout des smartphones Pine64 et OnePlus.

Il y aurait environ 2 000 à 5 000 utilisateurs.

* Plasma Mobile

https://plasma-mobile.org

« Un écosystème pour les téléphones qui respecte la confidentialité, les logiciels gratuits et sécurisés ».

Plasma Mobile peut être installé sur des distributions Linux telles que PostmarketOS ou Mobian.

Il y aurait peu d'utilisateurs de Plasma Mobile, environ 1 000, car c'est un projet à ses débuts.

* PureOS

https://www.pureos.net/

« Un système d'exploitation entièrement convergent, convivial, sécurisé et respectueux de la liberté pour votre utilisation quotidienne. Avec PureOS, vous êtes le seul à contrôler votre vie numérique ».

PureOS est officiellement compatible uniquement avec le smartphone Librem 5 fabriqué par Purism.

Il y a quelques projets communautaires pour le rendre compatible des PinePhone et de Mobian sur quelques Nokia.

Purism a livré environ 20 000 Librem 5 avec PureOS.

→ À l'échelle mondiale, les utilisateurs alternatifs de distributions Linux sur les smartphones sont de 300 000 à 450 000.

Distributions Android alternatives :

* /e/OS

https://e.foundation/e-os/

« /e/OS est un écosystème mobile complet, entièrement dé-Googlé ».

/e/OS est un système d'exploitation mobile open source associé à des applications soigneusement sélectionnées. Ils forment un système interne compatible avec la confidentialité pour votre smartphone. Et ce ne sont pas seulement les affirmations : l'open source signifie une confidentialité vérifiable.

/e/OS a reçu une reconnaissance académique de chercheurs de l'Université d'Édimbourg et du Trinity College de Dublin.

/e/OS aurait pu se concentrer sur un système d'exploitation, mais les applications et les services en ligne sont également des éléments cruciaux de l'expérience quotidienne.

Ces services en ligne, y compris le moteur de recherche, la plate-forme de messagerie, le stockage cloud et d'autres outils en ligne, créent un environnement unique et amélioré de confidentialité.

Il est compatible avec les appareils suivants : https://doc.e.foundation/devices. Murena vend quelques smartphones avec /e/OS préinstallé.

Les applications sont installées depuis l'App Lounge : l'App Lounge est la deuxième itération du magasin d'applications intégré à /e/OS. Il permet à chacun d'accéder à des millions d'applications directement à partir de l'écran d'accueil de son téléphone.

Il combine des applications Android courantes, des applications open source et même des applications Web progressives dans un seul référentiel. C'est le seul magasin d'applications qui le fait aujourd'hui. Vous n'avez pas besoin de vous connecter à un compte pour télécharger des applications.

Il y aurait environ 200 000 utilisateurs d'/e/OS.

* LineageOS

https://lineageos.org/

« Un système d'exploitation gratuit et open source pour divers appareils, basé sur la plate-forme mobile Android ».

Il est le successeur de CyanogenMod.

Il est compatible avec les appareils suivants : https://wiki.lineageos.org/devices/.

Il comprend un ensemble d'applications open source. Les applications Google ne sont pas intégrées à LineageOS mais peuvent être téléchargées séparément.

Il y aurait environ 1 800 000 utilisateurs de LineageOS.

* GrapheneOS

https://grapheneos.org/

« Le système d'exploitation mobile privé et sécurisé compatible des applications Android. Développé comme un projet open source à but non lucratif ».

Il est compatible avec les appareils suivants : https://grapheneos.org/faq#supported-devices, exclusivement des Google Pixel, en raison des exigences matérielles de sécurité de GrapheneOS.

GrapheneOS est une version à sécurité durcie d'Android, libérée de Google, avec son propre magasin d'applications. Google Play Store peut être installé éventuellement dans un bac à sable.

GrapheneOS fournit probablement la meilleure compatibilité avec les applications Google Play Store.

Il y aurait environ 60 000 utilisateurs de GrapheneOS.

* CalyxOS et Pixel Experience ne sont plus maintenus.

→ À l'échelle mondiale, en tenant compte des utilisateurs de CalyxOs et de Pixel Experience, il y aurait environ 2 600 000 utilisateurs de distributions Android alternatives.

* Huawei

https://consumer.huawei.com

Le cas de Huawei est spécifique: Huawei vend des smartphones Android, sans aucun accès aux logiciels de Google.

Les smartphones Huawei n'ont pas accès à Google Play Store, ni à une application Google, mais à leur propre magasin d'applications.

D'une certaine manière, les utilisateurs de smartphones Huawei sont exempts du pistage par Google, mais il est remplacé par celui de Huawei !

* XDA Developers

https://xdaforums.com/

Sur les forums XDA Developers, vous pouvez trouver des ROM personnalisées pour certains appareils Android.

3.3) Utilisation des smartphones Android du commerce

La plupart des utilisateurs d'Android utilisent des appareils Android avec le système d'exploitation fourni par le fabricant (Android 14, 15, 16…) et son ajustement.

Cependant, l'utilisateur peut configurer son appareil Android commercial afin d'améliorer sa sécurité, sa confidentialité et même avoir un certain anonymat.

* Protection contre les logiciels malveillants, les pisteurs et la publicité.

Cette partie s'applique également aux smartphones Android avec une distribution Android alternative.

Nous parlons ici de logiciels malveillants sur Internet (sites malicieux), pas des logiciels malveillants que vous pouvez installer depuis les magasins. Les deux meilleurs résolveurs DNS filtrant concernant la protection des logiciels malveillants sont :

« zero.dns0.eu », il protège contre l'hameçonnage (il ne répond pas aux demandes de sites Web de moins d'un mois, ce qui est le cas pour la plupart des sites Web d'hameçonnage avec une petite durée de vie) et protège contre les attaques homographes en filtrant des sites Web frauduleux avec des caractères cyrilliques dans l'URL,

« protective.joindns4.eu » et d'autres résolveurs DNS de filtrage de la famille joindns4.eu, il comprend une base de données de plus de vingt millions de sites Web malveillants. Cette base de données est continuellement mise à jour, l'IA est utilisée pour analyser le comportement des sites Web.

1re méthode : utilisation d'un résolveur DNS de filtrant et du navigateur DuckDuckgo.

Choisissez le résolveur DNS filtrant que vous voulez, voir Résolveurs DNS filtrants, et entrez son nom DoT dans le paramètre DNS privé qui se trouve trouvé dans les paramètres / Internet et réseau.

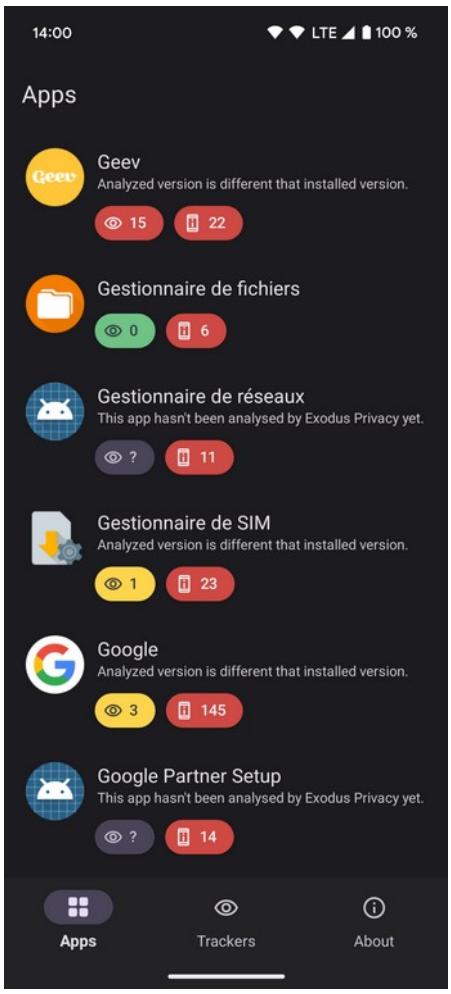
Exemples:

> « zero.dns0.eu » pour le résolveur DNS à sécurité renforcée de dns0.eu,
>
> « 1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com » pour un résolveur DNS Rethink avec les filtres Security Full et Privacy Agressive.

Le filtrage sera fait à l'échelle du système, pour toutes les applications installées et le système d'exploitation.

Installez le navigateur DuckDuckgo depuis Google Play Store. DuckDuckGo Browser est un mauvais navigateur (pas d'extension, basé sur WebView et qui révèle l'adresse IP interne via une fuite WebRTC), mais nous l'utiliserons juste pour ajouter une couche de filtrage supplémentaire des pisteurs des applications installées sur l'appareil, en utilisant sa protection contre le pistage par les applications. Pour plus d'information, voir https://duckduckgo.com/duckduckgo-help-pages/p-app-tracking-protection/what-is-app-tracking-protection.

Le pistage par les applications est différent du pistage habituel qui se produit lors de l'utilisation d'un navigateur ; les pisteurs sont spécifiques. Vous pouvez installer sur votre smartphone Android l'application Exodus Privacy ; elle analysera les applications installées sur votre smartphone et téléchargera les rapports donnant, pour chaque application, les pisteurs utilisés par l'application et la liste des autorisations requises par l'application.



En couplant à la fois le filtrage par un résolveur DNS et la protection de DuckDuckGo contre le pistage par les applications, vous pouvez protéger votre appareil Android contre les logiciels malveillants, les publicités et le pistage.

2e méthode : utilisation de Personal DNS Filter

Personal DNS Filter est une application qui peut être téléchargée depuis Google Play Store et peut être utilisée sur un périphérique Android standard, sans mode racine.

Elle combine l'utilisation du résolveur DNS de votre choix, à l'aide d'adresses IPv4 ou IPv6 (cela exclut le résolveur DNS Rethink), avec un ensemble de filtres, acceptant deux syntaxes : fichier « hosts » ou filtres DNS. Vous pouvez choisir un ou plusieurs des filtres préexistants ou ajouter un filtre de votre choix.

Plus d'informations, voir https://www.zenz-solutions.de/personaldnsfilter-wp/.

J'utilise le résolveur DNS « protective.joindns4.eu », en mode DoT, avec les adresses IP suivantes :

86.54.11.1

86.54.11.201

2a13:1001::86:54:11:1

2a13:1001::86:54:11:201

Voici les listes de filtres que j'utilise (maliciels, publicités, pisteurs et réseaux sociaux) :

Publicités :
https://v.firebog.net/hosts/AdguardDNS.txt;
https://v.firebog.net/hosts/Easylist.txt;
https://raw.githubusercontent.com/lassekongo83/Frellwits-filter-lists/master/Frellwits-Swedish-Hosts-File.txt.
Maliciels :
https://raw.githubusercontent.com/greatis/Anti-WebMiner/master/hosts;
https://raw.githubusercontent.com/hoshsadiq/adblock-nocoin-list/master/hosts.txt;
https://malware-filter.gitlab.io/malware-filter/urlhaus-filter-hosts.txt;
https://urlhaus.abuse.ch/downloads/hostfile/;
https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.Spam/hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/rpz/tif.mini.txt;
https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/lists/latestdomains.piHole.txt.
Pisteurs :
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.amazon.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.apple.txt;
https://v.firebog.net/hosts/Easyprivacy.txt;
https://hostfiles.frogeye.fr/multiparty-trackers-hosts.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.huawei.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.winoffice.txt;
https://raw.githubusercontent.com/mullvad/dns-blocklists/refs/heads/main/files/tracker;
https://raw.githubusercontent.com/notracking/hosts-blocklists/master/hostnames.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.oppo-realme.txt;
https://gitlab.com/quidsup/notrack-blocklists/-/raw/master/trackers.hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.tiktok.extended.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.vivo.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.xiaomi.txt.
Filtres multiples :
https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts;
https://big.oisd.nl/domainswild2;
https://raw.githubusercontent.com/hagezi/dns-blocklists/main/wildcard/pro-onlydomains.txt.
(Publicités, Affiliation, Pistage, Métriques, Télémétrie, Hameçonnage, Maliciels, Arnaque, Faux, Voleurs de cryptomonnaies et autres mer..s).
Réseaux Sociaux :
https://raw.githubusercontent.com/mullvad/dns-blocklists/refs/heads/main/files/social.
(NB: L'utilisation de cette liste empêchera l'utilisation de Facebook, Instagram, etc., mais permettra l'utilisation de WhatsAppp).

Avec Personal DNS Filter, pas besoin du navigateur DuckDuckgo ; de plus, il comprend la possibilité de mettre en liste blanche certains sites Web (inclus dans les filtres) auxquels vous voudriez vous connecter et d'ajouter manuellement certains sites Web que vous voudriez filtrer,

ainsi que de mettre des applications en liste blanche (pour lesquelles les filtres ne s'appliqueront pas).

* Libération partielle de Google

Ceci ne s'applique pas aux smartphones avec une distribution alternative d'Android.

J'ai désinstallé ou désactivé (lorsque la désinstallation est impossible) toutes les applications Google que je n'utilise pas :

- Android Auto,
- Gemini,
- Gmail (remplacé par Thunderbird),
- Google,
- Google Assistant,
- Google Chrome (remplacé par Firefox),
- Google Docs (remplacé par Collabora Office),
- Google Fit,
- Google Maps (peut être utilisé de manière plus confidentielle dans un navigateur),
- Google Meet (peut être utilisé de manière plus confidentielle dans un navigateur),
- Google News (peut être utilisé de manière plus confidentielle dans un navigateur),
- Google TV,
- Google Voice Recognition and Synthesis,
- Notes Keep,
- YouTube (peut être utilisé de manière plus confidentielle dans un navigateur),
- YouTube Music (remplacé par VLC).

Un zoom sur Firefox :

Firefox pour Android est mon navigateur par défaut, il remplace Google Chrome.

J'ai installé les extensions suivantes :

- « Canvas Blocker », protection contre le pistage par empreintes du navigateur,
- « CSS Exfil Protection », empêche la fuite de données via les feuilles de styles,
- « Dark Reader », permet d'afficher les pages avec des caractères blancs sur fond noir (c'est une question de goût)
- « DuckDuckGo Search and Tracker Protection », protection de la confidentialité, elle installe la recherche DuckDuckGo comme page d'accueil, le moteur de recherche DuckDuckGo par défaut et l'extension « DuckDuckGo Privacy Essentials »,
- « Privacy Badger », protection contre le pistage,
- « Font Fingerprint Defender », protection contre le pistage par empreintes du navigateur,
- « uBlock Origin », l'un des meilleurs filtres de la publicité, contre le pistage et contre les maliciels.

Notez que toutes les extensions de Firefox ne sont pas disponibles pour la version Android de Firefox. Cependant, l'utilisation du mode de débogage (tapez cinq fois sur les paramètres / à propos de Firefox) permet d'installer n'importe quelle extension à partir d'un fichier.

Officiellement, « about :config » n'est pas disponible dans la version Android de Firefox ; mais c'est là, juste caché ! Dans la barre d'adresse, tapez:

« chrome: //geckoview/content/config.xhtml »

et le contenu habituel de « about :config » est là! Mettez-le dans vos signets.

Apportez les modifications suivantes dans « about :config » :

- « Browser.Cache.Disk.enable » à mettre sur « False », pour désactiver la mise en cache disque,
- « webgl.enable-debug-rendu-info » à mettre sur « False », pour éviter que le pilote graphique soit exposé,
- « media.peerconnection.enabled » à mettre sur « False », pour désactiver la fuite par WebRTC,
- « javascript.options.baselinejit » à mettre sur « False », pour désactiver la compilation JavaScript en temps réel, cela réduit la surface d'attaque de JavaScript,
- « Network.idn_show_punycode » à mettre sur « True », pour être protégé contre les attaques homographes IDN, (les URL avec des caractères non latins seront affichées sous forme de punycode).

Vous voudrez peut-être installer d'autres navigateurs que Firefox :
- IronFox dérive de Firefox, basé sur l'ancien Mull, c'est une version à sécurité durcie de Firefox, à travers des préférences de configuration; Fission y est activé, cela signifie que tous les onglets sont isolés et fonctionnent dans des processus différents (bien que cela soit activé dans les versions de bureau Firefox, ce n'est pas encore disponible sur la version Android de Firefox, mais c'est déjà activé sur IronFox). Voir :
https://gitlab.com/ironfox-oss/IronFox
- Cromite dérive de Chromium, basée sur l'ancien Bromite, c'est une version à confidentialité renforcée de Chromium, avec filtre intégré, offrant toujours la forte sécurité de Chromium. Voir :
https://github.com/uazo/cromite

Ces navigateurs ne sont pas disponibles sur Google Play Store, pour les installer vous devez d'abord télécharger et installer F-Droid, à partir de https://f-droid.org/fr/. Ensuite,
- Pour installer IronFox, ajoutez le référentiel suivant à F-Droid :
https://gitlab.com/ironfox-oss/fdroid/-/raw/main/fdroid/repo
Puis, recherchez IronFox dans F-Droid et installez-le.
- Pour installer Cromite, ajoutez le référentiel suivant à F-Droid :
https://www.cromite.org/fdroid/repo/fingerprint=49f37e74dee483dca2b991334fb5a0200787430d0b5f9a783dd5f13695e9517b
Ensuite, recherchez Cromite dans F-Droid et installez-le.
Notez que Ironfox et Cromite sont maintenus par de très petites équipes et pourraient disparaître sans préavis, comme l'ont fait leurs prédécesseurs ; vérifiez qu'ils sont mis à jour régulièrement.

* Autres précautions

- Activez la localisation, NFC, Bluetooth, Wi-Fi uniquement lorsque vous en avez besoin,
- ne vous connectez jamais à un spot Wi-Fi public,
- pour chaque application installée, définissez ses notifications, ses autorisations, l'utilisation de la batterie,
- utilisez l'application « System Manager » pour définir le « mode d'économie d'énergie », il empêchera la plupart des applications de fonctionner en arrière-plan,

- si le réglage est disponible (Android 14 et plus tard), désactivez la 2G,
- lorsque cela est possible, préférez utiliser le navigateur qu'une application dédiée (exemple : connectez-vous à Facebook avec Firefox, n'utilisez pas l'application Facebook),
- gardez votre système, Google Play Service et vos applications à jour.

* VPN

Il est possible d'utiliser un VPN dans les appareils Android. Une fois installé, la connexion VPN peut être définie comme permanente dans Paramètres / Internet et réseau.
Notez que l'utilisation d'un VPN empêche l'utilisation du navigateur DuckDuckgo et de Personal DNS Filter ; bien qu'ils ne soient pas des VPN, ils utilisent le réglage VPN d'Android.

* Anonymat

Le navigateur Tor Browser est disponible dans le Play Store ; utilisez les mêmes paramètres que pour Firefox et utilisez l'extension NoScript Security Suite.
Cependant, pas plus que Firefox pour Android, Tor Browser pour Android n'utilise pas Fission et il n'y a pas d'isolation des processus. Pour une alternative plus sûre, utilisez Orbot et lancez avec Orbot en mode VPN le navigateur de votre choix, IronFox ou Cromite.
Plusieurs applications de messagerie offrent l'anonymat et le chiffrement complet de bout en bout. Évitez WhatsApp (source non divulguée), Telegram (chiffré jusqu'aux serveurs, personne ne sait ce qui se passe sur les serveurs), préférez Signal ou, en France, Olvid.

4. iPhones

4.1) Introduction aux iPhones

Les iPhones sont exclusivement fabriqués par Apple; leur système d'exploitation, iOS, est du genre « source non divulguée », et toutes les applications sont préinstallées par Apple ou proviennent d'Apple App Store.

L'UE a demandé à Apple d'ouvrir ses smartphones aux magasins alternatifs, menaçant Apple de centaines de millions de dollars d'amendes ; Apple a finalement accepté et a supprimé toute difficulté d'utiliser un autre magasin depuis iOS 18.6. Bien entendu, la sécurité des applications installées depuis un autre magasin n'est pas gérée / garantie par Apple.

La sécurité est ainsi sous le contrôle strict d'Apple. Les failles de sécurité sont peu connues. Apple n'a pas de programme de récompenses pour les chercheurs qui trouvent des failles de sécurité, tandis qu'une entreprise israélienne (Pégasus) paie pour cela et crée des programmes permettant d'espionner iOS, programmes vendus à un coût très élevé aux gouvernements. La sécurité globale semble très bonne.

Les applications sont fortement isolées, au point qu'elles ne peuvent rien partager (si vous souhaitez utiliser Apple Music et VLC pour écouter de la musique, vous devez copier votre musique dans les répertoires des deux applications).

iOS a une certaine protection contre le suivi, la protection contre le pistage croisé par les applications n'est qu'un paramètre à sélectionner, et Safari, le navigateur Web, comprend une certaine protection contre le pistage.

Les publicités semblent s'afficher moins agressivement dans les applications que dans leurs versions Android.

4.2) Protection contre les maliciels, la publicité et le pistage dans iOS

Il n'y a qu'une seule méthode qui fonctionne à l'échelle du système : l'utilisation d'un résolveur DNS filtrant (voir Résolveurs DNS filtrants).

Il n'y a pas d'équivalent à Personal DNS Filter pour iOS, et le navigateur DuckDuckgo pour iOS ne peut pas fonctionner comme une protection contre le pistage par les applications.

Les deux meilleurs résolveurs DNS filtrant concernant la protection des logiciels malveillants sont :
« zero.dns0.eu », il protège contre l'hameçonnage (il ne répond pas aux demandes de sites Web de moins d'un mois, ce qui est le cas pour la plupart des sites Web d'hameçonnage avec une petite durée de vie) et protège contre les attaques homographes en filtrant des sites Web frauduleux avec des caractères cyrilliques dans l'URL,
« protective.joindns4.eu » et d'autres résolveurs DNS de filtrage de la famille joindns4.eu, il comprend une base de données de plus de vingt millions de sites Web malveillants. Cette base de données est continuellement mise à jour, l'IA est utilisée pour analyser le comportement des sites Web.

Si vous souhaitez utiliser un résolveur DNS filtrant les logiciels malveillants et les publicités, vous devez utiliser :

- un des résolveurs DNS de DNS4EU, « noads.joindns4.eu », ou « child-noads.joindns4.eu »,
- un des résolveurs DNS de Mullvad, « base.dns.mullvad.net », « extended.dns.mullvad.net », « family.dns.mullvad.net », « all.dns.mullvad.net »,
- une version personnalisée du résolveur DNS Rethink DNS, par exemple avec les filtres Security Full et Privacy Aggressive :

  « 1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com ».

Afin de définir un résolveur DNS dans les appareils iOS, vous avez besoin d'un profil DNS ; un tel profil DNS peut être téléchargé pour DNS0.EU, DNS4EU et Mullvad DNS à partir de leurs sites Web (voir les liens dans Résolveurs DNS filtrants).

Rethink DNS n'offre pas une telle possibilité. Vous pouvez générer un profil DNS à partir du créateur de profil DNS sécurisé, https://dns.notjakob.com/.

Une fois que vous avez le profil dont vous avez besoin, vous l'importez dans votre appareil iOS (envoyez-le par courriel), installez-le dans les paramètres généraux / VPN et gestion des appareils et validez-le ; il sera actif dans la section « Restrictions et Proxy ».

Navigateur : il n'est pas nécessaire d'utiliser un autre navigateur que Safari ; en raison des restrictions d'Apple, Firefox pour iOS est très médiocre, basé sur WebKit (le même moteur de rendu que Safari), et n'a pas d'extension. Le seul intérêt est pour Firefox Focus, qui peut être utilisé comme navigateur avec des fonctionnalités « oubli rapide » et « anti-pistage » ; de plus, il peut agir comme un bloqueur de contenu pour Safari.

Vous pouvez installer l'extension « UBlock Origin Lite » pour Safari ; une fois installée, donnez-lui les autorisations nécessaires, définissez le niveau de protection et sélectionnez les listes de filtres.

Vous pouvez compléter les fonctionnalités anti-pistage à l'aide de Firefox Focus et utiliser une version gratuite d'Adguard ou d'AdBlock Plus comme bloqueurs de contenu supplémentaires.

4.3) Autres précautions pour iOS

- Il est recommandé d'arrêter et de redémarrer périodiquement les appareils iOS, pour supprimer les maliciels persistant en mémoire,
- comme pour tout système d'exploitation, il est recommandé de le mettre à jour le plus souvent possible (système et applications), pour les corrections de bogues et les correctifs de sécurité,
- activez la localisation, Bluetooth et Wi-Fi uniquement lorsque vous en avez besoin,
- ne vous connectez jamais à un spot Wi-Fi public,
- pour chaque application installée, définissez ses notifications et autorisations,
- désactivez Siri, globalement et dans chaque réglage d'application,
- utilisez le mode économie d'énergie en permanence, il empêche les applications de fonctionner en arrière-plan,

- mettez en place la protection contre le pistage croisé par les applications,
- Lorsque cela est possible, préférez utiliser le navigateur qu'une application dédiée (exemple : connectez-vous à Facebook avec Safari, n'utilisez pas l'application Facebook),
- gardez votre système (version d'iOS) et les applications à jour.

4.4) VPN sur iOS

L'utilisation d'un VPN est possible sur iOS. Voir Paramètres généraux / VPN et gestion des appareils.

4.5) Anonymat sur iOS

Le navigateur Tor Browser n'est pas disponible dans le Play Store, mais vous pouvez utiliser Onion Browser ou Orbot et Safari sur iOS (avec une protection de la confidentialité réduite en raison des restrictions d'Apple, qui limitent la mémoire accessible à 50 MB, ce qui empêche de trouver de longs chemins dans le réseau Tor).
Plusieurs applications de messagerie offrent l'anonymat et le chiffrement complet de bout en bout. Évitez WhatsApp (source non divulguée), Telegram (chiffré jusqu'aux serveurs, personne ne sait ce qui se passe sur les serveurs), préférez Signal ou, en France, Olvid.