Forum: Vos freewares préférés

Topic: uBlock Origin - mode de blocage: Facile et +

Subject: uBlock Origin - mode de blocage: Facile et +

Publié par: Anonyme
Contribution le : 12/10/2017 02:34:31

Mode de blocage: **facile**

Par Raymond Hill (Aout 2015)
Page d'origine en anglais: (traduit avec l'aide de Deepl)

Il s'agit du mode par défaut de uBlock Origin.
Semblable à peu près à l'utilisation d'Adblock Plus avec de nombreuses listes de filtres.
Les publicités sont bloquées par EasyList et la liste de serveurs publicitaires de Peter Lowe, et l'utilisation d'EasyPrivacy réduit l'exposition à la vie privée. Certaines listes de filtres anti logiciels malveillants sont sélectionnées par défaut. De plus, les listes de filtres propres à uBlock Origin sont sélectionnées en complément des listes de filtres tiers sélectionnées.
Ce mode convient à ceux qui souhaitent réduire leur exposition à la protection de la vie privée, mais qui préfèrent quand même une installation et une utilisation facile.

Caractéristiques:
Faible probabilité de rupture des pages Web.
Les pages Web devraient se charger un peu plus rapidement que le mode très facile.

Comment activer ce mode:
Volet Réglages: Je suis un utilisateur avancé: **non coché**
Filtres tiers: Toutes les listes de filtres personnalisés d'uBlock origin: **coché**
EasyList: **coché**
Peter Lowe's Ad server list: **coché**
EasyPrivacy: **vérifié**
Liste des domaines malveillants: **cochée**
Domaines de programmes malveillants: **vérifiés**
Toutes les autres listes de filtres: **décochées**

Conseils:
Vous pouvez augmenter considérablement la puissance de blocage en mode simple en activant simplement plus de listes de filtres. Si vous ajoutez d'autres listes de filtres, gardez à l'esprit que:
- plus on utilise de listes de filtres, plus la probabilité de bris de page Web est élevée.
- toutes les listes de filtres ne sont pas de bonne qualité: certains peuvent casser trop de page web.
- certaines listes peuvent entraîner des requêtes réseau pour se débloquer de manière inattendue.

Une autre façon encore plus efficace d'augmenter la puissance de blocage en mode facile est d'activer "Activer les fonctionnalités avancées" à partir du panneau "Paramètres" du tableau de bord, et de bloquer des tierces parties spécifiques à l'aide du filtrage dynamique -- c'est-à-dire essentiellement en utilisant le filtrage dynamique en mode par défaut. Par exemple, on pourrait choisir de bloquer globalement facebook. com et facebook. net afin d'empêcher Facebook de pouvoir vous suivre partout où vous allez, sauf sur Facebook. Le blocage Glboally bloquant les

noms d'hôtes omniprésents sauf sur leurs sites Web respectifs est un moyen très facile de réduire de manière significative l'exposition à la vie privée.

Filtrage dynamique: pour réduire facilement l'exposition à la vie privée:

Source

Les sites omniprésents sont ces tiers dont les ressources sont intégrées dans d'innombrables pages Web. Votre exposition à la protection de la vie privée est fortement augmentée par ces sites omniprésents.
Un exemple évident en est Facebook: les widgets Facebook (boutons like) pour aimer quelque chose sont intégrés dans d'innombrables pages web, et en tant que tels, ces widgets servent d'excellents dispositifs de suivi pour Facebook pour construire un profil de votre historique de navigation. C'est également vrai pour d'autres entités telles que Twitter, Google, Disqus, etc.

Le filtrage dynamique d'uBlock Origin peut vous aider à empêcher les serveurs omniprésents de créer un profil de vos habitudes de navigation.
Nous utiliserons Facebook comme exemple. Facebook aura toujours la possibilité de suivre vos habitudes de navigation lorsque vous utilisez uBlock Origin avec ses paramètres par défaut[voir les données brutes du benchmark pour le mode Facile: notez dans la liste des tierces parties comment facebook. net est omniprésent].
Premièrement, nous bloquons globalement les noms d'hôtes liés à Facebook, de telle sorte que les requêtes réseau vers les serveurs Facebook sont bloquées par défaut, partout: **Voir image attachée df1.png** (En bas de cet article)

Toutes les règles de blocages globales suggérées pour Facebook:

* facebook.net * block
* facebook.com * block
* fbcdn.net * block

Ces règles feront en sorte que Facebook sera bloqué partout par défaut, même lorsqu'il visitera son propre site. C'est ce qui empêche Facebook de recueillir des données sur vos habitudes de navigation.
Bloquer Facebook lorsque vous visitez Facebook n'est pas l'idéal, et il n'y a pas d'avantage réel à le faire. Nous allons donc créer une exception aux règles globales ci-dessus, mais juste pour quand nous visiterons le site de Facebook: **Voir image attachée df2.png** (En bas de cet article)

Tous ont suggéré des règles de noop global pour Facebook.

facebook.com facebook.com * noop
facebook.com facebook.net * noop
facebook.com fbcdn.net * noop

Le même type de règles de filtrage dynamique peut être utilisé pour n'importe quel site pour lequel vous souhaiteriez que les widgets Facebook fonctionnent.

exemple. com facebook. com * noop
example. com facebook. net * noop
example. com fbcdn. net * noop

Ceci n'est qu'un exemple, la même chose peut être appliquée à n'importe quel serveur omniprésent. Le volet de filtrage dynamique de l'interface popup d'uBlock Origin vous tiendra informé de tous les serveurs tiers auxquels une page Web se connecte (ou tente de se connecter) et à partir de là, vous pourrez simplement pointer et cliquer pour créer des règles globales/locales de blocage/noop afin de déjouer la capacité des tiers à enregistrer votre historique de navigation.

"block" sur les sites Web omniprésents réduira facilement votre exposition à la protection de la vie privée.

En utilisant l'exemple ci-dessus de blocage de Facebook partout avec le résultat de référence pour le mode Facile (mode par défaut d'uBlock Origin), le nombre de tiers aurait été ramené de 512 à 437, un moyen facile de réduire considérablement votre exposition à la vie privée en quelques clics.

Conclusion concernant les actions:

Une règle peut faire l'une des trois choses suivantes:

block (cliquer à gauche dans la cellule pour la rendre rouge): la requête net correspondante sera bloquée.
les règles de filtrage dynamique "block" remplacent tous les filtres d'exceptions statiques existants. Ainsi, vous pouvez les utiliser pour bloquer avec 100% de certitude (à moins que vous ne définissiez une autre règle de filtrage dynamique prioritaire).

allow (cliquer à droite dans la cellule pour la rendre verte): la requête net correspondante sera autorisée.
permettre aux règles de filtres dynamiques de prendre le pas sur tous les filtres à blocs statiques et dynamiques existants.
Ils sont donc très utiles pour créer des exceptions plus fines, et pour désassembler les sites web cassés par des filtres statiques quelque part.

noop (cliquer au milieu dans la cellule pour la rendre grise): empêcher que les requêtes réseau correspondantes ne soient soumises à un filtrage dynamique.
Il annule le filtrage dynamique, mais il n'annule pas le filtrage statique.

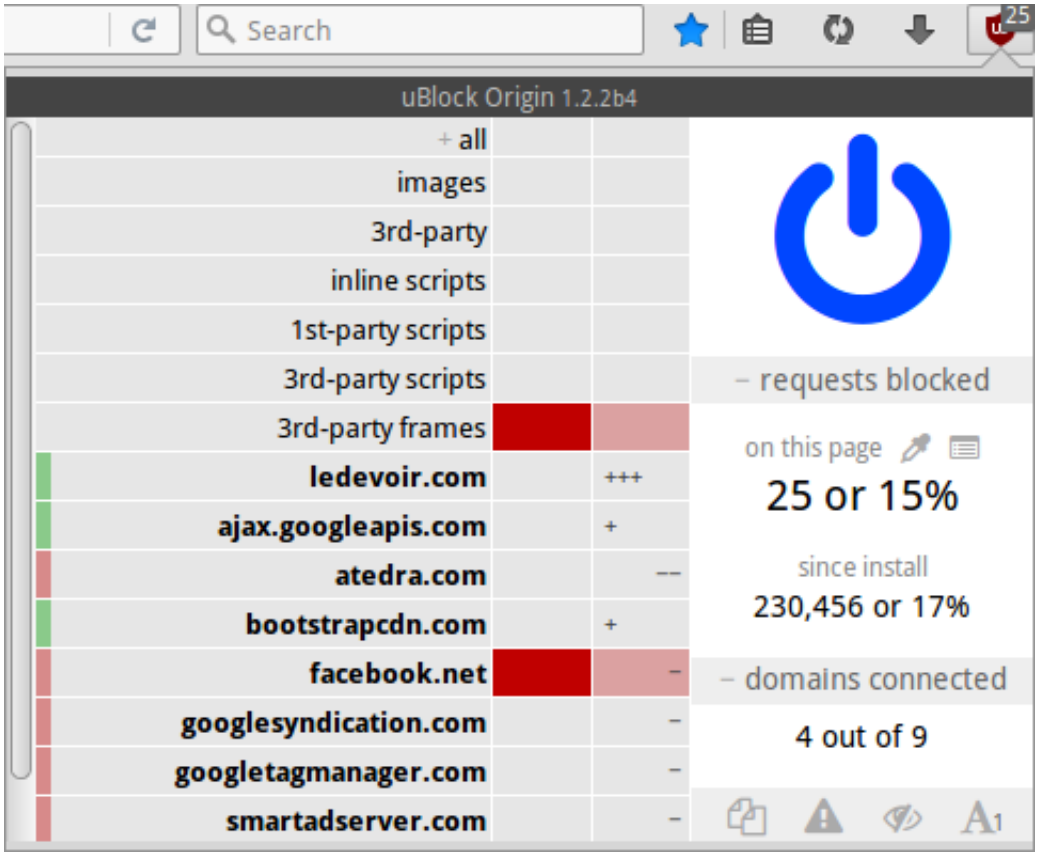
Dans la **colone de gauche**, ces actions seront affectées globalement pour **tous les sites consultés** .

Dans la **colone de droite**, ces actions seront affectées localement, c-a-d **uniquement pour le**

domaine actuellement consulté.

Fichier(s) attaché(s):

df1.png (42.41 KB)



df2.png (36.83 KB)