Windows 10 : plongée en eaux troubles

*Vous avez sans doute remarqué que lorsque les médias grand public évoquent les entreprises dominantes du numérique on entend « les GAFA » et on a tendance à oublier le **M** de Microsoft. Et pourtant… On sait depuis longtemps à quel point Microsoft piste ses utilisateurs, mais des mesures précises faisaient défaut. Le bref article que Framalang vous propose évoque les données d'une analyse approfondie de tout ce que Windows 10 envoie vers ses serveurs pratiquement à l'insu de ses utilisateurs…*

Article original : 534 Ways that Windows 10 Tracks You – From German Cyber Intelligence

Traduction Framalang : Khrys, goofy, draenog, Sphinx

Selon les services allemands de cybersécurité, Windows 10 vous surveille de 534 façons

par Derek Zimmer

L'Office fédéral de la sécurité des technologies de l'information (ou BSI) a publié un rapport [1] (PDF, 3,4 Mo) qui détaille les centaines de façons dont Windows 10 piste les utilisateurs, et montre qu'à moins d'avoir la version *Entreprise* de Windows, les multiples paramètres de confidentialité ne font pratiquement aucune différence.

Seules les versions *Entreprise* peuvent les arrêter

Les versions normales de Windows ont seulement trois niveaux différents de télémétrie. Le BSI a trouvé qu'entre la version *Basic* et la version *Full* on passe de 503 à 534 procédés de surveillance. La seule véritable réduction de télémétrie vient des versions *Entreprise* de Windows qui peuvent utiliser un réglage supplémentaire de « sécurité » pour leur télémétrie qui réduit le nombre de traqueurs actifs à 13.

C'est la première investigation approfondie dans les processus et dans la base de registre de Windows pour la télémétrie

L'analyse est très détaillée, et cartographie le système *Event Tracing for Windows* (ETW), la manière dont Windows enregistre les données de télémétrie, comment et quand ces données sont envoyées aux serveurs de Microsoft, ainsi que la différence entre les différents niveaux de paramétrage de la télémétrie.

Cette analyse va jusqu'à montrer où sont contrôlés les réglages pour modifier individuellement les composants d'enregistrement dans la base de registre de Windows, et

comment ils initialisent Windows.

Voici quelques faits intéressants issus de ce document :

• Windows envoie vos données vers les serveurs Microsoft toutes les 30 minutes ;
• La taille des données enregistrées équivaut à 12 à 16 Ko par heure sur un ordinateur inactif (ce qui, pour donner une idée, représente chaque jour à peu près le volume de données d'un petit roman comme Le Vieil homme et la mer d'Hemingway) ;
• Il envoie des informations à sept endroits différents, y compris l'Irlande, le Wyoming et la petite ville de Boston en Virginie.

Hostname	IP address	Location
geo.settings-win.data.microsoft.com.akadns.net, db5-eap.settings-win.data.microsoft.com.akadns.net, settings-win.data.microsoft.com, db5.settings-win.data.microsoft.com.akadns.net, asimov-win.settings.data.microsoft.com.akadns.net	40.77.226.249	Ireland, Dublin
db5.vortex.data.microsoft.com.akadns.net, v10-win.vortex.data.microsoft.com.akadns.net, geo.vortex.data.microsoft.com.akadns.net, v10.vortex-win.data.microsoft.com	40.77.226.250	Ireland, Dublin
us.vortex-win.data.microsoft.com	13.92.194.212	Virginia (US), Boston
eu.vortex-win.data.microsoft.com	52.178.38.151	Netherlands, Amsterdam
vortex-win-sandbox.data.microsoft.com	52.229.39.152	California (US), Los Angeles
alpha.telemetry.microsoft.com	52.183.114.173	California (US), Los Angeles
oca.telemetry.microsoft.com	13.78.232.226	Wyoming (US), Cheyenne

C'est la première « plongée en eaux profondes » que je voie où sont énumérés tous les enregistrements, ainsi que les endroits où va le trafic et à quelle fréquence.
Logiquement l'étape suivante consiste à découvrir ce qui figure dans ces 300 Ko de données quotidiennes. J'aimerais aussi savoir à quel point l'utilisation de Windows Media Player, Edge et les autres applications intégrées influe sur l'empreinte laissée par les données, ainsi que le nombre d'éléments actifs d'enregistrement.

Difficile de se prémunir

Au sein des communautés dédiées à l'administration des systèmes ou à la vie privée, la télémétrie Windows est l'objet de nombreuses discussions et il existe plusieurs guides sur les méthodes qui permettent de la désactiver complètement.

Comme toujours, la meilleure défense consiste à **ne pas utiliser Windows**. La deuxième meilleure défense semble être d'utiliser la version de Windows pour les entreprises où l'on peut désactiver la télémétrie d'une manière officielle. La troisième est d'essayer de la bloquer en changeant les paramètres et clefs de registre ainsi qu'en modifiant vos pare-feux (en dehors de Windows, parce que le pare-feu Windows ignorera les filtres qui bloquent les IP liées à la télémétrie Microsoft) ; en sachant que tout sera réactivé à chaque mise à jour majeure de Windows.

À propos de Derek Zimmer

Derek est cryptanalyste, expert en sécurité et militant pour la protection de la vie privée. Fort de douze années d'expérience en sécurité et six années d'expérience en design et implémentation de systèmes respectant la vie privée, il a fondé le *Open Source Technology Improvement Fund* (OSTIF, Fond d'Amélioration des Technologies Open Source) qui vise à créer et améliorer les solutions de sécurité *open source* par de l'audit, du *bug bounty*, ainsi que par la collecte et la gestion de ressources.

21degrés de liberté – 13

Nos comportements font désormais l'objet d'une surveillance de plus en plus intrusive de la part du commerce, qu'il soit ou

non virtuel, au point de surveiller même les achats que nous ne faisons pas…

Voici déjà le 13e article de la série écrite par Rick Falkvinge. Le fondateur du Parti Pirate suédois. Il attire aujourd'hui notre attention sur une forme inattendue du pistage à caractère commercial.

Le fil directeur de la série de ces 21 articles, comme on peut le voir clairement dans les épisodes précédents que nous vous avons déjà livrés, c'est la ***perte de certaines libertés*** *dont nous disposions encore assez récemment, avant que le passage au tout-numérique ne nous en prive.*

On espionne non seulement tout ce que nos enfants achètent, mais également tout ce qu'ils N'ACHÈTENT PAS

Source : Rick Falkvinge sur privateinternetaccess.com

Traduction Framalang : draenog, dodosan, goofy et un anonyme

Nous avons vu comment les achats de nos enfants, que ce soit en liquide ou par carte, sont surveillés au mépris de leur vie privée, d'une manière qui aurait fait frémir nos parents. Pire encore : la vie privée de nos enfants est également violée par l'espionnage des achats qu'ils ne font pas, qu'ils les refusent sciemment ou qu'ils passent simplement leur chemin.

Amazon vient d'ouvrir son premier magasin *Amazon Go*, où il est possible de mettre des articles dans son sac et de partir, sans avoir à passer par une caisse. Pour présenter ce concept[2], Amazon indique qu'il est possible de prendre un article, qui sera inscrit dans vos achats, puis de changer d'avis et de le reposer, auquel cas le système enregistre que l'article n'a pas été acheté.

Évidemment, on ne paie pas pour un article à propos duquel on a changé d'avis, ce qui est le message de la vidéo. Mais il ne s'agit pas seulement d'enlever un article du total à payer : Amazon sait que quelqu'un a envisagé de l'acheter et ne l'a au final pas fait, et l'entreprise utilisera cette information.

Nos enfants sont espionnés de cette manière chaque jour, si ce n'est à chaque heure. Nos parents n'ont jamais connu cela.

Lorsque nous faisons des achats en ligne, nous rencontrons même des plugins simples pour les solutions commerciales les plus courantes, qui réalisent ce qu'on nomme, par un barbarisme commercial, une « analyse en entonnoir » ou « analyse d'abandon de panier », qui détermine à quel moment nos

enfants décident d'abandonner le processus d'achat.

On ne peut même plus quitter un achat en cours de route sans qu'il soit enregistré, consigné et catalogué pour un usage futur.

Mais cet « abandon de panier » n'est qu'une partie d'un plus vaste problème, à savoir le pistage de ce qui nous intéresse, à l'ère de nos enfants du numérique, sans pour autant que nous l'achetions. On ne manque pas aujourd'hui de personnes qui jureraient avoir tout juste discuté d'un type de produit au téléphone (disons, « jupe noire en cuir ») pour voir, tout à coup, des publicités spécifiques pour ce type de produit surgir de tous les côtés sur les pubs Facebook et/ou Amazon. Est-ce qu'il s'agit vraiment d'entreprises à l'écoute de mots-clés via notre téléphone ? Peut-être, peut-être pas. Tout ce qu'on sait depuis Snowden, c'est que s'il est techniquement possible de faire intrusion dans notre vie privée, alors c'est déjà en place.

(On peut supposer que ces personnes n'ont pas encore appris à installer un simple bloqueur de publicités… Mais bon.)

Dans les endroits les plus surchargés en pubs, comme les aéroports (mais pas seulement là), on trouve des traqueurs de mouvements oculaires pour déterminer quelles publicités vous regardez. Elles ne changent pas encore pour s'adapter à vos intérêts, comme dans *Minority Report*, mais puisque c'est déjà le cas sur votre téléphone et votre ordinateur, il ne serait pas surprenant que cela arrive bientôt dans l'espace public.

Dans le monde analogique de nos parents, nous n'étions pas enregistrés ni pistés quand nous achetions quelque chose.

Dans le monde numérique de nos enfants, nous sommes enregistrés et suivis même quand nous n'achetons pas quelque chose.

La vie privée demeure de votre responsabilité.