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.