Windows 10 aspire vos données personnelles toutes les 5 minutes

On le sait, Windows 10 est un véritable aspirateur à données personnelles. Et un nouveau rapport vient confirmer, s'il était besoin, les indiscrétions de l'OS de Microsoft jetant un peu plus d'huile sur le feu d'une polémique que tente d'éteindre l'éditeur qui indique anonymiser les données personnelles. Plixer, une société américaine spécialisée dans la surveillance et la sécurisation des flux de données, s'est à son tour penché sur les informations que Windows 10 envoie aux serveurs de Redmond. Et le résultat tend à confirmer les conclusions des précédents constats. *« Nous avons décidé d'enquêter sur plusieurs éditeurs et le résultat pour certains d'entre nous est un peu effrayant »*, annonce la société de Kennebunk (Maine) dans son rapport (dont l'accès nécessite de remplir un formulaire).

Plixer y rappelle que, si l'utilisateur laisse la configuration livrée par défaut à l'installation de l'OS ou à l'achat d'un nouveau PC, *« la moins respectueuse de votre vie privée »*, Microsoft récupère des informations sur les contacts, l'agenda, le texte saisi, ainsi que les interactions tactiles, la localisation des données *« et bien plus »*. Autant de données que l'utilisateur n'aura d'autre choix que de laisser partir s'il veut profiter de Cortana, l'assistant vocal de Windows 10.

Plixer a également regardé ce qui se passe quand toutes les options propres à l'utilisation des données privées sont désactivées. Et les résultats ne sont pas tristes, comme on s'en doute. Ainsi, même une fois les options les plus protectrices de la vie privée activées, *« une certaine forme de métadonnées était encore envoyée à Microsoft toutes les 5 minutes »*. Lesquelles ? Difficile à dire puisque Microsoft les chiffre. Elles sont envoyées à ssw.live.com depuis le port 80 sur une connexion HTTP non sécurisée. Alors que l'éditeur aurait pu choisir une liaison sécurisée HTTPS sur port 443 pour éviter que des oreilles indiscrètes ne s'intéressent aux paquets échangés. *« Cet effort supplémentaire pour chiffrer indique que non seulement Microsoft ne veut pas que les utilisateurs non autorisés de la machine accèdent aux données [mais] aussi qu'il ne veut pas que l'utilisateur final sache ce qui est envoyé »*, affirme sans détour le rapport.

Les données télémétriques impossible à désactiver

Autre écueil, l'exploitation des données télémétriques dont l'usage est regroupé dans une fonctionnalité de stratégie de groupe baptisée Allow Telemetry. *« Le seul moyen de désactiver cette fonction intégralement est, malheureusement, de souscrire à la version Entreprise de Windows 10 »*, écrit Plixer. Qui ajoute : *« nous soupçonnons [que les données envoyées] contiennent des détails sur votre profil, notamment votre adresse IP faciale. »* Plixer laisse entendre que l'envoi de cette dernière, renfermant des données de géolocalisation, serait nécessaire pour établir la connexion avec les serveurs du premier éditeur mondial.

[Lire aussi notre dossier : Windows 10, un OS aux multiples facettes]

Pour conserver le contrôle de ses données, l'utilisateur n'a d'autre choix que de bloquer, au niveau du firewall, les serveurs de Microsoft qui se montrent trop indiscrets (particulièrement ceux cachés derrière les adresses IP 55.113.11, 65.55.113.12, 65.55.113.13, et 134.170.30.221 aujourd'hui). Un choix risqué puisque la firme de Satya Nadella pourrait changer l'usage de ces adresses pour, par exemple, y basculer le service de mise à jour Windows Update qui se retrouverait donc bloqué.

Plixer suggère également de détourner, au niveau du serveur DNS de l'entreprise, le trafic émis vers les domaines ssw.live.com et dmd.metaservices.microsoft.com pour le rediriger vers une autre destination (le localhos, ou 127.0.0.1, par exemple). Sachant que, là aussi, les utilisateurs ne sont pas à l'abri d'un changement de domaine décidé par Redmond. Les utilisateurs français, peuvent de leur côté espérer que Microsoft mette Windows 10 en conformité avec les exigences de la Cnil (ce qui, au mieux, ne fera que limiter la collecte ou apporter une plus grande transparence sur l'utilisation des données, sans en arrêter l'exfiltration).

Il n'y a pas que Microsoft

Microsoft n'est pas le seul à exceller dans la récupération d'informations à caractère privé. Plixer s'est également intéressé aux pratiques de Plantronics et McAfee (aujourd'hui entre les mains d'Intel Security). Dans le premier cas, il s'avère que, lorsqu'ils sont connectés au Plantronics Hub, les casques audio du constructeur envoient des données chiffrées toutes les minutes vers les serveurs de la firme. Sans celle-ci ne précise pas dans ses licences produit quelles données sont ainsi récupérées. Plixer soupçonne l'envoi des numéros de téléphones appelés ou encore des données sur la qualité des appels. Mais sans certitude.

Dans le cas de McAfee, Plixer soupçonne l'éditeur d'antivirus de s'appuyer sur une URL ultra longue (comme a-0.19.a7000001.90d0083.1644.1ff1.36d4.210.0.pse53rw8vethftele7m28hf5uv.avts.mcafee.com) pour y dissimuler un message chiffré lorsque le logiciel de sécurité de la machine établit une connexion avec les serveurs de l'éditeur. *« Bien que nous convenons que McAfee est un fournisseur de confiance, nous aimerions savoir ce qu'il envoie, nous voulons être en mesure de déchiffrer le message en utilisant des méthodes de déchiffrement traditionnellement acceptées, et nous voulons avoir la possibilité de le désactiver »*, pestent les auteurs du rapport. Et de conclure qu'il *« est peut être temps pour nos gouvernements d'intervenir et de s'impliquer pour créer une législation qui empêche les entreprises de prendre d'excessives libertés dans l'exploitation der nos informations personnelles identifiables »*.

Lire également
Pourquoi Windows 10 est une porte ouverte sur vos données personnelles
Même paramétré, Windows 10 envoie des données à Microsoft
Windows 10 : des apps pour bloquer la collecte de données

crédit photo © Gajus – shutterstock