INNOVATION & SOLUTIONS | GUERRE EN UKRAINE | NEWS
Publié le 07 mars 2022, 13:25. Modifié le 08 mars 2022, 12:04.

Kaspersky, un antivirus russe qui n'est plus en odeur de sainteté

par Grégoire Barbey

L'entreprise russe Kaspersky fournit des logiciels de cybersécurité. | Kaspersky

«Dans le contexte actuel, l'utilisation de certains outils numériques, notamment les outils de la société Kaspersky, peut être questionnée du fait de leurs liens avec la Russie», écrit l'Agence nationale française de sécurité des systèmes d'information (ANSSI) dans une note publiée mercredi 2 mars. En Suisse, nombre d'entreprises et de particuliers ont recours aux produits de l'entreprise russe Kaspersky, qui commercialise notamment des antivirus. Faut-il s'en distancer?

Pourquoi on en parle. Kaspersky est une entreprise fondée par Eugene Kaspersky, un spécialiste de la cybersécurité diplômé de la haute école des services de renseignement russes (FSB). Le siège social de l'entreprise et une partie de ses centres de recherche et développement sont basés en Russie.

La prudences s'impose. «De manière générale, quand on fait appel à un service ou qu'on achète un produit informatique, on est tributaire du pays où est basé le fournisseur, relève Steven Meyer, CEO de l'entreprise de cybersécurité ZenData à Genève. Que ça soit les Etats-Unis avec Microsoft, Israël avec les produits de NSO Group ou la Russie avec Kaspersky.»

Compte tenu des liens présumés d'Eugene Kaspersky avec les services de renseignement russes – l'intéressé s'en défend –, Steven Meyer n'a jamais recommandé l'utilisation des outils de l'entreprise russe à ses clients. «Il existe un scénario, très théorique, où le gouvernement russe prendrait le contrôle de Kaspersky pour diffuser des mises à jour malveillantes, même si je n'y crois pas», souligne Steven Meyer. En 2017, l'administration

Trump a banni l'utilisation des outils de Kaspersky au sein du gouvernement américain, estimant qu'ils représentaient un «risque grave» pour la sécurité nationale.

Le risque le plus concret, comme le relève l'ANSSI et de nombreux experts en cybersécurité, c'est que l'entreprise ne puisse plus fournir de mises à jour à ses clients étrangers à terme. Soit parce que les sanctions occidentales l'en empêchent, soit parce que le gouvernement russe le lui interdirait en guise de représailles face aux décisions occidentales.

Le tweet controversé d'Eugene Kaspersky / Capture d'écran

Une position controversée sur la guerre en Ukraine. Eugene Kaspersky a suscité la controverse dans le milieu de la cybersécurité après la diffusion d'un tweet dans lequel il utilise la formulation «situation en Ukraine» le 1er mars pour évoquer l'invasion russe. Une manière sans doute de rester dans les bonnes grâces d'un gouvernement russe qui multiplie la répression contre les entités qui ne se plient pas aux éléments de langage instaurés par les autorités pour parler de la guerre en Ukraine.

Ce d'autant plus que, d'après *Cybernews*, l'infrastructure web du Ministère russe de la défense semble être protégée par… Kaspersky. L'entreprise s'en défend et affirme par ailleurs tout mettre en œuvre pour protéger les données personnelles de ses clients. A noter que le centre de traitement des données de Kaspersky est basé en Suisse depuis deux ans.

Une transparence inédite. Comme d'autres sociétés du secteur des télécommunications et de la cybersécurité, Kaspersky publie un rapport annuel détaillant l'ensemble des demandes de coopération émises par les autorités du monde entier et la réponse donnée par l'entreprise pour chacune d'elle. Là où Kaspersky se distingue de la concurrence, c'est avec son centre dédié à la transparence. L'entreprise donne accès à l'ensemble du code source de ses services et est audité par un organisme indépendant. Mais ces gages de bonne foi ne convainquent pas les experts dans le contexte actuel.

Le choix du boycott. En France, la fédération de défense des consommateurs, l'UFC Que Choisir, a formellement pris ses distances avec Kaspersky, retirant les produits de l'entreprise russe de l'ensemble de ses comparateurs. Contactée, la Fédération romande des consommateurs (FRC) répond:

> «La FRC rejoint l'UFC Que Choisir dans son analyse. Considérant la situation actuelle, la capacité de mettre à jour l'antivirus édité par l'entreprise Kaspersky peut être compromise à moyen terme. Nous recommandons donc aux consommateurs de privilégier un antivirus pérenne mis à jour très régulièrement et adapté au système d'exploitation de l'ordinateur.»

Steven Meyer ne fait pas de recommandation à l'égard d'un antivirus en particulier. Il relève néanmoins qu'en général, les produits achetés par les particuliers sont bons. «Le problème, c'est plutôt la configuration de l'antivirus, souligne le CEO de ZenData. Lorsqu'un antivirus signale le blocage d'un logiciel malveillant, cela ne signifie pas forcément que cette action a empêché le virus de mener à bien sa mission. Il faut parfois du temps pour qu'un antivirus puisse détecter un malware.»

Pour l'expert, il n'en reste pas moins indispensable de continuer à protéger ses appareils, smartphones et tablettes compris, avec des logiciels de sécurité. Ce d'autant plus dans un contexte de vulnérabilité informatique exacerbé.

A noter qu'en Suisse, le Centre national pour la cybersécurité se montre beaucoup plus prudent que son équivalent français. Contacté par *Heidi.news*, il précise:

> «Le NCSC analyse en permanence l'évolution de la situation sur le plan des cybermenaces. S'il n'est jamais exclu que des Etats puissent influencer le développement de logiciels, une estimation de l'influence ou non de la Russie dans ce cas est difficile et ne pourrait que relever de la spéculation.»

Guerre En Ukraine **Cybersécurité** **Cyberdéfense** **Russie** **Solutions**