L’antivirus Kaspersky complice, ou victime, d’un vol de données de la NSA

Kaspersky subit une nouvelle charge en provenance des Etats-Unis. Selon le *Wall Street Journal*, l’antivirus de l’éditeur russe aurait permis à des pirates travaillant pour le gouvernement de Vladimir Poutine de dérober des données stratégiques de la NSA, l’Agence nationale américaine de la sécurité.

Dans les faits, un sous-traitant de la NSA aurait, en 2015, rapporté des informations confidentielles à son domicile pour les transférer sur son ordinateur personnel. Une machine protégée par l’antivirus Kaspersky. Lequel aurait été en mesure de permettre aux pirates de détecter que les fichiers provenaient de l’agence américaine puis de pénétrer la machine à partir de failles de sécurité de l’antivirus pour dérober les documents.

Les données en question se rapportaient à la façon dans les services américains infiltrent les réseaux informatiques étrangers et se défendent contre des cyberattaques. *« Le vol est considéré par les experts comme l’une des violations de sécurité les plus importantes de ces dernières années*, déclare une source anonyme au *WSJ*. *Il offre un aperçu de la façon dont la communauté du renseignement pense que le renseignement russe exploite un logiciel commercial largement disponible pour espionner les États-Unis. L’incident s’est produit en 2015, mais il n’a été découvert qu’au printemps de l’an dernier. »*

Une lutte géopolitique

Le quotidien américain n’avance aucune preuve concrète et se réfère à des sources dites « proches du dossier ». De son côté, Kaspersky réfute farouchement de telles accusations. *« Kaspersky Lab n’a reçu aucune preuve de l’implication de la compagnie dans l’incident rapporté par le* Wall Street Journal *le 5 octobre 2017 […], et il est regrettable que la couverture médiatique des allégations non prouvées continue de perpétuer les accusations portées contre la compagnie »*, peut-on lire dans son communiqué.

Et la firme de continuer à rappeler que, en tant que société privée, elle n’a aucun lien *« inapproprié »* avec un gouvernement, y compris la Russie, son pays d’origine. Pour l’éditeur, *« la seule conclusion semble être que Kaspersky Lab est pris au milieu d’une lutte géopolitique »*.

Certes, Kaspersky n’est peut-être pas directement impliqué dans ce vol. Les pirates se sont peut-être contentés d’exploiter les vulnérabilités de sa solution. Car, comme tous les logiciels, le code de la suite de sécurité russe n’est pas sans défaut. Et, à plusieurs reprises, des bugs de sécurité y ont été découverts. Notamment par Travis Ormandy, un chercheur du Project Zero de Google qui avait fait remonter un faille zero day en septembre 2015. Mais le code de Kaspersky n’est certainement pas plus, ni moins, troué que celui de ses concurrents.

Le SI de la NSA aussi troué que le code de Kaspersky

La vulnérabilité mise à jour par Google aura donc peut-être été exploitée dans l’affaire remontée

par le *WSJ*. Mais c'est quand même un heureux hasard que cela tombe sur Kaspersky alors que le FBI et les autorités américaines ne cessent ces derniers temps de taper sur l'éditeur russe.

Ce qui est aussi très étrange est la façon dont l'affaire a été menée. Comment un sous-traitant de la NSA pouvait encore, en 2015, être en mesure de rapporter des devoirs à la maison ? L'Agence de sécurité n'aurait donc par renforcé son système anti-fuite alors que les révélations en 2013 d'Edward Snowden, ex sous-traitant de la NSA, ont fait scandale sur les pratiques d'espionnage numérique des Américains (et Britanniques) ?

C'est à croire que le SI de l'Agence de sécurité est aussi troué que le code de Kaspersky. Dans ses conditions, à défaut de regarder la nationalité des éditeurs pour sélectionner ses fournisseurs de sécurité, l'administration américaine devrait peut-être commencer par faire le ménage dans ses méthodes de travail.

Lire également

Sécurité IT : l'administration américaine bannit les solutions Kaspersky
Le FBI appelle les entreprises US à abandonner Kaspersky
Kaspersky veut concurrencer Windows Defender avec un antivirus gratuit