Kaspersky accusé d'avoir infecté ses concurrents avec de faux virus

Selon Reuters, Kaspersky a tenté de faire passer des fichiers bénins pour malicieux afin de tromper les capacités de détection de ses concurrents sur le marché des antivirus. Ces affirmations, très graves pour l'éditeur russe, se basent sur les déclarations à nos confrères de deux ex-employés de la société basée à Moscou, aujourd'hui parmi les leaders mondiaux des logiciels de sécurité.

Cette duperie, qui aurait démarré il y a plus de dix ans – avec un pic entre 2009 et 2013 -, ciblait notamment les antivirus de Microsoft, AVG ou Avast et visait à les inciter à effacer des fichiers importants sur les PC de leurs utilisateurs. Les deux sources de nos confrères, qui demeurent anonymes, affirment que des chercheurs ont été affectés à ces sabotages pendant des semaines ou des mois, avec pour tâche principale la rétro-ingénierie des technologies de détection des concurrents ciblés. Une étape indispensable à la mise au point de faux positifs.

Intoxiquer la concurrence

Reuters assure que, dans certains cas, la décision a été prise par Eugene Kaspersky en personne (en photo ci-dessus), le fondateur de l'éditeur russe souhaitant se venger de concurrents qui, selon lui, se contentaient d'imiter sa technologie. La société a démenti ces pratiques, assurant « *n'avoir jamais mené de campagne secrète pour tromper des concurrents avec de faux positifs (des fichiers bénins identifiés comme malwares, NDLR)* ».

En 2010, Kaspersky s'était plaint de l'exploitation que ses concurrents faisaient de ces travaux. A l'appui de sa démonstration, l'éditeur avait créé 10 fichiers sans risque et les avaient déclarés comme malicieux à VirusTotal, l'outil de partage d'informations sur les menaces de Google. Une semaine et demi plus tard, 14 fournisseurs d'outils de sécurité estimaient ces fichiers dangereux, suivant aveuglément les conclusions de la société russe, selon Kaspersky.

D'après les deux sources de Reuters, Kaspersky ne se serait pas arrêté à cette opération de communication. La société injectait ainsi du code malicieux dans des fichiers fréquemment rencontrés sur les PC puis les signalait anonymement à VirusTotal dans l'espoir de voir les antivirus concurrents assimiler ces fichiers essentiels au fonctionnement d'un PC à des malwares.

Pratiques connues

Reuters affirme par ailleurs que Microsoft, AVG et Avast lui ont confirmé que des tiers non identifiés avaient tenté d'introduire de faux positifs dans leur mécanisme de détection au cours des dernières années. Dennis Batchelder, qui dirige la recherche antimalware de Microsoft, a ainsi expliqué à Reuters avoir identifié, à partir de mars 2013, des fichiers altérés afin de paraître malicieux. Et d'affirmer que ses équipes ont isolé des centaines, voire des milliers de cas de la sorte. Sans toutefois faire un quelconque lien avec Kaspersky. Plus largement, aucun concurrent du Russe n'a émis de commentaire sur l'implication éventuelle de la société moscovite.

A lire aussi :

Eugène Kaspersky : « nous allons nous focaliser sur la sécurité industrielle »

Hacking : pourquoi les États s'en prennent aux éditeurs de sécurité