Kaspersky : de faux virus oui, mais nous en avons été victimes

Il a beau jeu, Eugene Kaspersky, de pointer les faiblesses de l'enquête de Reuters concernant sa société. Dans un billet de blog, le fondateur de l'éditeur de logiciels de sécurité écrit que l'article de nos confrères, qui pointe la responsabilité de la société dans la création et la diffusion de faux virus afin d'intoxiquer ses concurrents, est « *un mélange de faits avec une généreuse quantité de pure fiction* ». Et de critiquer le fait que l'article en question s'appuie sur des témoignages anonymes. Pour son scoop, Reuters cite en effet **deux sources non identifiées** qu'il présente comme d'ex-employés de l'éditeur. Ces deux sources affirment que Kaspersky a délibérément injecté du code malicieux dans des fichiers fréquemment rencontrés sur les PC puis les a signalés anonymement à VirusTotal (outil de partage d'informations sur les menaces de Google) dans l'espoir de voir les antivirus concurrents assimiler ces fichiers à des malwares. Des affirmations aussitôt démenties par la société.

Voir une société spécialiste de la sécurité – secteur qui a massivement recours à l'anonymisation pour protéger l'identité de ses clients – critiquer vertement des journalistes qui y font appel pour protéger leurs sources ne manque toutefois pas de sel.

Une attaque d'origine inconnue

Dans son billet de blog, Eugène Kaspersky va cependant au-delà de cette attaque facile. Il explique que ces faux-positifs (des fichiers non infectieux mais repérés par les antivirus) ont bel et bien touché les éditeurs d'outils de sécurité. « *Malheureusement, nous faisions partie des entreprises sérieusement touchées par ce problème* », ajoute l'homme d'affaires russe, selon qui il s'agissait d'une attaque coordonnée contre l'industrie de l'antivirus dans son ensemble. « *Quelqu'un diffusait des fichiers légitimes entrelacés avec du code malicieux afin de tromper les moteurs d'antivirus de nombreuses entreprises, dont Kaspersky* », assure le fondateur de l'éditeur. Selon ce dernier, **l'attaque s'est étalée sur 2012-2013** et l'auteur de cette campagne d'intoxication resterait inconnu à ce jour.

Eugène Kaspersky assure que ses concurrents ont eux aussi identifié des fichiers spécialement modifiés afin de tromper leur outil de détection. « *Au total, nous avons reçu plusieurs douzaines de fichiers légitimes renfermant du code malicieux* », écrit Eugène Kaspersky. Et d'expliquer que les outils maison ont depuis été mis à jour pour éviter de tomber dans ce genre de pièges.

Les slides de Microsoft

Le fondateur de la société russe ajoute d'ailleurs que, courant 2013, **une réunion a été organisée sur le sujet**. Elle rassemblait les éditeurs visés par l'attaque ainsi que d'autres acteurs au courant de cette campagne, selon Kaspersky. « *Malheureusement, la réunion n'a débouché sur aucune percée capitale, même si d'intéressantes théories sur l'origine de l'attaque ont été émises* », écrit le Pdg. Dans un communiqué, l'éditeur pointe vers un lien renfermant des slides émanant de Microsoft ; diapositives qui auraient été diffusées lors de cette réunion ou en marge de celle-ci. Cette

rencontre entre les éditeurs d'antivirus se serait tenue en octobre 2013 lors de la Virus Bulletin International Conference de Berlin. Dans ces slides, le premier éditeur mondial soupçonne une campagne destinée à étudier les réactions des moteurs de détection et à en tester les limites ainsi qu'une volonté d'**exploiter la façon dont l'industrie partage l'information sur les menaces**. La présentation de Microsoft précise que les faux positifs ont été soumis sur VirusTotal via le réseau d'anonymisation Tor.

Dans l'enquête de Reuters, Microsoft, AVG et Avast confirment que des tiers non identifiés ont bien 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 et qui est un des auteurs des slides cités ci-dessus, 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. Aucun concurrent du Russe n'a toutefois émis de commentaire sur l'implication éventuelle de la société moscovite.

La piste des services de renseignement

Signalons que les éditeurs d'antivirus sont une cible privilégiée pour les services de renseignement, afin notamment de s'assurer que leurs malwares restent indétectables et d'étudier l'évolution des algorithmes de détection. Des recherches qui leur permettent de concevoir des menaces qui resteront longtemps sous les radars. En juin dernier, un article de *The Intercept*, basé sur des documents exfiltrés par Edward Snowden, assurait que la NSA et ses compères du GCHQ britannique ont ciblé spécifiquement les éditeurs d'antivirus, recherchant des failles dans leurs systèmes, étudiant le trafic réseau entre les logiciels déployés chez leurs clients et leurs serveurs ou encore mettant en œuvre des techniques de rétro-ingénierie afin de décortiquer le fonctionnement de leurs logiciels. Parmi les cibles préférées des deux services de renseignement, selon ces documents… l'éditeur russe Kaspersky.

A lire aussi

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