# Le réseau de Kaspersky piraté par Duqu 2.0

Les cordonniers sont les plus mal chaussés, y compris dans la sécurité. Karsperky a annoncé avoir découvert une attaque avancée sur son propre réseau interne. *« [L'attaque] a été complexe, furtive, elle a exploité plusieurs vulnérabilités zero-day, et nous sommes à peu près certains qu'il ya un Etat-nation derrière elle »*, déclare Eugene Kaspersky dans un billet de blog.

Derrière cette attaque, l'éditeur de solutions de sécurité soupçonne l'intervention d'une organisation étatique. Et plus particulièrement l'équipe à l'origine de Duqu, une menace persistante (APT pour *advanced persistent threat*) qui, en 2011, défrayait la chronique pour ses tentatives d'espionnage du programme nucléaire iranien, de détournement de certificats numériques et dont les traces se retrouvaient également en Hongrie, Autriche, Indonésie, au Royaume-Uni ou encore au Soudan. Comme pour Duqu, l'attaque dont a été victime Kaspersky a tout fait pour rester la plus indétectable possible ce qui la rend d'autant plus difficile à neutraliser. D'où l'appellation de Duqu 2.0 que lui a attribué l'entreprise russe. *« Il semble que les gens derrière Duqu 2.0 étaient pleinement convaincus qu'il serait impossible de voir leur activité clandestine exposée »*, ajoute le fondateur. Qui ajoute avoir pu détecter la menace grâce à la version Alpha de sa nouvelle solution anti-APT.

## Le programme nucléaire iranien espionné

Un nouvel outil qui permet à Kaspersky de délimiter le périmètre de l'attaque. Selon l'éditeur, les assaillants ont cherché à espionner ses technologies propres à la protection des systèmes d'exploitation, à la prévention des fraudes, à la sécurité du réseau et aux solutions et services anti-APT. *« Les malfaiteurs voulaient aussi en savoir plus sur nos enquêtes en cours et en apprendre davantage sur nos méthodes de détection et de capacités d'analyse »*, précise Eugène Kaspersky. Le dirigeant se veut néanmoins rassurant et affirme qu'aucun produit ou service n'a été compromis et que l'attaque ne fait courir aucun risque aux clients de l'éditeur. *« Le code source de nos produits est intact. Nous pouvons confirmer que nos bases de données de logiciels malveillants n'ont pas été touchées, et que les assaillants n'ont pas eu accès aux données de nos clients. »* A croire sur parole.

Le dirigeant en viendrait presque à se réjouir de cette agression dont l'étude va lui permettre de renforcer ses propres technologies de défense. La détection de Duqu 2.0 est ainsi d'ores et déjà introduite dans les produits maison. Ce qui n'empêche pas les équipes des laboratoires de Kasperky de poursuivre leurs enquêtes sur la menace qui aurait déjà espionné les activités de personnalités, notamment les participants aux négociations internationales autour du programme nucléaire iranien et ceux du 70e anniversaire de la libération d'Auschwitz.

## Un coût colossal

Kaspersky va poursuivre son travail d'analyse. Il lui faudra encore plusieurs semaines avant d'évaluer pleinement l'ampleur des dégâts. Si l'éditeur se garde de pointer un gouvernement ou un autre derrière cette attaque, il ne fait guère de doute, à ses yeux, qu'il s'agit d'une organisation suffisamment structurée et motivée pour couvrir le *« le coût colossal »* de développement et maintien de ce framework malveillant. Israël, avec l'aide des Etats-Unis, est soupçonné d'être à

l'origine de la création de Duqu, et son prédécesseur Stuxnet. Certains chercheurs ont avancé qu'Israël pourrait avoir agi seul. Son exclusion des négociations du programme nucléaire iranien conforterait cette volonté d'espionnage des manœuvres de son voisin iranien considéré comme une menace.

Mais Kaspersky se refuse à toute spéculation polémiste. Ce qui n'empêche pas Eugène Kaspersky de pousser sa gueulante. *« Si divers groupes officiant dans l'ombre -souvent liés aux gouvernements- traitent l'Internet comme un Far West sans règles et se déchaînent en toute impunité, cela mettra en danger le progrès global durable des technologies de l'information*, alerte le dirigeant. *Donc, je lance une fois de plus un appel à tous les gouvernements responsables de se réunir et s'accorder sur ces règles, afin de lutter contre la cybercriminalité et les logiciels malveillants, pas les parrainer et les promouvoir. »* A bon entendeur…

---

**Lire également**
Eugène Kaspersky : « nous allons nous focaliser sur la sécurité industrielle »
Un malware résistant à un formatage de disque dur : l'œuvre de la NSA ?
Sécurité : face à la menace Duqu, Microsoft tarde à réagir

**Crédit Photo : AlexSkopje-Shutterstock**