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

Selon un récent article de The Intercept, basé sur des documents exfiltrés par Edward Snowden, 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 : l'éditeur russe Kaspersky.

Un Kaspersky qui, voici quelques jours seulement, annonçait avoir mis au jour « *une cyber-intrusion affectant plusieurs de ses systèmes internes* ». Une attaque perpétrée par « *une nouvelle plate-forme de malware conçue par un des groupes les plus compétents, mystérieux et puissants du monde de l'APT (Advanced Persistent Threat)* ». Une plate-forme que l'éditeur a baptisé Duqu 2.0, en raison de l'exploitation d'une nouvelle version du malware Duqu, identifié en 2011. Ce dernier étant lui-même présenté comme **un cousin de Stuxnet**, le malware qui a ciblé le programme d'enrichissement d'uranium iranien et qui a été conçu, selon les révélations de la presse, par les Etats-Unis et Israël.

En raison de la complexité de cette attaque – qui exploite au moins trois failles zero-day, selon Kaspersky -, l'éditeur penche pour la responsabilité d'un État. « *Nous en sommes à peu près certains* », dit Eugène Kaspersky, dans un billet de blog. Les assaillants ont employés des techniques leur permettant de **rester indétectables très longtemps**, notamment en exploitant un certificat numérique signé par Foxconn probablement dérobé au sous-traitant asiatique. Autre preuve de la sophistication de Duqu 2.0 : le malware tourne uniquement en mémoire, afin de demeurer le plus furtif possible. Selon la société russe, Duqu 2.0 a nécessité des millions de dollars d'investissement. Et n'a été détecté que grâce à la version alpha d'une solution anti-APT à laquelle travaille l'éditeur. Selon Eugène Kaspersky, « *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* ».

RSA et Bit9 déjà pris pour cibles

Cette série d'informations confirme l'intérêt des services secrets étatiques pour les éditeurs de logiciels de sécurité, des acteurs dont la nature se révèle intéressante à plus d'un titre pour des États. Selon nos informations, Kaspersky n'est pas le seul éditeur de solutions de sécurité à avoir été victime d'une attaque probablement perpétrée par un État. Et les États-Unis, via la NSA, ne sont pas les seuls à tenter de s'immiscer sur les systèmes des éditeurs de solutions de sécurité. Un des cinq principaux éditeurs dans le monde dans le domaine, concepteur notamment d'un antivirus, a confirmé à *Silicon.fr* avoir lui aussi été victime d'une attaque menée, selon lui, par **la Chine**. Celle-ci a été découverte il y a environ deux ans.

Ces attaques ne constituent d'ailleurs en rien des surprises pour les experts en sécurité. En 2011 déjà, l'éditeur RSA Security avait été ciblé. Objectif des pirates, selon les données disponibles : dérober des informations sur le système d'authentification à deux facteurs vendu par l'entreprise pour s'introduire chez certains de ses clients, notamment l'industriel américain Lockheed-Martin. Là

encore, les assaillants auraient été liés à un gouvernement, selon RSA. Début 2013, c'est l'éditeur américain Bit9, spécialiste des technologies de listes blanches (référençant les applications légitimes), qui reconnaissait avoir été pris pour cible. Objectif de l'attaque : signer un malware avec un des certificats de l'entreprise, afin que ses clients l'identifie comme un logiciel de confiance.

Pourquoi cibler spécifiquement ces acteurs ? Au moins deux raisons principales s'imposent. Espionner les entreprises spécialisées dans la détection des menaces permet, à un État, de **s'assurer que ses propres malwares restent indétectables**. « *Surveiller les activités de l'entreprise en charge de l'analyse de logiciels malveillants inconnus permet à l'attaquant de s'assurer que sa création n'a pas été détectée ou, au contraire, de modifier rapidement son scénario pour continuer à rester invisible sur la cible réelle* », résume Arnaud Kopp, responsable technique Europe du Sud de Palo Alto Networks (firewall et sécurité des réseaux et des terminaux). Plus largement, disposer d'informations sur la manière dont les équipes de détection orientent leur recherche permet de **concevoir des malwares plus 'performants'**, donc plus longtemps exploitables. « *Le second intérêt peut être de se servir des logiciels de sécurité pour distribuer du contenu malveillant. Des outils comme les antivirus s'exécutent sur toutes les machines avec des droits élevés*, remarque Gérôme Billois, senior manager en gestion des risques et sécurité chez Solucom, un cabinet de conseil intervenant surtout auprès des grandes entreprises. *Dans le cas de Kaspersky, il ne faut pas oublier que cet éditeur fait aussi beaucoup d'interventions sur incidents et d'analyse de malware. Et il est toujours utile de savoir qui est attaqué et comment.* »

Moins sécurisés que Windows ou Acrobat Reader ?

Arnaud Kopp met en exergue un autre intérêt du piratage d'un éditeur comme Kaspersky. « *En plus de leurs clients particuliers, entreprises ou organisations gouvernementales, leur business model comporte la mise à disposition de technologies à destination d'autres éditeurs de solutions de sécurité* », explique-t-il. Autrement dit, la technologie de la société russe est embarquée dans de multiples autres solutions, démultipliant l'intérêt potentiel d'une découverte de vulnérabilité au sein du moteur de Kaspersky. Or, précisément, les cordonniers ne sont pas toujours les mieux chaussés. Selon Joxean Koret, un expert en sécurité de la société singapourienne Coseinc, cité par *The Intercept*, les éditeurs d'antivirus ne sont en effet pas irréprochables : « *Les antivirus, à quelques exceptions près, ont des années de retard sur les applications clientes les plus avancées en matière de sécurité comme les navigateurs ou les lecteurs de documents. Cela signifie qu'Acrobat Reader, Microsoft Word ou Google Chrome sont plus difficiles à pirater que 90 % des antivirus présents sur le marché.* »

Alors les éditeurs de sécurité cibles de choix des espions cyber des nations les plus agressives en la matière ? Probablement. Même si Eugène Kaspersky s'en désole. Dans un billet de blog, le fondateur de l'éditeur éponyme explique ne pas comprendre les motivations de l'État qui s'est attaqué à sa société. Trop de risques, pour trop peu d'informations réellement utiles, selon lui. D'autant que, du fait de la mise au jour de Duqu 2 .0, « *les assaillants doivent maintenant retourner à leur planche à dessin car leur plate-forme est désormais connue de l'ensemble de l'industrie de la sécurité IT* ».

Ne tirez plus sur l'ambulance !

Dans les faits – et comme le laisse augurer le processus de certification de produits mis en place par l'Anssi en France -, le marché de la sécurité est en train d'exploser, avec l'apparition de **marchés**

nationaux où dominent des acteurs locaux ayant la confiance de leur gouvernement. Une évolution qui ne peut que déranger des entreprises se voulant globales comme Kaspersky. Son fondateur compare désormais les cyber-agressions des États au fait de tirer sur les infirmiers sur un champ de bataille : un acte « *méprisable* » et « *honteux* », écrit Eugène Kaspersky.

Pour Gérôme Billois, de Solucom, « *les intérêts des États n'ont jamais été complètement alignés avec ceux des acteurs de la sécurité. En particulier dans les services de renseignements : on le voit bien avec les révélations sur la NSA qui essaie depuis longtemps de diminuer les niveaux de sécurité ou d'introduire des portes dérobées. Et même si les acteurs de la sécurité ont des offres globales et vendues dans le monde entier, pour les actions les plus sensibles, on peut parler d'acteurs 'zonaux' qui reflètent les oppositions entre grands blocs* ». En devenant un enjeu de souveraineté et de domination pour les États, la cybersécurité découvre aussi la realpolitik.

A lire aussi :

Eugène Kaspersky : « nous allons nous focaliser sur la sécurité industrielle »
Un malware résistant à un formatage de disque dur : l'œuvre de la NSA ?

Crédit photo : adike / shutterstock