Le Monde du 12 mai 2024 :
“**Des parlementaires français ciblés par des espions chinois**”

Des parlementaires français ciblés par des espions chinois

Plusieurs élus ont reçu, en janvier 2021, des e-mails envoyés par APT31, un groupe de pirates soupçonné d'être contrôlé par Pékin

Lundi 6 mai, la tête de liste du parti Les Républicains (LR) aux élections européennes, François-Xavier Bellamy, a annoncé avoir fait l'objet d'une tentative d'espionnage en provenance de Chine. Au moment même où le président de la République, Emmanuel Macron, recevait à Paris son homologue chinois, Xi Jinping, M. Bellamy a fait part de son intention de déposer plainte auprès de la section spécialisée J3 du parquet de Paris pour « introduction et maintien frauduleux dans un système de traitement automatisé de données ».

Au cours des dernières semaines, d'autres parlementaires ont également affirmé avoir fait l'objet d'une campagne d'espionnage chinoise. Leur point commun ? Tous sont reliés à l'Alliance interparlementaire sur la Chine (IPAC), un réseau d'élus dont certains membres ont été vivement critiqués par Pékin.

« Il est désormais confirmé que nous sommes sept parlementaires français à avoir été la cible d'une cyberattaque commanditée par l'Etat chinois au début de l'année 2021 », expliquent-ils dans un communiqué publié lundi 6 mai, appelant les autorités françaises à sanctionner les responsables. Des auditions menées par le sénateur des Français établis hors de France Olivier Cadic devraient également avoir lieu à partir du mois de juin, a-t-il été annoncé lors d'une conférence de presse le même jour.

L'origine de toutes ces déclarations n'est pas à aller chercher du côté des services français mais plutôt des enquêteurs fédéraux américains (FBI). Le 25 mars, les autorités américaines ont publié un acte d'inculpation visant sept membres présumés d'APT31. Ce groupe de pirates, soupçonné d'être directement contrôlé par un organe étatique chinois, est relié à de multiples opérations de cyberespionnage depuis une dizaine d'années.

François-Xavier Bellamy a fait part de son intention de déposer plainte

Si le rapport entre peu dans les détails sur les opérations d'APT31 hors du sol américain, on y trouve la mention d'une campagne orchestrée en janvier 2021 et ayant consisté en l'envoi de *« plus de 1 000 e-mails à plus de 400 comptes ou individus associés à l'IPAC »*. André Gattolin, ex-sénateur La République en marche, et Anne Genetet, députée Renaissance, ont confirmé au *Monde* avoir reçu à l'époque un courrier électronique contenant des images, et dont le texte avait notamment trait à la crise liée au Covid-19. Tous deux assurent avoir déposé plainte. D'autres élus de l'IPAC ont reçu des e-mails similaires, en Belgique, en Nouvelle Zélande, ou encore au Royaume-Uni. Selon nos informations, une réunion entre des membres de l'IPAC pris pour cible et les autorités américaines s'est tenue jeudi 9 mai. Du côté des élus tricolores concernés, on déplore un manque de communication des autorités françaises. *« On échange avec le Parlement européen car on ne sait pas si l'opération a été jusqu'au bout »*, explique François-Xavier Bellamy.

Des accès aux messageries

Dans la pratique, selon l'acte d'inculpation de la justice américaine, les images reçues par les élus visaient surtout à rassembler *« des informations techniques »* à leur sujet. Elles contenaient un pixel de suivi, un outil courant dans le marketing qui permet de transmettre à l'émetteur du courriel certains éléments techniques de base sur son destinataire, comme l'adresse de connexion, le navigateur ou le logiciel de messagerie utilisé. Une sorte de phase de reconnaissance avant, potentiellement, d'envoyer un message plus sophistiqué, qui contiendrait par exemple un fichier malicieux.

André Gattolin explique aussi avoir fait l'objet d'une autre attaque durant l'été 2023, qui visait cette fois-ci sa messagerie personnelle chez Microsoft. *« A l'époque il y avait des dysfonctionnements de ma boîte e-mail et je recevais des avertissements de Microsoft »*, se souvient-il. L'ancien sénateur affirme avoir été alerté, peu après, par l'Agence nationale de la sécurité des systèmes d'information et la Direction générale de la sécurité intérieure, d'un piratage réalisé par Storm-0558, un autre acteur soupçonné d'agir pour les autorités chinoises.

En juillet 2023, Microsoft a révélé que ce groupe était derrière une importante campagne de piratage des messageries de ses clients. De nombreux officiels américains ont été pris pour cible, et si l'entreprise américaine fait état d'élus attaqués en Europe, aucune victime française n'avait alors été révélée.

Les rapports de Microsoft suggèrent que Storm-0558 est actif depuis plusieurs années et cherche à obtenir des accès frauduleux aux messageries *« des entités diplomatiques, économiques et législatives américaines et européennes, ainsi que des individus reliés aux intérêts taïwanais ou au dossier des Ouïgours »*. Les experts de l'entreprise ont bien trouvé des liens techniques très ténus avec APT31 et d'autres acteurs chinois, mais affirment *« avec un haut degré de confiance que Storm-0558 est un groupe distinct »*. Contactés, l'Agence nationale de la sécurité des systèmes d'information, le parquet de Paris et le FBI n'ont pas répondu aux sollicitations du *Monde*. ■

FLORIAN REYNAUD