Affaire Epstein : comment un nombre hors-norme de données du FBI liées au pédocriminel ont été soustraites par un pirate «étranger»

Par Steve Tenré

RÉCIT - Un rapport de 64 pages au sein des fichiers Epstein confirme les faits, et étaye minute par minute cet étonnant piratage.

Où sont donc passés ces fichiers, et que contenaient-ils? Les révélations continuent de tomber en série, plusieurs semaines après la publication de millions de documents du dossier Epstein par le ministère de la Justice américain. Après avoir appris que le pédocriminel, mort en cellule le 10 août 2019, entretenait de mystérieuses relations de mécène avec tout le gotha mondial (musiciens français, scientifiques de renommée internationale...), *Le Figaro* a mis la main ce mercredi 11 mars sur un rapport de 64 pages, détaillant quasiment minute par minute la découverte d'une intrusion hors-norme au sein d'un serveur du FBI, contenant plus de 500 To de données liées au financier américain.

La cyberattaque a eu lieu le 12 février 2023 et a été confirmée ce mercredi par une source proche du dossier à Reuters, après des révélations de CNN quelques semaines plus tôt. Le FBI avait lui qualifié l'intrusion d'*«incident isolé»* commis par un *«pirate» «étranger»*, et a assuré avoir, à l'époque, *«restreint l'accès de l'acteur malveillant et rétabli le réseau». «L'enquête est toujours en cours, nous n'avons donc pas d'autres commentaires à fournir pour le moment»*, avait poursuivi le FBI.

Il y aurait, en réalité, beaucoup à dire, à la lumière du rapport figurant dans les dossiers Epstein, alors que ni l'identité ni la nationalité du pirate n'ont été révélées pour l'heure. *«Qui ne chercherait pas à obtenir les dossiers Epstein si vous êtes les Russes ou quelqu'un intéressé par du kompromat?»* a d'ailleurs commenté Jon Lindsay, spécialiste du rôle des technologies émergentes dans la sécurité mondiale au Georgia Institute of Technology. *«Si les services de renseignement étrangers ne considèrent pas sérieusement les dossiers Epstein comme une cible, j'en serais surpris.»*

Détails de l'intrusion heure par heure

Selon le rapport consulté par *Le Figaro* - un document portant sur deux jours de déposition de l'agent Aaron E. Spivack, premier à avoir constaté l'attaque -, l'intrusion a eu lieu en plein Super

Bowl, suivie chaque année par plus d'une centaine de millions de téléspectateurs américains. L'attaque a été repérée le lendemain matin par cet agent de la CT-25, une brigade située à New York et luttant à la fois contre le terrorisme intérieur et l'exploitation sexuelle des enfants.

Dès son arrivée au bureau à 7h30 du matin, un message apparaît sur son ordinateur, prévenant que *«son réseau a été compromis»*. *«J'ai lancé l'antivirus , repéré une menace potentielle et tenté de l'effacer, mais mes privilèges d'administrateurs avaient été révoqués»*, détaille Spivack. À 9 heures du matin, après plusieurs appels à des collègues, l'agent identifie un *«piège informatique»*. *«Le piège se serait déclenché lorsque notre programme Axiom (une solution de criminalistique numérique) l'a analysé»*, poursuit Spivack. Il découvre dans la foulée qu'un des serveurs du FBI a été neutralisé, et apprend auprès de son fabricant qu'un disque dur défaillant est à l'origine de la compromission.

À 15 heures, le serveur n'était toujours pas réparé. *«Après plusieurs recherches, nous nous sommes également rendu compte que les dossiers (du serveur) qui contenaient nos données étaient vides»*, continue l'agent du FBI. 30 minutes plus tard, son équipe parvient à localiser les divers fichiers de connexion et découvre en leur sein deux adresses IP qui n'avaient rien à faire là. L'une d'elles appartenait à un ordinateur du FBI, et l'autre à un ordinateur inconnu, *«ce qui nous a amenés à penser qu'il s'agissait d'un ordinateur ayant accédé à notre réseau d'une manière ou d'une autre»*. Et de déclarer: *«Son activité consistait à parcourir certains fichiers issus de l'enquête Epstein»* C'est la seule fois que Spivack mentionnera le nom du financier lors de ses dépositions, préférant se concentrer sur l'analyse des données et sur les détails de l'attaque.

À 17 heures, le FBI décide d'éteindre tous les serveurs, et de déconnecter Internet. Mais trop tard: le mal est fait, et *«500 terabytes (*teraoctets, en français*) de données ont disparu du fait de l'intrusion»*, selon Spivack. Le nombre est hors-norme, et fait probablement état de données en double ou non compilées. *«J'ai toutefois pu récupérer environ 400 térabytes de ces données. On m'a dit de chercher sur Google comment récupérer les données, mais personne d'autre n'a essayé de nous aider»*, a-t-il également indiqué.

À lire aussi Affaire Epstein : comment le pédocriminel pourrait avoir secrètement «manipulé» les masses

La troublante mention d'une start-up

Le résultat de cette attaque n'a évidemment pas satisfait le FBI, qui décide de blâmer Spivack et son équipe, pourtant l'une des plus émérites de l'organisation. *«Avant l'intrusion, notre équipe était l'une des plus efficaces en matière de lutte contre la traite d'enfant. Notre équipe a sauvé des centaines de victimes et amené devant la justice des dizaines de délinquants sexuels»*, dit-il en conclusion. *«Après l'intrusion, nous avons reçu l'ordre de délaisser nos locaux, et de rendre tous nos appareils pour qu'ils soient analysés. Notre efficacité a chuté de 95,52%.»*

Ces dépositions ont été effectuées dans le cadre d'une enquête du FBI, ouverte contre Spivack, qui aurait *«stocké de manière inappropriée des preuves à son domicile»*, et pour avoir *«dépassé les limites de son autorité en engageant une société extérieure pour développer un logiciel au nom du FBI»*. Car selon l'institution, Spivack n'aurait pas suffisamment protégé ces données. L'agent, lui, se défend tout au long du rapport, expliquant que son équipe devait faire face à des appareils et des logiciels trop lents voire défectueux. Selon le document, il aurait, en 2021, accepté seul les services d'une start-up, ApostleX, spécialisée dans la protection des communications chiffrées. À l'époque,

ApostleX aurait démarché l'ensemble des forces de l'ordre américaines. *«Le manque de technologies permettant de préserver les applications chiffrées ou les communications autodestructrices était un problème largement reconnu»*, s'est justifié Spivack. Le lien entre ApostleX et le dossier Epstein est toutefois peu clair pour l'heure.

L'agence de presse Reuters a pu interroger une source proche du dossier, pour qui l'intrusion était le fait d'un cybercriminel plutôt que d'un gouvernement étranger. Selon elle, le hacker, qui aurait été retrouvé puis confronté plus tard par le FBI en visioconférence, n'aurait même pas eu conscience qu'il avait pénétré un serveur de la police. Il aurait, en sus, exprimé son dégoût après avoir découvert la présence d'images d'abus de mineurs dans les fichiers. A-t-il été interpellé ou au moins sanctionné? L'histoire ne le dit pour l'instant pas. Toujours est-il que l'affaire démontre non seulement la sensibilité du dossier Epstein, mais aussi la fragilité, contre toute attente, de la sécurisation des données, et ce, même au sommet de l'État.

Le ministère de la Justice a publié le 30 janvier dernier *«plus de trois millions de pages»* en partie caviardées de ce dossier, affirmant que l'administration Trump s'était ainsi acquittée de son obligation, imposée par une loi adoptée en novembre par le Congrès, de faire toute la lumière sur ce dossier explosif. Depuis, nombre de dirigeants et personnalités du monde entier ont été éclaboussés par la révélation de leurs liens passés avec Jeffrey Epstein, provoquant enquêtes pénales, arrestations et démissions, principalement en Europe.