financiers. Dans ce scénario hypothétique, détaille l'équipe dans un rapport publié cette année, des hackeurs nord-coréens se servent d'un prestataire de services extérieur, par exemple une société de stockage informatique, pour infiltrer le réseau d'un établissement financier et y implanter un ver autonome qui supprime les données. Lorsque d'autres établissements entrent en communication avec la banque infectée, le ver se propage également à leurs réseaux. Ce scénario vient rappeler qu'une attaque peut rapidement faire boule de neige et que les établissements financiers focalisés sur la sécurisation de leur propre réseau informatique négligent le risque d'être compromis par celui de partenaires de confiance.

Si un tel scénario devait se produire, un programme baptisé Sheltered Harbor ["Havre de sécurité"] pourrait permettre de pallier au moins la perte de données. Mis sur pied par le secteur bancaire en 2015, il a pour but de prémunir les banques contre la disparition de données précieuses à la suite d'une cyberattaque – les données des banques participantes sont cryptées et sauvegardées chaque jour sur des supports sécurisés hors ligne, de sorte qu'elles puissent être restaurées au cas où elles viendraient à être effacées ou modifiées, ou si l'accès en était bloqué.

Entités interconnectées. En vertu d'un décret de la Maison-Blanche de 2013, le ministère de l'Intérieur a dû dresser la liste des infrastructures critiques sur lesquelles un incident de cybersécurité serait susceptible d'avoir des *"effets régionaux ou nationaux catastrophiques sur la santé publique et la sécurité publique, la sécurité économique ou la sécurité nationale"*. Les ministères de l'Intérieur et de l'Économie ont ainsi identifié plus d'une vingtaine de poids lourds du secteur, selon des sources qui préfèrent rester anonymes, ces informations étant jugées sensibles.

Peu de temps après l'élaboration de cette liste, Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan, Morgan Stanley, State Street et Wells Fargo, huit des principaux établissements financiers américains, ont créé le Centre d'analyse et de résilience systémiques pour évaluer les risques de cyberattaques.

Mais les banques elles-mêmes ne sont pas nécessairement le risque numéro un pour le système. Bon nombre de services d'infrastructures indispensables sont composés d'entités interconnectées, ce qui complique la cybersécurité – une attaque lancée contre un acteur clé fait potentiellement peser un risque sur tous les autres. Le secteur financier est plus interconnecté que la plupart des autres et repose sur une poignée de prestataires qui, s'ils sont touchés, peuvent paralyser

JPMorgan, la première banque des États-Unis, dépense 600 millions de dollars par an pour la cybersécurité.

des services et des opérations qui jouent un rôle central pour l'ensemble du secteur. Ce qui comprend les services de traitement des paiements par carte, les chambres de compensation comme ACH [Automated Clearing House] et Fedwire [deux organismes financiers qui servent d'intermédiaires pour les transferts de fonds], et des systèmes de règlement des opérations régissant notamment les échanges d'obligations, d'actions et d'options – par exemple, la National Securities Clearing Corporation et la Depository Trust and Clearing Corporation.

Les organismes financiers ne sont pas les uniques sources d'inquiétudes. Une défaillance de prestataires extérieurs au secteur de la finance, comme les services de *cloud*, les fournisseurs publics d'électricité ou les services de stockage de données, pourrait avoir des répercussions considérables sur les services financiers.

"On a du mal à imaginer les répercussions d'une défaillance, qu'elle survienne par accident ou par malveillance, d'une entreprise informatique jugée 'too big to fail' [*trop grosse pour faire faillite*] (*comme un grand fournisseur de services cloud*)*"*, font remarquer les auteurs d'une étude [du groupe de réflexion] Brookings [de 2018] sur la stabilité financière et les cyber-risques.

Eric Goldstein, directeur adjoint de la cybersécurité à l'Agence de cybersécurité et de sécurité des infrastructures au ministère de l'Intérieur, se garde d'évaluer le degré de préparation du secteur. Il précise que son agence a pour mission d'aider tous les acteurs – pas uniquement dans le secteur de la finance – à mettre en place les contrôles de sécurité et les mesures d'adaptation nécessaires à la poursuite de l'activité en cas d'attaque.

Certains experts jugent les établissements financiers suffisamment solides pour résister à des attaques et aux vagues de retraits massifs qu'elles entraîneraient.

Informer le public. Darrell Duffie, professeur à l'école de commerce de Stanford, s'est penché sur les répercussions potentielles d'une telle cyberpanique dans un article cosigné [en 2019] avec Joshua Younger, administrateur à JPMorgan. Les banques sont tenues de disposer de trente jours de liquidités – c'est-à-dire d'avoir la possibilité d'accéder sous trente jours à des fonds permettant de couvrir l'ensemble des dépôts et lignes de crédit, au cas où tous les clients retireraient leurs liquidités ou se verraient demander de rembourser des crédits. Sur un échantillon de douze grandes banques américaines, les auteurs concluent que toutes disposent de suffisamment de liquidités, ainsi que d'un accès à des fonds supplémentaires de la Réserve fédérale, pour résister à une cyberattaque *"relativement grave"*.

Reste que leur capacité à résister à une cyberpanique n'éviterait pas des dégâts sur l'économie, précisent Darrell Duffie et Joshua Younger. Les marchés financiers, sans doute plus encore que toute autre activité essentielle (élections mises à part), ont besoin de la confiance de l'opinion. Or celle-ci peut s'effriter rapidement, même si l'attaque n'est pas massive.

Les clients professionnels et les entreprises du secteur de la finance qui ne sont pas directement touchés par une attaque mais qui ont besoin d'avoir accès à des sommes d'argent importantes dans un délai très court pourraient décider malgré tout de retirer leur argent des banques pour le placer là où un accès rapide leur est garanti. Ils pourraient également suspendre leurs paiements par mesure de précaution. Par ailleurs, si un service indispensable de traitement ou de paiement se trouvait paralysé, l'instabilité engendrée *"aurait des conséquences dévastatrices sur la performance des marchés financiers"*, confie Darrell Duffie au *New York Times*.

"Si les transactions se poursuivaient sans être honorées, les investisseurs deviendraient extrêmement nerveux", prédit-il, ajoutant que, si l'incertitude devait persister plusieurs jours, les cours pourraient chuter *"vite et fort"*.

Eric Goldstein, au ministère de l'Intérieur, conseille dès lors aux établissements de préparer une stratégie visant à informer explicitement le public des répercussions potentielles d'un incident de cybersécurité, et de la mettre en œuvre dans les meilleurs délais.

"La dernière chose qu'un établissement souhaite, c'est qu'une mauvaise interprétation ou même des informations erronées sur l'incident ne poussent les usagers, les clients ou les fournisseurs à prendre des mesures" qui pourraient aggraver le problème, conclut-il.

—Kim Zetter
Publié le 3 juillet