trans-versales. économie

Et si Wall Street était hacké ?

Les plus grandes banques américaines dépensent des millions en sécurité informatique. Mais les cyberattaques se font plus massives. Et la menace d'une déstabilisation du système financier est réelle.

↙ *Dessin de* **Martirena**, *Cuba.*

—The New York Times *New York*

Lors d'une séance du Congrès [américain] en mai, les patrons des six plus grandes banques de Wall Street se sont vu demander quelle était, selon eux, la plus grande menace qui planait sur leurs établissements et le système financier dans son ensemble. Ils n'ont cité ni la pandémie mondiale, ni le dérèglement climatique, ni les facteurs qui ont contribué à la crise financière de 2008. Leur réponse la plus fréquente a plutôt été : *"La sécurité informatique."*

Voilà au moins une décennie que banquiers, spécialistes de la sécurité et fonctionnaires fédéraux se préparent à des cyberattaques potentiellement dévastatrices pour le secteur financier. Mais le problème se pose avec plus d'acuité encore ces dernières années, du fait de la multiplication des cyberattaques menées par des États contre des infrastructures critiques, comme les attaques informatiques russes qui ont privé l'Ukraine d'une partie de son réseau électrique ou le ver informatique WannaCry – lié à la Corée du Nord – qui a frappé le secteur hospitalier et le commerce international. Le patron de la Réserve fédérale, Jerome Powell, confiait récemment à *60 Minutes* [magazine d'informations de la chaîne américaine CBS] : *"Le risque que nous jugeons prioritaire à l'heure où nous parlons, c'est le cyber-risque."*

Le gouvernement fédéral et les établissements financiers ont créé des cellules d'échanges d'informations, organisé des exercices de simulation et investi massivement dans la cybersécurité. JPMorgan Chase [première banque des États-Unis] dépense à elle seule près de 600 millions de dollars [508 millions d'euros] chaque année dans la cybersécurité et fait plancher *"plus de 3000 collaborateurs"* de près ou de loin sur la question.

Néanmoins, les experts attirent l'attention sur les lacunes béantes en matière de sensibilisation et de préparation à une cyberattaque contre Wall Street, et constatent qu'on se focalise sur des menaces contre des établissements en particulier plutôt que sur des menaces d'ordre systémique. La dernière vague d'attaques au rançongiciel est venue rappeler la vulnérabilité des systèmes informatiques de certaines entreprises.

Les simulations ne suffisent pas. *"Je pense que tout le monde est conscient qu'un établissement peut se retrouver paralysé"*, juge Greg Rattray, ancien directeur de la sécurité informatique au Conseil de sécurité nationale et ancien responsable de la sécurité de l'information de JPMorgan. En revanche, prévient-il, *"on ne prend pas véritablement la mesure du risque systémique"*.

Les plus grandes banques simulent bien des cyberattaques, mais selon Greg Rattray, ces exercices engendrent un sentiment de surconfiance qui est trompeur. Contrairement aux simulations méticuleuses qui servent à préparer secouristes et militaires aux ouragans, aux incendies de forêt ou aux guerres, *"on ne simule pas l'ampleur des dégâts et jamais la durée"* pour les cyberattaques, regrette Greg Rattray. *"On ignore les dommages qu'une cyberattaque pourrait causer, et à quelle vitesse."*

Le système financier pourrait sans doute résister au naufrage d'un poids lourd du secteur, mais si plusieurs grandes institutions financières devaient baisser le rideau à la suite d'une cyberattaque, la pagaille pourrait durer des semaines, met-il en garde.

Par ailleurs, si les hackeurs frappaient pendant une période de forte volatilité sur les marchés – par exemple, pendant un "vendredi des trois sorcières", qui survient une fois par trimestre, quand les stock-options, les contrats à terme et les options sur indice boursier arrivent tous à échéance le même jour –, les effets pourraient être démultipliés.

Une telle attaque réclamerait cependant des compétences, des moyens et une coordination dont les hackeurs n'ont pas fait montre jusqu'à présent. La plupart des cyberattaques lancées à ce jour contre des établissements financiers se résument au détournement de numéros de cartes bancaires et d'identifiants ; quelques attaques ont bien été soutenues par des États, mais elles sont restées limitées quant à leurs répercussions et à leur portée.

À la fin de 2011, des hackeurs iraniens affiliés au corps des Gardiens de la révolution islamique ont lancé pendant plusieurs mois une attaque par déni de service [une attaque qui rend le service indisponible pour les utilisateurs] contre plusieurs dizaines d'établissements financiers américains, dont American Express, JPMorgan et Wells Fargo, selon des documents du ministère de la Justice. L'attaque a bloqué les sites des banques en question, empêchant des centaines de milliers de clients d'accéder à leurs comptes en ligne. Et, en 2016, des hackeurs en cheville avec la Corée du Nord sont parvenus à s'infiltrer dans [le système informatique de] la Banque du Bangladesh et à y subtiliser les identifiants des salariés, avec l'objectif de voler 951 millions de dollars [806 millions d'euros] via le réseau Swift, un système de messagerie utilisé par les établissements financiers. Ils sont parvenus à faire main basse sur 81 millions de dollars [68 millions d'euros].

Des attaques plus élaborées et plus préjudiciables ne sont pas impossibles, cependant. La New York Cyber Task Force – une équipe d'experts issus du public et du privé, réunie par l'université de Columbia et pilotée par Greg Rattray – s'est penchée sur un scénario *"extrême mais plausible"* impliquant plusieurs établissements