# Cyberattaques dans le secteur financier : un état de la menace

**« Connaissez l'ennemi et connaissez-vous vous-même ; en cent batailles vous ne courrez jamais aucun danger. » Sun Tzu, l'art de la guerre**

MALIKA SMAILI,

Auditrice IHEDN, spécialiste en risques du domaine bancaire

Le sujet se démocratise, il devient accessible partout et pour tout le monde mais seulement lorsqu'il est trop tard, lorsque la menace a été mise à exécution et que le système d'information n'est plus disponible, terrassé par une attaque cyber. Toutes les entreprises, quelque soit leur taille, sont des cibles et les établissements bancaires n'y échappent pas. Rappelons-nous de la banque centrale européenne, victime d'une intrusion sur un service de partage de fichiers en janvier 2021, de la bourse de Nouvelle Zélande paralysée pendant quatre jours en août 2020 après une compromission des données de marché, ou des attaques de rançongiciels (ce petit programme informatique qui chiffre les données) dont ont été victimes la filiale asiatique d'AXA en mai 2021 et TRAVELEX en décembre 2019. Lorsque les données sont ainsi codées, il n'est possible de récupérer la clé de chiffrement qu'en échange de paiement d'une rançon à minima ; car il arrive que la victime soit exposée à une double extorsion, lorsque le pirate met en vente les dites données sur le marché noir même après avoir reçu l'argent de la rançon. Un véritable fléau particulièrement pour les données bancaires de millions de clients. Ces attaques ne sont pourtant pas une fatalité à condition de s'y préparer et d'y répondre à temps.

## Boostés par la pandémie et la digitalisation

Comme dans bien d'autres domaines, la crise sanitaire a exacerbé la tendance. Selon un rapport de la Banque des règlements Internationaux (BRI) datant de 2021[1], les institutions financières ont été largement plus exposées à des attaques que la plupart des autres secteurs (en dehors de la santé). Un rapport du FMI sur les pertes que pourraient causer les cyberattaques dans le secteur financier estime le montant à près de 9% du bénéfice net mondial des banques (100 milliards de dollars)[2]. Les attaques à l'encontre d'établissements financiers surfant sur la vague du Covid 19 sont passées de 5000 par semaine en février 2020 à plus de 200 000 en mai de la même année. Beaucoup de clients utilisaient les services bancaires en ligne pour gérer leurs comptes et pour la majorité des paiements. Le télétravail massif a également engendré des situations inédites dans lesquelles des traders travaillaient depuis leur domicile, alors qu'ils sont soumis à des règles règlementaires strictes qui exigent une surveillance et un enregistrement de leurs appels en permanence. Or, partager son réseau avec les autres membres de la famille, pouvait les exposer à des logiciels malveillants ou

1/ https://www.bis.org/publ/bisbull37.pdf
2/ https://www.imf.org/en/Blogs/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

à d'autres opportunités pour le pirate (vol de données, intrusion dans le système, compromission de comptes de traders etc… ).

## Cyberattaques et biais cognitifs

C'est dans le domaine bancaire qui déploie des trésors d'imagination pour maintenir ses performances que l'on observe le plus d'innovation technologique (utilisation massive de cloud, d'intelligence artificielle, numérisation des services…). Profitant de la forte digitalisation du secteur bancaire et de la crise sanitaire, les pirates, sans scrupules, ont déployé des trésors d'imagination pour amener les utilisateurs là où ils voulaient qu'ils aillent : activer certains biais cognitifs bien connus en sciences sociales et jouer sur leurs désirs et leurs émotions. Pour décider, le cerveau humain a tendance à prendre des raccourcis mentaux, plus faciles d'accès et moins coûteux en temps, en énergie et en concentration. Ainsi, il s'agit d'amener la victime à agir en profitant du biais d'autorité ou d'expertise (la cible accorde de la crédibilité au message du fait de la position dont l'attaquant se réclame) ; l'attaquant peut aussi utiliser une stratégie d'urgence (« transmettez-moi le plus vite possible tel document ») ou actionner la curiosité ou l'appât du gain en proposant de remporter la loterie du siècle.

## Etat des lieux de la menace

**Qui sont les attaquants**

Un rapport publié par l'Autorité des Marchés Financiers[3] en 2021, et relatif à l'état de la menace dans le domaine boursier, indique que les cybercriminels sont organisés en groupes spécialisés dans le secteur financier, parfois encouragés par des états (Russie, Chine, Corée du Nord, etc.) utilisant des outils sophistiqués, disponibles dans un véritable supermarché du cybercrime sur le Dark Web.

Parmi les autres typologies d'acteurs, il peut s'agir d'activistes motivés par le rayonnement que pourrait avoir l'impact de l'attaque sur leur cause idéologique. D'autres acteurs malveillants pourraient aussi être motivés par l'abolition de nos systèmes démocratiques ; et quoi de mieux que d'd'exploiter des vulnérabilités systémiques d'un monde financier interconnecté pour entrainer perte de confiance, agitation et chaos social.

**Pourquoi et comment menacent-ils ?**

Du braquage d'une agence à l'attaque informatique ciblée, la motivation du pirate reste la même : le gain financier. Seules les méthodes changent. Mais l'appât du gain n'est pas la seule motivation. Le système bancaire repose sur la confiance du consommateur, l'attaquant peut donc être motivé par l'exécution d'un sabotage visant à déstabiliser le système bancaire ou nuire à l'image de marque de l'institution, surtout si l'attaque génère des perturbations du service à la clientèle. Moins dans le monde bancaire que dans l'industrie, mais cependant non négligeable, il peut s'agir d'espionnage parrainé par des États-nations dans un contexte de tensions géopolitiques afin d'obtenir des informations critiques (secrets d'affaires, renseignements exclusifs, etc..). La Banque de France le rappelle bien dans son dernier rapport évaluant les risques du système financier français publié en 2021[4].

Une des techniques d'attaque les plus populaires dans le secteur bancaire est de cibler les clients, et dans une moindre mesure les collaborateurs après une reconnaissance préalable, en utilisant un mail d'hameçonnage (phishing) qui incite le destinataire à cliquer. Ce clic va permettre le téléchargement silencieux d'un programme qui s'exécutera immédiatement ou qui est programmé pour un déclenchement ultérieur. Une fois le ver dans le fruit, les conséquences sont multiples : pertes financières pour les clients, attaque du système d'information de l'établissement visé etc..

L'autre menace principale et redoutée, est une utilisation d'une chaine d'approvisionnement en exploitant une des ses potentielles vulnérabilités. Les établissements financiers sont particulièrement exposés car ils sont interconnectés dans un écosystème complexe et difficilement traçable, dont le moindre grain de sable pourrait entrainer des réactions en chaines d'une ampleur considérable (risque systémique). Utiliser le maillon le plus faible de la chaine reste donc un bon moyen pour l'attaquant bien

3/ https://www.amf-france.org/sites/institutionnel/files/2020-02/study-stock-market-cybercrime-_-definition-cases-and-perspectives.pdf

4/ https://publications.banque-france.fr/sites/default/files/medias/documents/2021_s1_ers_0.pdf

informé. Et quoi de plus simple que de se renseigner sur le fournisseur de telle ou telle solution digitale bancaire, puis d'attaquer les infrastructures de celui-ci ? le site de relations professionnelles LinkedIn est une source précieuse et ouverte de données accessiblesà tous. Pour exemple, l'affaire Solarwinds en 2021, reste aujourd'hui un cas d'école en matière de compromission des systèmes de distribution de logiciels. C'est l'une des opérations de cyberespionnage les plus sophistiquées de ces dernières années. Les pirates ont eu accès au réseau de l'éditeur et ont infecté son logiciel de gestion, permettant ainsi de cibler l'ensemble des clients de l'éditeur.

Le déni de service distribué reste encore en 2023 un scenario redouté. Il s'agit, via des robots, de générer et simuler un trafic internet très important pour épuiser les ressources du serveur et par conséquent bloquer le site web. Les clients ne pouvant plus se connecter à leur espace, c'est un risque d'image avéré.

D'autres techniques peuvent aussi ébranler les marchés boursiers. Il peut s'agir d'une fausse information diffusée via un « deepfake », des contenus élaborés grâce à une intelligence artificielle et diffusant des informations fausses mais totalement crédibles et réalistes pour les personnes mal informées. L'AMF, mais aussi les régulateurs australiens, anglais et américains ont renforcé le cadre juridique pour lutter contre ce type d'attaques. En France, c'est l'article L465-3-213 du Code monétaire et financier qui sanctionne ce comportement frauduleux. Souvenons-nous de l'affaire Vinci en 2016 et du faux communiqué annonçant des erreurs comptables et le licenciement du directeur financier. L'information reprise par Bloomberg a fait immédiatement plonger le cours de l'action Vinci. Huit minutes après la diffusion de l'information par Bloomberg, l'agence publie un démenti. L'action retrouvera presque instantanément son précédent prix, et l'affaire sera portée devant les tribunaux.

## Atténuation des impacts

Contrôler, évaluer, couvrir, tester sont les maitres-mots de la lutte contre les cyber-attaques. Les banques sont considérées comme des opérateurs d'importance vitale, et le secteur bancaire est l'un des mieux avancés en termes de protection. Malgré une digitalisation très avancée, on ne dénombre aucun incident de portée systémique dans le secteur financier. Les régulateurs ont bien conscience que la résilience du système financier passe par la mise en œuvre d'exigences très fortes, au travers de règlements très contraignants (CROE, DORA, NIS2 ...).Mais la conformité ne règlera pas tout, et déployer des procédures préventives pour simplement ne pas s'exposer au risque d'amende, est insuffisant. Dans certains domaines, seule la mise en place d'un cadre de gestion des risques et de contrôles associés permettra de limiter l'impact d'une attaque.

Il faut veiller à identifier les rôles critiques de l'organisation et estimer leur potentielle exposition à un risque d'espionnage ou d'usurpation d'identifiants de connexion. Renforcer les contrôles permettra d'identifier des vulnérabilités exploitables par des personnes malveillantes. L'humain, maillon de la chaine dans les processus bancaires, devra être sensibilisé très régulièrement, au moins une fois par an, et des tests de phishing régulièrement exécutés pour maintenir sa vigilance à un niveau acceptable.

Il est aussi important de ne pas négliger les sujets opérationnels : Connaitre son système d'information, cartographier ses dépendances, tracer sa chaine d'approvisionnement, réaliser des tests d'intrusion, sont autant d'actions bénéficiant à la prévention. Une bonne connaissance du système d'information permettra également de mieux gérer l'accès à l'information au travers du principe du « besoin d'en connaitre », l'accès aux applicatifs critiques, le filtrage de contenu, la politique de couverture des vulnérabilités logicielles (patching). Les banques et les assureurs français n'ont pas attendu pour s'organiser, ils occupent une place prépondérante au campus cyber, ce lieu voulu par le président Macron, qui permet de mener des projets communs au profit de la cybersécurité. ■

**Malika Smaïli**

Ingénieure en électronique, diplômée en intelligence économique et auditrice de la 3e session nationale souveraineté numérique et cybersécurité de l'IHEDN, Malika Smaïli est aujourd'hui experte en risques opérationnels et cybersécurité du monde bancaire.