Cyberattaques contre les banques et places boursières : source de déstabilisation de l'économie mondiale ?

Daniel Ventre, CNRS (CESDIP). Titulaire de la Chaire Cybersécurité & Cyberdéfense

13 mars 2016. Article IV-9

Nous savons pratiquement tous les systèmes informatisés vulnérables à des cyberattaques, qu'ils soient connectés en réseau ou non. Ces vulnérabilités (failles d'origine technique et humaine) les exposent potentiellement aux actions de la cybercriminalité, des organisations terroristes, des Etats. Les incidents révélés ces derniers jours, n'en sont que les derniers exemples. Des hackers auraient détourné 80 millions de $ de la banque du Bangladesh, sur ses fonds déposés auprès de la réserve fédérale de New York. Les sommes auraient été transférées sur un compte aux Philippines. L'incident aurait eu lieu en février 2016, mais n'a fait l'objet de communiqués que le 11 mars. Les autorités du Bangladesh soupçonnent des hackers chinois.

Nous retrouvons dans cette affaire les ingrédients des recettes de la cybercriminalité : une dimension internationale (plusieurs pays sont ici impliqués : Etats-Unis, Bangladesh, Indonésie, Chine…) qui rendra le traitement de l'enquête plus complexe; des victimes qui tardent à connaître et/ou reconnaître les faits ; des acteurs qui ne sont guère enclins à assumer des responsabilités ; des hackers qui sont capables d'exploiter intelligemment les opportunités qui s'offrent à eux (des systèmes où la protection fait de toute évidence défaut, des ressources financières importantes exposées à qui sait oser les saisir), et qui disposent pour cela des moyens suffisants ou connaissances pour le faire, mais qui dans le même temps échouent dans leur projet à trop en vouloir et font preuve du plus grand amateurisme (ce sont des erreurs d'orthographe dans le libellé des ordres de transfert qui ont fait naître des suspicions). Rappelons que les cyberattaques contre les banques et institutions financières peuvent avoir quatre objectifs principaux : le premier consiste à voler l'argent de ces institutions ; le second prend l'institution financière ou le système bancaire comme cibles et vise à les déstabiliser ; le troisième a pour ambition de perturber une économie toute entière, éroder

la confiance des clients, citoyens, voire semer le désordre dans la société ; le quatrième a une visée politique, activiste (défigurer les sites internet des institutions ; voler leurs données confidentielles et les divulguer…) A chacun de ces objectifs correspondront des acteurs spécifiques, des modes opératoires particuliers.

Au-delà de l'atteinte à l'image des institutions et des pertes purement financières, c'est la question plus large de la sécurité des systèmes informatisés des institutions bancaires et financières qui est soulevée. Depuis de nombreuses années les discours[1] se font de plus en plus alarmants quant aux risques pesant sur l'ensemble des infrastructures critiques, essentielles au fonctionnement de nos sociétés modernes. Le système financier est de celles-ci.

Les systèmes informatisés des institutions bancaires et des places boursières, font certainement l'objet de mesures de cybersécurité. Mais cela n'empêche pas les contournements de ces mesures. Les cas se multiplient :

- La fraude à la carte bancaire est un phénomène planétaire, qui alimente petite et grande délinquance
- En juillet 2015 la bourse de New-York (NYSE) doit interrompre son fonctionnement. La Corée du Nord aurait revendiqué être à l'origine de cette perturbation par cyberattaques[2].
- En 2013, paralysie des réseaux des banques sud-coréennes, bloquant les distributeurs de billets. L'origine en serait une cyberattaque menée par Pyongyang[3]
- En 2013, un groupe de hackers, Cyber Fighters of Izz ad-din Al Qassam, revendique les cyberattaques (par déni de service) qui ont fait tomber les sites internet de 9 grandes banques américaines, durant plusieurs jours pour certaines d'entre elles[4]. Ces attaques proviendraient d'Iran
- En septembre 2015 l'autorité monétaire de Hong Kong affirmait que la cybercriminalité intensifie ses attaques contre les systèmes de ses institutions financières (17 cas rapportés d'attaques par déni de service de janvier à septembre 2015 ; 3 attaques similaires en 2014)[5]
- Le Carbanak Cybergang aurait volé 300 millions de $ en attaquant 100 banques dans 30 pays. (Révélation faite dans un rapport Kaspersky du 14 février 2015. L'info est également publiée par le New York Times[6]).

Nous ne poursuivons pas ici la longue liste qu'ouvrirait un recensement exhaustif des incidents connus. Une étude publiée par la Purdue University[7] en 2014 montre que les incidents subis par les

---

[1] Exemples :
- https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf
- http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518

[2] http://www.thegatewaypundit.com/2015/07/cyber-security-expert-north-korea-takes-credit-for-nyse-attack-no-coincidences-this-is-major-attack-video/

[3] http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0

[4] http://www.reuters.com/article/us-cyber-summit-banks-idUSBRE94G0ZP20130518

[5] http://www.financeasia.com/News/402260,cyber-attacks-on-hong-kong-banks-escalate.aspx

[6] http://www.net-security.org/secworld.php?id=17956

[7] http://www.academia.edu/7600570/U.S._Bank_of_cyber_An_analysis_of_cyber_attacks_on_the_U.S._financial_system

banques américaines du fait de l'exploitation criminelle de leurs réseaux et systèmes informatisés, prennent forme dès les années 1970. Le phénomène semble s'accélérer au cours des deux dernières décennies.

Une question nous paraît essentielle : que sait-on réellement de l'impact que peuvent avoir les cyberattaques menées contre les systèmes critiques que sont ceux des banques et places boursières, sur les économies nationales et sur l'économie mondiale ?

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires