La filière bien structurée de la CYBERCRIMINALITÉ

Les loups solitaires font place à des entreprises spécialistes du piratage informatique

Tamas Gaidosch

La cybercriminalité est devenue une filière bien structurée fonctionnant de manière très semblable à celle des entreprises légitimes en quête de profits. Pour lutter contre le cybercrime, il faut battre en brèche un modèle économique qui emploie des outils simples afin de dégager de gros bénéfices sans grand risque.

Oubliés, les hackers «loups solitaires» de la fin des années 80, qui voulaient prouver leur maîtrise virtuose de l'informatique en faisant intrusion dans les ordinateurs d'autrui. Depuis les années 90, c'est la recherche du profit qui fait désormais battre le cœur des spécialistes du cybercrime, avec tous les attributs des entreprises normales : marchés, bourses et opérateurs spécialisés, services externalisés, chaînes d'approvisionnement intégrées, etc. Plusieurs États-nations ont suivi la même démarche pour amasser un arsenal de cyberarmes servant à la collecte d'informations, à l'espionnage industriel et à fragiliser les infrastructures vulnérables de leurs adversaires.

Évolution

Le cybercrime a proliféré, bien que l'offre de spécialistes ultra-qualifiés n'ait pas augmenté au même rythme que la technicité croissante nécessaire pour mener à bien des attaques fructueuses en toute impunité. L'écart a été comblé grâce au perfectionnement des armes informatiques et de l'automatisation. L'arsenal des pirates s'est considérablement enrichi au cours des vingt dernières années. Dans les années 90, les tests d'intrusion servant à déterminer les points faibles d'un système informatique faisaient fureur dans la profession. La plupart des outils de l'époque étaient simples, souvent fabriqués sur mesure, et, pour les manipuler, il fallait avoir une connaissance approfondie de la programmation, des protocoles de réseau, de l'organisation du système d'exploitation et d'une foule d'autres détails techniques. De ce fait, seul un petit nombre de professionnels étaient capables de repérer les points faibles et d'en tirer parti.

Avec l'arrivée d'outils plus perfectionnés et simples à manier, des adolescents, moins expérimentés, mais motivés (qualifiés non sans dérision de «pirates-débutants»), en ont fait leurs premières armes avec un succès relatif. De nos jours, pour lancer une attaque d'hameçonnage (pratique frauduleuse qui consiste à envoyer un courriel censé provenir d'un correspondant fiable pour obtenir des informations confidentielles), il suffit de maîtriser les concepts de base, d'être motivé et d'avoir quelques fonds en liquide. De nos jours, le plan d'attaque est simple (voir graphique).

Il est extrêmement difficile d'évaluer les pertes dues au cyberrisque. Les statistiques sont rares et peu fiables, en partie parce qu'il y a peu d'intérêt à dévoiler le montant des pertes, surtout si l'incident ne fait pas la une des journaux ou si l'entreprise n'est pas assurée contre le cybercrime. La nature des menaces change rapidement, et les statistiques historiques perdent donc leur utilité pour la prévision des pertes à venir.

La modélisation à base de scénarios, utilisée pour jauger le coût potentiel d'un incident donné sur tel ou tel pays, livre des évaluations de l'ordre de dizaines ou de centaines de milliards de dollars. Lloyd's of London estime à 53,05 milliards de dollars le coût d'une panne de services de stockage infonuagique qui toucherait les pays avancés pendant 2,5 à 3 jours. Une modélisation effectuée par le FMI évalue les pertes totales sur un an à 97 milliards de dollars au mieux et environ 250 milliards de dollars dans le pire des cas.

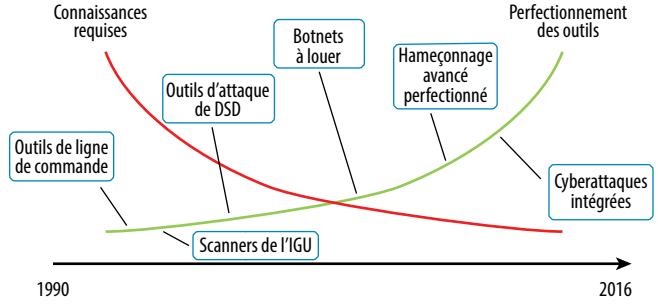
Causes et conséquences

Dans le monde réel, la criminalité à but lucratif est en général motivée par l'appât de gains bien supérieurs

ILLUSTRATION: ISTOCK / UGURHAN; VANREEEL

Un jeu d'enfant

Grâce à des outils perfectionnés, le piratage demande désormais moins de connaissances techniques et fait mouche bien plus souvent.



Source : université Carnegie Mellon.
Note : DSD = déni de service distribué ; IGU = interface graphique utilisateur ; botnet = réseau zombie.

aux bénéfices des entreprises légitimes, que les malfaiteurs considèrent comme justifiés par le surcroît de risque. Dans le monde du cybercrime, on peut encaisser à bien moindre risque des bénéfices équivalents, voire même supérieurs : il y a moins de danger de se faire prendre et poursuivre en justice et quasiment aucun risque de se faire tirer dessus. La profitabilité de l'hameçonnage est estimée à plusieurs centaines, voire plus de mille, points de pourcentage. Nul ne peut chiffrer avec exactitude les bénéfices engrangés par les plus habiles experts du vol de propriété intellectuelle. Les éléments de base sont pourtant les mêmes : l'efficacité des procédés et la perspective d'un rapport risque/bénéfice exceptionnel ont un attrait irrésistible, et c'est ce qui explique l'accroissement considérable et la professionnalisation de la cybercriminalité.

Le cybercrime constitue un risque systémique dans plusieurs domaines d'activité, différencié selon les secteurs, celui de la finance étant probablement le plus exposé. Les attaques à but destructif constituent une menace relativement récente. Les malfaiteurs qui cherchent à déstabiliser le système financier ciblent les proies les plus prometteuses. L'infrastructure du marché financier est particulièrement vulnérable à cause de son rôle crucial sur le marché mondial. Le secteur financier étant dépendant d'un nombre relativement petit de systèmes techniques, les retombées des défauts ou retards causés par les attaques victorieuses peuvent être considérables et avoir des effets systémiques.

Étant donné l'interconnection inhérente des acteurs du secteur financier, la déstabilisation des systèmes de paiement, de compensation ou de règlement (ou le vol d'informations confidentiels) aurait des répercussions considérables et menacerait la stabilité financière.

Heureusement, nous n'avons pas jusqu'à présent eu affaire à une cyberattaque suivie de conséquences systémiques. Cependant, les décideurs et les régulateurs financiers sont de plus en plus sur leurs gardes, au vu des récents incidents qui ont immobilisé des réseaux de guichets automatiques et des attaques dirigées contre les systèmes bancaires en ligne, les banques centrales et les systèmes de paiement.

Depuis des décennies, le secteur financier est tributaire des technologies de l'information et veille à s'entourer d'un solide arsenal de contrôles réglementaires. Il est peut-être sans doute le plus exposé aux cyberattaques, mais leurs auteurs courent aussi de grands risques du fait notamment de l'attention particulière des forces de l'ordre (comme à l'époque des braquages de banques d'antan). Le secteur financier coopère aussi de son mieux avec les services de police — notamment en tenant des registres très complets, qui sont un appoint précieux lors des investigations. Un surcroît d'investissement peut souvent renforcer l'efficacité de la cybersécurité. (Exception notable : Equifax, dont l'attaque était sans doute la conséquence d'un système réglementaire non proportionné aux risques.)

La situation est différente dans le secteur de la santé. Sauf dans les pays les plus riches, le secteur de la santé n'a pas en général les ressources requises pour se prémunir efficacement face aux cyberattaques. Cela ressort à l'évidence des attaques contre les systèmes de stockage électronique des dossiers de santé visant à rançonner la société Allscripts et deux hôpitaux régionaux aux États-Unis. Bien que très réglementé et soumis à des règles strictes de protection des données, le secteur de la santé n'a guère investi dans l'intelligence artificielle comparativement au secteur financier, dont il n'a pas acquis les réflexes de contrôle systématique. Le secteur de la santé est donc plus vulnérable aux cyberattaques. Cette lacune est particulièrement préoccupante, car à la différence du secteur financier, des vies humaines pourraient être en jeu si les attaques visaient les systèmes de survie électroniques.

Les services publics, en particulier les réseaux d'électricité et de communications, sont souvent cités au nombre des prochains secteurs où de vastes cyberattaques pourraient être lourdes de conséquences. Dans ce cas, cependant, la préoccupation majeure est l'interruption ou l'infiltration des systèmes par des États rivaux, soit directement, soit par des

La coopération internationale dans la lutte et les poursuites juridiques à l'encontre de la cybercriminalité est sans commune mesure avec la dimension mondiale du problème.

organisations commanditées. À l'instar du cas d'école que fut l'attaque massive montée en 2007 contre l'infrastructure de l'Internet en Estonie qui a déconnecté les institutions financières, les médias et les administrations publiques, plus l'économie est florissante et basée sur les transactions en ligne, plus les cyberattaques peuvent faire de dégâts. L'Estonie est l'une des sociétés les plus numérisées au monde (voir « L'E-stonie décolle » dans l'édition de mars 2018 de *F&D).*

Contre-mesures

Si le fonctionnement des infrastructures critiques, par exemple les réseaux d'électricité, de télécommunications et de transports, est perturbé, ou si, à la suite d'une attaque, les pouvoirs publics ne peuvent plus lever les impôts ou assurer les services essentiels, cela menace de causer de graves perturbations, lourdes de conséquences économiques et éventuellement des risques sanitaires ou sécuritaires. Dès lors, le total des risques pesant sur l'économie mondiale peut être supérieur à la somme des risques individuels, à cause de l'internationalisation des réseaux et plateformes informatiques, de la dimension nationale des structures de secours, du manque d'efficacité de la coopération internationale, voire même du fait que certains des attaquants sont des États-nations.

La coopération internationale dans la lutte et les poursuites juridiques à l'encontre de la cybercriminalité est sans commune mesure avec la dimension mondiale du problème. Le meilleur moyen de faire échec au cybercrime est de s'attaquer à son modèle opérationnel, fondé sur deux éléments : un énorme rapport risque/bénéfice et le manque total d'efficacité des poursuites. Cela étant, il faut rehausser significativement le risque commercial des cybercriminels, ce qui n'est possible qu'avec une meilleure coopération internationale.

Les attaques cybercriminelles peuvent viser plusieurs pays, et il est alors plus difficile de les stopper et de poursuivre leurs auteurs. Certains pays réagissent avec lenteur ou inefficacité, ou refusent de coopérer à la chasse au cybercrime. Une meilleure coopération permettrait de repérer et poursuivre les suspects plus rapidement et efficacement.

Les régulateurs du secteur financier ont défini des normes d'évaluation spécifiques, fixé des objectifs et des points de repère et encouragé le partage des informations et la collaboration entre les sociétés et avec les instances réglementaires. Celles-ci passent en revue les pratiques informatiques et mesures des entreprises pour vérifier l'état de préparation aux tests d'épreuve, de la planification stratégique et de l'intégrité et de la sécurité de leurs systèmes. Certaines instances réglementaires exigent des simulations de cyberattaques, pour évaluer la résilience des entreprises en cas d'attaque. Les sociétés financières ont aussi investi davantage dans la cybersécurité, qui est désormais un élément de leurs plans de gestion des risques. Certaines ont aussi contracté une cyberassurance pour amoindrir leurs risques.

La filière cybersécuritaire est actuellement disparate et décentralisée, et les risques sont traités pour l'essentiel comme des problèmes locaux spécifiques. Il y a bien quelques mécanismes de coopération et un surcroît d'efforts de la part des instances gouvernementales et réglementaires, mais les choix en matière de cybersécurité sont essentiellement dictés par les besoins de chaque entreprise — « chacun pour soi ». Il faut faire évoluer les mentalités pour affermir l'ensemble du système de lutte contre le cyberrisque. Il faut prendre de vigoureuses mesures défensives d'ordre réglementaire et technologique dans tous les secteurs. Il importe tout particulièrement de s'accorder sur des normes minimales de cybersécurité, qu'il incombe aux instances réglementaires d'appliquer de manière coordonnée. Le développement de formations de sensibilisation à la cybersécurité contribuera à déjouer les défauts techniques et les erreurs des usagers qui causent la plupart des défaillances.

Les cyberattaques et les défaillances de la cybersécurité semblent inévitables, et il faut donc aussi vérifier combien de temps il faut pour détecter l'attaque, si la riposte est efficace et combien de temps il faut pour rétablir la situation. FD

TAMAS GAIDOSCH, expert principal du secteur financier au département des marchés monétaires et de capitaux du FMI, est un professionnel de la cybersécurité ayant plus de vingt années d'expérience, notamment dans le domaine de l'évaluation des systèmes bancaires pour détecter les cyberrisques. Il était précédemment à la tête du département de la supervision des technologies de l'information à la banque centrale de Hongrie.