UQÀM
CHAIRE RAOUL-DANDURAND
EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS

©Bossier County Sheriff's Office

Cybersécurité et pandémie : les hackers étatiques exploitent la crise

par Danny Gagné

Alors que le monde est frappé de plein fouet par la pandémie de COVID-19, notre univers numérique a lui aussi été pris de court. Cet autre combat qui se joue dans l'ombre de la crise sanitaire pourrait cependant laisser de graves séquelles sur nos États déjà hors d'haleine.

Vous lirez sans doute ce texte depuis votre salon ou votre cuisine, et pour cause : le confinement nous force à faire à la maison ce qu'il y a peu de temps encore nous faisions ailleurs. Y compris, pour beaucoup, travailler. Qu'il s'agisse du secteur privé ou public, la COVID-19 a, en l'espace de quelques jours seulement, généré une augmentation exponentielle du nombre de télé-travailleurs à travers le monde industrialisé. Il n'en fallait pas plus pour voir une augmentation tout aussi fulgurante du nombre de cyberattaques ciblant des travailleurs isolés et dépendants en majorité de réseaux Wi-Fi personnels, véritables mines d'or pour les pirates de tout acabit.

Alors que l'on observe en effet une hausse dans l'utilisation des campagnes d'hameçonnage propageant des logiciels d'extorsion, ces activités criminelles s'accompagnent progressivement d'activités à caractère géopolitique : espionnage pur et dur, déstabilisation de pays adverses, quête désespérée d'informations sanitaires, etc. Certains États jouent des coudes pour tirer leur épingle du jeu au milieu de la pandémie. Qui fait quoi? Dans quel but? Trois dynamiques majeures agitent pour l'heure le cyberespace des sociétés confinées.

Frapper l'adversaire au tapis

En premier lieu, les mêmes activités étatiques malveillantes se poursuivent, mais dans un contexte de vulnérabilité accrue : utilisateurs avides d'informations sur la crise, services informatiques surchargés par l'explosion du télétravail, le contexte de pandémie a ouvert grand les portes aux pirates. Une situation qui offre, entre autres, un extraordinaire potentiel de cyberespionnage.

Depuis la fin février, plusieurs attaques recensées par la firme de cybersécurité FireEye ont ainsi été attribuées à la Chine. Cette dernière, via deux groupes de hackers déjà connus, profiterait de la crise pour nuire à des pays dans son collimateur depuis un certain temps déjà, pour des motifs politiques ou territoriaux : le Vietnam, les Philippines, la Mongolie et Taiwan. La Russie aurait, elle aussi, profité de la situation pour s'en prendre à diverses entités ukrainiennes, alors que la Corée du Nord aurait fait de même contre sa voisine du Sud.

Dans la plupart des cas, la stratégie employée misait directement sur le contexte de la pandémie : les hackers utilisaient par exemple des courriels imitant ceux des ministères de la Santé des pays respectifs pour communiquer des informations au sujet du coronavirus, afin d'installer des logiciels espions dans les postes de travail d'employés. La référence au coronavirus contribuait ainsi à rendre les cibles moins vigilantes, permettant alors de mettre la main sur diverses informations sensibles (mots de passe, documents, etc.) ou d'installer discrètement des *backdoors* sur certains ordinateurs, ces fonctionnalités qui donnent accès à l'appareil à l'insu de l'utilisateur. L'idée ne serait donc pas tant de nuire à ces pays durant la crise, mais plutôt de profiter de la crise actuelle pour préparer des actions futures.

Souffler sur les braises

En deuxième lieu, on observe également plusieurs cas d'actions étatiques malveillantes cherchant à exploiter l'anxiété des opinions publiques pour décrédibiliser des gouvernements adverses ou semer la panique dans certaines sociétés. En Ukraine, la Russie aurait par exemple utilisé le groupe de pirates prorusses Hades pour inonder les réseaux sociaux de messages alarmistes sur une soi-disant éclosion de COVID-19 dans le pays. Bien que l'offensive puisse sembler anodine, le *timing* lui ne l'était pas : la même journée, un avion chargé de rapatrier de Chine des citoyens ukrainiens était en route pour Kharkiv, dans l'est du pays.

Il n'en fallut pas plus pour pousser des Ukrainiens, exaspérés depuis longtemps par un système de santé sous-performant, à organiser des émeutes, certains allant jusqu'à saccager les autobus qui devaient accueillir les rapatriés. Un autre message fallacieux affirma par la suite que des employés de l'hôpital de Novi Sanzhary, où les citoyens rapatriés étaient en quarantaine, avaient fui les lieux et représentaient ainsi une menace sanitaire pour le pays. Un affrontement entre émeutiers et la garde nationale s'ensuivit devant l'hôpital en question.

Des incidents comparables, à l'issue toutefois moins violente, ont également pu être observés aux États-Unis. À la mi-mars, le département de la Santé et des Services sociaux (HHS), l'organe gouvernemental responsable de répondre à la crise, a été la cible d'attaques de type DDoS (Distributed Denial Of Service) à plusieurs reprises (ce type d'attaque vise à compromettre l'accès à des systèmes informatiques ou à un site Internet). Si le secrétaire du HHS, Alex Azar, a affirmé que les systèmes de télétravail n'avaient pas été compromis et que le site de l'agence avait

pu continuer à fonctionner, celui-ci a néanmoins accusé un ralentissement considérable. Au même moment, le 16 mars, un ensemble de comptes Twitter automatisés (*bots*) disséminait une fausse nouvelle affirmant que le président Trump s'apprêtait à mettre le pays en quarantaine forcée pour deux semaines.

Les membres du Conseil de sécurité nationale de la Maison-Blanche ont par la suite déclaré qu'ils voyaient un lien direct entre la fausse nouvelle et les attaques contre le HHS, et que l'objectif de la démarche était de ralentir l'aide du gouvernement pour semer la panique dans la population. Bien que les autorités américaines croient que l'attaque a été parrainée par un État concurrent, elles n'ont pour l'heure pas identifié de coupables. Cette stratégie n'est pas sans rappeler un précédent similaire : plusieurs médias français avaient été la cible de cyberattaques de type DDoS dans la foulée des attaques terroristes de Paris en 2015.

L'OMS cible des convoitises

Enfin, une troisième vague d'actions étatiques observées depuis le début de la pandémie révèle un constat alarmant : faute d'un élan unanime et inconditionnel de coopération internationale pour faire face à la COVID-19, plusieurs pays semblent chercher désespérément à mettre la main sur des informations permettant de mieux gérer la pandémie sur leur territoire.

Le 2 avril dernier, l'OMS accusait par exemple l'Iran d'avoir mené une cyberattaque contre ses infrastructures informatiques. L'attaque, évidemment démentie par Téhéran, aurait consisté en une série d'envois de courriels d'hameçonnage visant à s'introduire dans les postes de travail d'employés de l'organisation. La République islamique, durement touchée par la pandémie, serait (selon une source anonyme proche du renseignement américain) à la recherche d'informations « inoffensives », mais difficiles à obtenir ouvertement : les plans d'intervention d'autres pays aux prises avec la COVID-19, le détail de traitements médicaux à l'étude, ou encore les estimations du rythme de propagation de l'infection.

Même stratégie, autre pays : en mars, le groupe de pirates DarkHotel, soupçonné d'être à la solde du gouvernement sud-coréen, a lui aussi été pointé du doigt pour une cyberattaque contre l'OMS. Plus inquiétant toutefois, selon l'agence de sécurité cybernétique chinoise Qihoo 360, DarkHotel chercherait aussi à identifier les lignes d'approvisionnement de matériel médical en provenance de la Chine, tel que les masques, les tests de dépistage et autres équipements essentiels. Reste à voir si les pirates informatiques vont ouvrir la porte à de véritables corsaires qui chercheraient par exemple à intercepter de tels chargements. Un constat demeure : les hackers s'adonnent eux aussi au télétravail, dans un contexte qui leur apparaît hautement favorable.

Loin des yeux, loin du cœur

Il est impossible de prévoir combien de temps va encore durer la crise provoquée par l'actuelle pandémie ni comment nous allons nous en sortir collectivement. Alors que nous sommes devant le triste constat de notre impréparation matérielle face à un défi de cette taille, ce qui se passe sur le web, loin des yeux du public, est également alarmant. Nous sommes actuellement fortement préoccupés (avec raison!) par les décès causés par la COVID-19, mais les exemples cités plus haut montrent que la pandémie représente également un défi pour nos infrastructures numériques. Si certains voyaient la planète comme un village global où la mobilité humaine devait transcender les frontières, l'idée que nous pourrions éventuellement être confinés pendant une si longue durée n'avait simplement pas été envisagée. Du point de vue de la cybersécurité, les mieux préparés à cette crise sont malheureusement les mêmes qui profitaient déjà des vulnérabilités de nos sociétés avant la pandémie.

Danny Gagné est chercheur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux:

https://dandurand.uqam.ca/