21 mai 2020
Menaces en ligne

Covid 19 : Comment les pirates informatiques exploitent férocement la déstabilisation des États, des entreprises... et des particuliers

En ces temps de Covid-19, et à l'image de l'attaque informatique sur les données de la compagnie Easy-Jet, le cyberespace est de plus en plus instable. États, entreprises et particuliers semblent promis à une période de très forte instabilité sur la toile mondiale.

Avec Franck DeCloquement

Atlantico : Que s'est-il passé au juste avec EasyJet ?

Franck DeCloquement : EasyJet a été victime d'une cyberattaque très sophistiquée comme l'a expliqué la compagnie aérienne britannique, dans un communiqué mardi dernier, sans toutefois préciser quand la cyberattaque a eu lieu… Alors le transporteur aérien est déjà fragilisé comme beaucoup d'autres par les conséquences économiques de la pandémie actuelle de Covid-19, des pirates informatiques de haut vol ont eu accès aux données personnelles de 9 millions de clients d'EasyJet, dont 320 de nos compatriotes apprend-on.

Les attaquants ont ainsi obtenu des adresses mails et le détail de leurs voyages. Mais également – et dans un faible nombre de cas – les données personnelles des cartes de crédit des passagers : soit 2.208 victimes au total. Easyjet affirme que tous les clients concernés seront contactés d'ici le 26 mai au plus tard, et que ceux dont les données bancaires ont été compromises l'ont déjà été.

Le transporteur précise qu'il a réussi à enrayer l'accès non autorisé à son système informatique, et assure sa clientèle qu'il n'y a pas d'indices laissant à penser que les données dérobées ont été utilisées « à des fins illégitimes ». Ce dont on peut très fortement douter… Pour autant, le groupe a immédiatement alerté le National Cyber Security Centre (NCSC), ainsi que le régulateur britannique de la protection des données (ICO)…

Atlantico : Dans quel contexte spécial cette attaque s'est-elle produite ? Et dans quelle mesure les effets économiques délétères du Covid-19 amplifient-ils encore l'occurrence de ce type d'action offensive ?

Franck DeCloquement : En situation de pandémie mondiale, le contexte international actuel est particulièrement troublé et sujet à de nombreuses formes de conflictualités exacerbées et de déstabilisations pernicieuses. Tant sur le plan cyber, que sur le plan politique ou sociétal. Le monde de l'air est donc pour le moins entrée en zone de turbulences comme le démontre sans ambages l'affaire EasyJet… Une attaque informatique de cette ampleur reste assez peu courante au Royaume-Uni, et cela même si des entreprises britanniques – tous secteurs confondus – sont régulièrement ciblées par les pirates. On se souviendra pour mémoire que la concurrente d'EasyJet, la compagnie aérienne British Airways, avait aussi été touchée par une cyberattaque à l'été 2018, suite à une importante faille informatique. Le tout s'étant soldé avec un vol de données financières affectant près de 400.000 clients en pleine

saison estivale. A l'issue, British Airways avait écopé d'une amende record de 183 millions de livres auprès de l'ICO qui avait estimé que le transporteur disposait de systèmes de sécurité informatiques défaillants…

Anticipant une hausse notable du nombre de cyberattaques en provenance « d'intelligences malveillantes » voulant profiter des effets déstabilisateurs de la pandémie actuelle pour agir, le géant britannique des télécoms Vodafone avait de son côté indiqué, la semaine dernière, avoir renforcé drastiquement son dispositif de sécurité informatique. Cette intuition s'est révélée être particulièrement fondée : « depuis que nous avons pris conscience de l'incident, nous avons compris qu'en raison du Covid-19 il y a de fortes craintes sur l'utilisation de données personnelles pour des arnaques en ligne », a déclaré dans la foulée Johan Lundgren, directeur général du groupe EasyJet.

C'est pour cette même raison que le transporteur recommande depuis très vivement à ses clients « d'être très vigilants, en particulier s'ils reçoivent des demandes non sollicitées ». C'est en effet le minimum légal, en tout état de cause… Pour tous ceux qui pourraient être impliqués, il est naturellement vital de procéder au changement immédiat de leurs mots de passe auprès d'EasyJet, mais également d'agir de même sur les autres plateformes commerciales en ligne ou sites internet, si d'aventure les mots de passe utilisés étaient identiques. Il est aussi primordial de garder un œil rivé sur ses relevés bancaires, afin de détecter précocement toute anomalie de dépenses indues sur ses comptes...

Atlantico : Le monde d'après Covid sera donc celui de la cyber-déstabilisation ? Mais pourrait-il être aussi celui des influences délétères, et des déstabilisations sociétales tous azimuts ?

Franck DeCloquement :C'est en effet très probable : cette cyberattaque est d'ailleurs dévoilée avant une assemblée générale des actionnaires d'EasyJet prévue vendredi 22 mai, qui doit se prononcer en outre sur l'éviction de l'équipe dirigeante... Ces résolutions sont portées par le fondateur et premier actionnaire d'EasyJet, Stelios Haji-Ioannou. Celui-ci fustige en effet la décision de la compagnie aérienne de conserver des commandes en cours de plus de 100 avions auprès d'Airbus en pleine crise mondiale du coronavirus. EasyJet presse de son côté l'ensemble de ses actionnaires de voter contre les propositions de Haji-Ioannou qui déstabiliseraient un peu plus la compagnie à un moment particulièrement délicat pour elle. On le voit, l'affaire est très sérieuse pour EasyJet et potentiellement explosive pour l'entreprise…

Rappelons que dans son rapport annuel publié en avril 2019, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) met en garde les entreprises contre les opérations de déstabilisation et d'influences pernicieuses, qui représenteraient aujourd'hui l'une des cinq menaces majeures pour les entreprises, avec les « attaques indirectes » ou « par rebond », le « cryptojacking », les fraudes en ligne et le cyber-espionnage.

Mais qu'entend-on au juste par « opération de déstabilisation et d'influence » ? Ces opérations ont été particulièrement nombreuses ces 5 dernières années, note l'ANSSI. Ces attaques, généralement peu sophistiquées, visent prioritairement à déstabiliser symboliquement des entreprises en nuisant à leurs activités, la paix sociale en interne ou l'image de leurs dirigeants. Les conséquences concrètes de ces opérations peuvent aller de la simple indisponibilité du service impacté au sabotage complet, mais aussi à la diffusion massive par des robots de « fake news ». Autrement dit, d'informations contrefaites : les fameuses « infox » ! Ces dernières représentent en effet plus de 50% du trafic sur internet, et les « mauvais bots » sont désormais légions. Au-delà de leur impact sur les systèmes informatiques, ces opérations sont susceptibles d'engendrer de graves conséquences pour les entreprises : atteintes à la réputation, fragilisation des systèmes informatiques, perte de confiance des clients et des partenaires financiers, et baisse consécutive du chiffre d'affaires… Si certains secteurs sont traditionnellement visés par des cyberattaques, les opérations de déstabilisation massives et d'influence délétère, à l'image des secteurs de la santé, de la défense ou de l'énergie, toute organisation publique ou privée est exposée au risque informatique. Ainsi, en début d'année, 92% d'entreprises déclaraient avoir été victimes d'une ou plusieurs attaques informatiques.

Concernant l'aspect « sociétal » des opérations de déstabilisation, je ne peux que renvoyer à l'excellent texte de Nicolas Zubinski disponible sur le site infoguerre.fr : « **le concept de guerre sociétale : mutation des political & information warfares**». L'article décrit en outre les leviers contemporains de re-modélisation et de déstabilisation sociétale induits par les opérations de guerre de l'information et de guerre politique. Paraphrasant ici Zubinski : « les mécanismes décrits reposent en grande partie sur les méthodologies mises en œuvre, d'une part, pour des opérations militaires d'influence et, d'autre part, pour des opérations de désinformation ayant ciblé les systèmes électoraux ces dernières années ». Nicolas Zubinski y dépeint des mécanismes propres aux « opérations psychologiques », aux « actions numériques », au « ciblage psycho-cognitif » et « socio-économique » des individus, ainsi que des méthodes de « délégitimation des institutions » et de « radicalisation des acteurs ». En mettant en perspective ces vecteurs de déstabilisation avec les doctrines russes et américaines de l'influence, civile ou militaire, l'analyse de Zubinski conclut à l'existence d'un nouveau type de conflictualité de basse intensité : « la guerre sociétale ». Selon lui, la spécificité de la guerre sociétale ne réside pas dans les moyens mobilisés, mais davantage dans les mécanismes des conflictualités utilisées pour et par la déstabilisation de l'échiquier sociétal.

In fine, la guerre sociétale se démarque par une conflictualité diffuse et subversive, à la temporalité singulière, et relève davantage de l'approche sociologique. Ce faisant, les approches classiques du renseignement et de la contre-ingérence ne parviennent qu'imparfaitement à déceler le potentiel déstabilisateur de ce type d'attaque. La nature des mécanismes de modélisation sociétale s'inscrit davantage dans la lignée des relations publiques (RP), de la communication stratégique et du « market shaping ». À ce titre, les opérations militaires contemporaines gagneraient fortement à intégrer davantage cet héritage de la sphère civile.

Ainsi, la « guerre sociétale » risque fort d'être un mode de conflictualité de plus en plus sollicité et usité, que cela soit par des services clandestins, des groupuscules politiques, des communautés radicalisées ou des entreprises en conquête de nouveaux marchés. Pour prémunir la société civile d'une altération manipulée de son pacte social, il est nécessaire de procéder à l'édification d'une résilience informationnelle à l'échelle sociétale. La crise actuelle du Covid-19 nous le démontre tous les jours s'il était besoin…

Le texte de Zubinski propose dans sa dernière partie les recommandations d'usage très intéressantes : un renforcement particulier de la spécialité « influence » dans l'écosystème français du renseignement et de la contre-ingérence, une adaptation de l'éducation

civique aux nouveaux enjeux de citoyenneté, et un développement des capacités de résilience sociétale des entreprises.

En somme, le bon sens en action en période trouble.