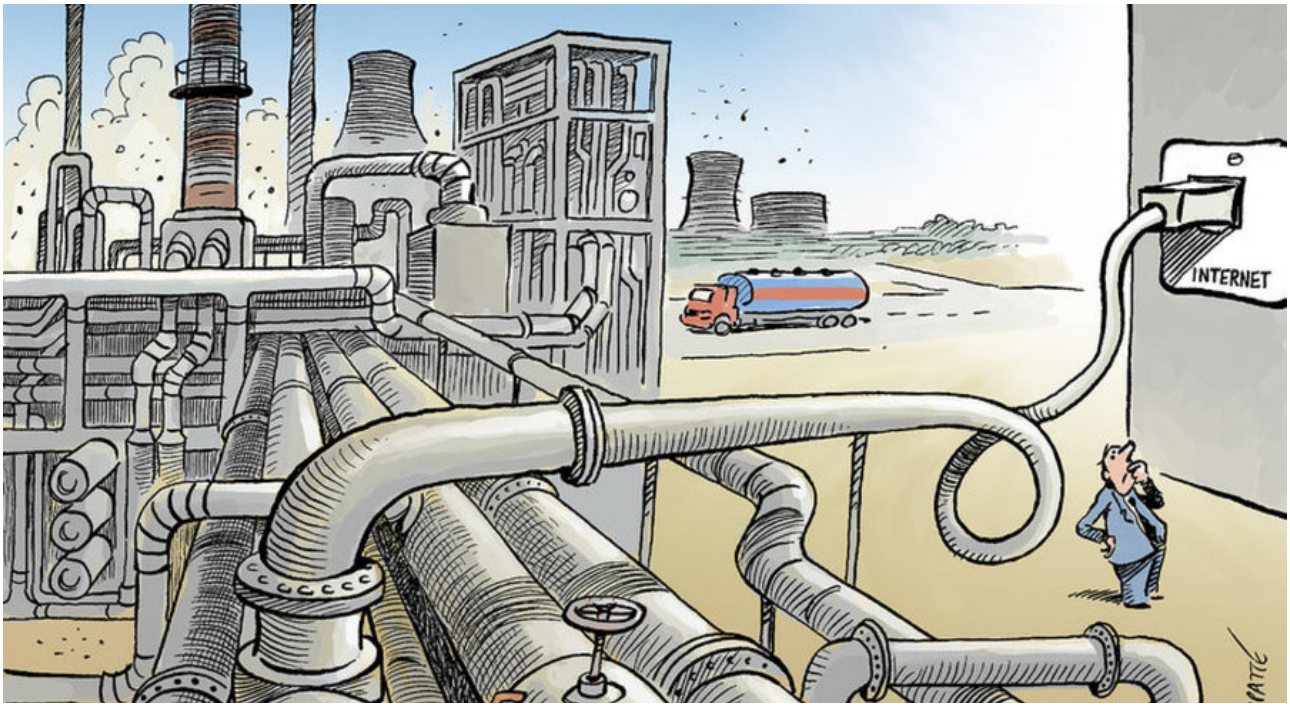
LE TEMPS

SÉCURITÉ

Du Texas à Genève, les «ransomwares» frappent. Et surtout, les victimes payent les rançons

Colonial Pipeline aurait payé une rançon de 5 millions de dollars pour reprendre le contrôle de son oléoduc, piraté par les hackers du groupe DarkSide. En Suisse aussi, des entreprises paient pour récupérer leurs données. Témoignage



Dessin de Patrick Chappatte. — © Chappatte

Anouch Seydtaghia
Publié samedi 15 mai 2021 à 07:55
Modifié samedi 15 mai 2021 à 12:29

Au téléphone, Steven Meyer est un peu stressé. Ce vendredi matin, le spécialiste en cybersécurité se trouve chez une entreprise en très mauvaise posture. «C'est un établissement financier basé à Genève. Il s'est fait attaquer par des pirates informatiques. Et nous nous préparons à leur payer une rançon», détaille le directeur de la société genevoise ZENdata, active dans la sécurité informatique. Cette entreprise active dans la Cité de Calvin va donc verser de l'argent à des hackers. Comme l'entreprise américaine Colonial Pipeline, qui aurait payé cette semaine 5 millions de dollars à des pirates pour reprendre le contrôle de son oléoduc. Deux exemples, aux Etats-Unis et en Suisse, qui démontrent la puissance et l'efficacité de ces criminels d'un nouveau genre.

Au niveau mondial, ce sont les révélations faites dans la nuit de jeudi à vendredi aux Etats-Unis qui ont l'effet d'un choc. Car jamais un acteur de l'importance de Colonial Pipeline – qui transporte près de 45% des carburants consommés sur la côte Est des Etats-Unis – n'avait, de manière quasi officielle, payé une rançon. Citant plusieurs sources, CNN, Bloomberg et le *New York Times* ont affirmé que la société, dont l'oléoduc va du Texas à New York, a obtempéré face à cette tentative d'extorsion. Interrogé à ce sujet, le président américain, Joe Biden, n'a pas voulu faire de commentaire.

Notre éditorial: L'extorsion numérique, cette activité si ordinaire

Ne pas payer, mais…

L'objectif de Colonial Pipeline semble avoir été de restaurer ses activités le plus rapidement possible, et à n'importe quel prix. Selon les médias américains, une fois qu'ils ont reçu le paiement, les pirates ont fourni à la société un outil de décryptage pour restaurer son réseau informatique désactivé. Cette semaine, le FBI a répété qu'il ne fallait pas payer de rançon aux hackers, pour ne pas les inciter à étendre leurs activités. Mais Anne Neuberger, principale responsable de la cybersécurité à la Maison-Blanche, a été plus nuancée: «Nous reconnaissons cependant que les entreprises sont souvent dans une position difficile si leurs données sont cryptées et qu'elles n'ont pas de sauvegardes et ne peuvent pas les récupérer», a-t-elle déclaré lundi.

Les pirates de DarkSide – ou leurs sous-traitants –, suspectés par Washington d'être proches de Moscou, ont donc réussi leur coup. Ils ont montré qu'ils étaient des criminels fiables, en déverrouillant l'accès aux ordinateurs après versement de la rançon. «Le paiement des rançons renforce les hackers, poursuit Steven Meyer. Cela valide le fait que leur approche est bonne. Et cela leur fournit des fonds pour faire de la recherche et du développement et recruter des talents.» Comme une entreprise classique, en somme.

Rançon réduite

Revenons à Genève. Pourquoi cette entreprise accepte-t-elle de verser une rançon? «C'est un calcul assez simple à faire, affirme le spécialiste en cybersécurité. L'établissement financier a estimé que payer une rançon serait plus rapide et beaucoup moins coûteux que d'accepter la perte de données, car le pirate a réussi à détruire les sauvegardes. C'est regrettable, mais c'est ainsi: il est souvent plus rationnel de payer.» Au départ, les hackers exigeaient 50 000 francs de leur victime genevoise. Après négociation, le prix est tombé à 15 000 francs.

Comment être sûr que les pirates tiendront parole et libéreront les ordinateurs? «Ils nous ont prouvé leur «bonne foi» en nous redonnant, pour l'exemple, l'accès à deux fichiers, répond Steven Meyer. Les hackers ont tout intérêt à se montrer fiables s'ils veulent recevoir l'argent.»

Plusieurs cas en Suisse

La transaction s'effectuera en cryptomonnaie, un moyen, pour le destinataire de la somme, de rester anonyme. «Cette entreprise n'est de loin pas un cas isolé. Ces derniers mois, plusieurs entreprises suisses nous ont contactés après que leurs systèmes ont été paralysés par des *ransomwares.* Et dans certains cas, les sociétés ont choisi de payer, parfois des montants plus importants, de plusieurs dizaines de milliers de francs», poursuit Steven Meyer.

Dans son dernier rapport paru le 10 mai, le Centre national pour la cybersécurité (NCSC) citait plusieurs entreprises suisses frappées par des *ransomwares:* Swatch Group, le constructeur d'hélicoptères Kopter, l'entreprise électrique Huber+Suhner et le groupe médical Hirslanden. «Comme pour presque toutes les cyberattaques, les attaques par *ransomware* se produisent par vagues. De manière générale, on peut dire que les cyberattaques accompagnées de demandes d'extorsion, y compris les attaques par *ransomware*, ont augmenté ces dernières années», note un porte-parole du NCSC, contacté par *Le Temps*.

Lire aussi: DarkSide, la PME du «ransomware» qui soigne son image

Porter plainte

Le NCSC donne par ailleurs des conseils. «Nous déconseillons vivement de payer une rançon, poursuit le porte-parole. Il n'y a aucune garantie que les données puissent être récupérées une fois que la rançon a été payée. Cependant, il existe des entreprises qui se plient aux demandes de rançon. Le NCSC ne dispose pas de chiffres concrets.». Le responsable ajoute que les victimes doivent impérativement déposer une plainte pénale auprès de la police cantonale.

Stéphane Duguin, directeur du CyberPeace Institute, basé à Genève, estime que «le paiement des rançons est au cœur du modèle criminel. Les gangs sont motivés par le gain et toutes les cibles sont bonnes.» Est-ce qu'un paiement spécifique va entraîner une multiplication? «Difficile à dire, répond-il. La convergence des réactions peut même avoir l'effet inverse: le gouvernement américain a réagi avec un Executive Order afin de s'attaquer aux problématiques systémiques de cybersécurité aux Etats-Unis. Mais, plus largement, la multiplication des extorsions à succès participe à la flambée du *ransomware*.»

Tendance à la hausse

Au niveau mondial, il semble que de plus en plus de cibles de hackers acceptent de payer une rançon. Selon une étude parue en 2020 et réalisée par la société de cybersécurité californienne Barracuda, 15% des services municipaux visés aux Etats-Unis les mois précédents avaient accepté de payer des sommes allant de 45 000 à 250 000 dollars. Pour tenter de s'en prémunir, il faut donc accroître, sans cesse, le niveau de protection des systèmes informatiques.