La cybercriminalité à l'heure de la Covid-19

Myriam QUEMENER
Magistrat
Docteur en droit

La crise de la Covid-19 a réactivé le fléau des cyberattaques qui se développe et qui profite du contexte anxiogène actuel, les cyberdélinquants jouant souvent sur la peur auprès des internautes. Le constat d'une explosion des attaques et d'une diversification de la menace d'origine cyber est partagé par l'ensemble des observateurs et des acteurs de la sécurité informatique. La digitalisation des activités humaines associées à des nouveaux usages numériques mal maîtrisés[1] conduit inévitablement à une explosion du phénomène qui implique une stratégie renouvelée en particulier au niveau de tous les pouvoirs publics. En outre, les nouveaux usages du numérique instaurent une véritable disruption[2] tant au niveau juridique que sociétal et organisationnel.

Les attaques informatiques par rançongiciels contre les entreprises sont devenues la méthode privilégiée par les cybercriminels, permettant de récupérer des sommes importantes et de faire de l'espionnage économique. Comme le souligne un récent rapport sénatorial[3], la cybercriminalité apparaît comme une menace en hausse notamment en raison de la numérisation croissante de la société.

Ce phénomène vise toutes les organisations y compris des hôpitaux par centaine comme aux Etats–Unis avec les établissements de la chaîne américaine Universal Health Services (UHS), groupe privé qui compte 400 établissements. Récemment, en Allemagne, une patiente est décédée, faute d'avoir pu être prise en charge. En France aussi, des attaques ont eu lieu. La plus grave contre le CHU de Rouen à la fin de l'année dernière, qui avait provoqué de grosses perturbations.

Toutes les entreprises peuvent en être victimes, comme par exemple Orange Business Services, M6, Fleury-Michon, Bouygues Construction, Eurofins, Altran mais également des hôpitaux, des ministères, des cabinets d'avocats et des collectivités territoriales. Les attaques par rançongiciels augmentent en nombre, en fréquence et en sophistication. Dernièrement, le groupe CMA CGM[4], quatrième armateur mondial dans le transport maritime, a annoncé sur Twitter être victime d'une cyberattaque sur ses serveurs périphériques. Depuis le début de l'année, l'Agence nationale de la sécurité des systèmes d'information a traité 104 attaques par rançongiciels : « Leurs conséquences sont de plus en plus dévastatrices, sur la continuité d'activité, voire la survie de l'organisation victime », note l'ANSSI.

---

[1] M. Quéméner, C. Wierre, F. Dalle, Quels droits face aux innovations numériques ? : Lextenso 2020.
[2] M. Quéméner, le droit face à la disruption numérique , Lextenso Gualino 2018

3 Sénat, S. Joissains et J. Bigot, « Cybercriminalité : un défi à relever aux niveaux national et européen », fait au nom de la commission des affaires européennes et de la commission des lois : rapp. info. n° 613 (2019-2020) 9 juill. 2020
4 https://www.usine-digitale.fr/article/cma-cgm-victime-d-une-cyberattaque-l-acces-a-ses-applications-informatiques-est-indisponible.N1010124

Rappelons qu'un rançongiciel[5] est un logiciel informatique malveillant qui chiffre les fichiers contenus sur les ordinateurs et demande une rançon.

L'analyse du rançongiciel permet de comprendre que la pièce jointe n'était qu'un fichier contenant en son sein des instructions permettant le téléchargement de la charge virale sur l'ordinateur de la victime, et ce, à l'insu de celle-ci, à partir d'un site distant dit « site de distribution ». Ces sites de distribution s'avéraient être des serveurs internes compromis, bien souvent à l'insu de leurs propriétaires, qui n'ont généralement pas réalisé la mise à jour des logiciels de leurs systèmes.

Les réponses juridiques

Les attaques par rançongiciel peuvent ainsi être poursuivies sur la base des atteintes aux systèmes de traitement automatisé de données (STAD). Les escroqueries au faux ordre de virement peuvent aussi être poursuivies au titre des atteintes au STAD.

Ces cyberattaques peuvent aussi être qualifiées d'extorsion simple ou en bande organisée sur le fondement des articles 312-1 et 312-6-1 du Code pénal. Les articles 313-1 à 313-3 du Code pénal, qui sanctionnent l'escroquerie, simple ou en bande organisée, peuvent être utilisés pour réprimer les escroqueries à la fausse amitié ou à la romance, les escroqueries à l'investissement en ligne, au faux site de vente en ligne ou encore l'arnaque au faux site administratif.

La justice se mobilise face à ce fléau depuis l'entrée en vigueur de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, l'article 706-72-1 du Code de procédure pénale confie au procureur de la République, au pôle de l'instruction, au tribunal correctionnel et à la cour d'assises de Paris une compétence concurrente nationale en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et d'atteintes aux intérêts fondamentaux de la Nation ce qui peut couvrir des hypothèses de cyber-sabotage.

Au sein du parquet, cette compétence est confiée à la section J3, anciennement dénommée section F1, ou section cybercriminalité. Au titre de sa compétence nationale, la section J3 peut se saisir des affaires de cybercriminalité complexes, où qu'elles se produisent sur le territoire, les parquets locaux demeurant compétents pour le reste du contentieux. Elle est seule compétente pour les infractions commises dans le ressort du parquet de Paris. En 2020, la section J3 a ouvert 249 enquêtes sur le fondement de cette compétence nationale, dont 225 sont toujours en cours.

Plusieurs affaires prospèrent et aboutissent comme en témoigne par exemple l'interpellation d'un russe, Alexander Vinnik[6], soupçonné d'être le créateur du rançongiciel Locky et administrateur d'une plateforme facilitant le blanchiment de fonds et qui va être jugé en France. Ce logiciel malveillant rend illisibles les fichiers qu'il attaque Arrêté pendant ses vacances en Grèce en juillet 2017, il a été remis aux autorités judiciaires françaises en janvier 2020. Il est poursuivi pour extorsion et blanchiment d'argent. Placé en détention préventive, il est soupçonné d'avoir orchestré les malversations de BTC-e, la plateforme d'échanges de bitcoins fondée en 2011 et devenue l'une des plus importantes au monde mais accusée d'extorsions en ligne et d'autres activités de cybercriminalité. Les services saisis de l'enquête ont recensé plus d'une centaine de victimes de Locky.

Le site de paiement vers lequel étaient redirigées les victimes correspondait à un site internet « onion », c'est-à-dire accessible uniquement par l'intermédiaire d'une connexion au réseau d'anonymisation TOR dont la particularité est de masquer l'adresse IP du serveur par une série de « serveurs passerelles ». En outre, à la différence de nom de domaine classique (.fr ou .eu), les noms de domaine en .onion ne sont enregistrés

5 ou ramsomwarel en anglais.

6 https://www.zdnet.fr/actualites/le-russe-alexander-vinnik-extrade-en-france-39898105.htm

auprès d'aucune autorité avec une déclaration d'identité mais simplement créé automatiquement par le logiciel. Les investigations ont permis d'établir que le site de paiement indiqué aux victimes proposait en échange du paiement de la rançon en bitcoin, un logiciel nommé « Locky Decryptor » permettant le déchiffrement des fichiers des victimes. Une aide était même proposée à ces dernières pour leur permettre d'obtenir des bitcoins afin de payer leur rançon. Cette procédure est un exemple qui a nécessité de mettre en œuvre de nombreuses investigations à l'international complexes.

Comment renforcer la lutte contre les attaques numériques ?

Les institutionnels conseillent dans les affaires de rançongiciels de ne pas payer la rançon et de déposer plainte et ce d'autant que les cybervictimes risquent de ne récupérer ni la totalité ni même une partie des fichiers chiffrés et cela peut favoriser la promotion de ces activités cybercriminelles. Carlson WagonLit Travel (CWT), spécialiste des voyages d'affaire, victime de Ragnar Locker, aurait payé 4,5 millions de dollars pour remettre en route les 30 000 PC paralysés. Au départ, le gang réclamait 10 millions de dollars et c'est le directeur financier de CWT en personne qui a assuré la négociation. Plaidant les difficultés de l'entreprise liées à la crise sanitaire, il a réussi à réduire le montant de la rançon.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié le 4 septembre 2020, en partenariat avec le ministère de la Justice et la DACG, un guide de sensibilisation destiné aux entreprises, collectivités et administrations. Le document propose des mesures préventives issues du guide d'hygiène informatique de l'ANSSI qui permettent d'éviter qu'un rançongiciel n'atteigne l'organisation ou, a minima, de réduire les pertes liées à une telle attaque. Il conseille notamment d'utiliser et de maintenir à jour les logiciels antivirus, de cloisonner le système d'information, de limiter les droits des utilisateurs et autorisations des applications, de sensibiliser les collaborateurs, d'évaluer l'opportunité de souscrire à une assurance cyber, de définir une stratégie de communication de crise cyber. En réunissant témoignages de victimes et bonnes pratiques de sécurité numérique, ce guide sensibilise les différents acteurs économiques aux rançongiciels et invite les organisations - du comité exécutif aux collaborateurs - à se saisir de ces questions.

Suite à l'explosion de ce fléau bien soulignée par de nombreux rapports ministériels[7] parlementaires[8] et du secteur privé[9], il est indispensable de mettre en œuvre les recommandations phares relatives notamment à la sensibilisation des citoyens, au renforcement des moyens humains et de la coopération internationale.

En outre, plusieurs rapports du Sénat tirent la sonnette d'alarme de façon accélérée depuis quelque temps sur l'ampleur que prend la menace cyber[10]. L'un de ces documents, d'ailleurs souligne l'impréparation de certaines administrations face aux cyberattaques qui nécessitent la mise en place d'un pilotage de la gestion de crise[11].

Si tous les acteurs sont concernés par cette lutte, il faut souligner que les ministères régaliens le sont en première ligne, ministère de l'Intérieur et de la Justice. À cet égard, l'institution judiciaire est de plus en plus saisie par des procédures relatives à la cybercriminalité, la délinquance glissant nettement vers les usages numériques, notamment en matière

---

7 L'état de la menace liée au numérique en 2019 : www.interieur.gouv.fr. - Protéger les internautes, rapp. sur la cybercriminalité, 2014 : www.justice.gouv.fr.

8 O. Cadic et R. Mazuir, Suivi de la cybermenace pendant la crise sanitaire : rapp. d'info. n° 502 (2019-2020), 10 juin 2020, fait au nom de la commission des affaires étrangères, de la défense et des forces armées : www.senat.fr.

9 Le rapport Risk Solutions souligne la taille, l'échelle et l'exposition monétaire des réseaux mondiaux de cybercriminalité : LexisNexis, https://risk.lexisnexis.com/global/fr/about-us/press-room/press-release/20200304-cybercrime-report.

10 J. Bascher, La sécurité informatique des pouvoirs publics : rapp. d'info. n° 82 (2019-2020), 22 oct. 2019, fait au nom de la commission des finances : www.senat.fr

11 ANNSI, État de la menace rançongiciel à l'encontre des entreprises et institutions, 5 févr. 2020 : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

économique et financière[12] où les préjudices sont souvent colossaux. Une campagne nationale de sensibilisation aurait à cet égard actuellement tout son sens.

S'il apparaît nécessaire d'augmenter les moyens du parquet spécialisé ainsi que le souligne le rapport pour être porté au niveau de ceux des grands États européens les plus engagés dans ce domaine, cette remarque vaut également pour les magistrats du siège. Si la spécialisation est nécessaire, elle ne doit pas être poussée à l'excès, compte tenu du caractère transversal du numérique. Il est important également que l'ensemble de la chaîne pénale, (siège et parquet) soit véritablement au fait de ce fléau et comprenne parfaitement les modes opératoires souvent complexes et évolutifs. Il est clair désormais que la lutte contre la cybercriminalité implique en outre un renforcement de la coopération public/privé et internationale.

En septembre 2020, la France, la Lituanie et la Lettonie ont proposé à l'UE un plan pour protéger les élections en Europe contre les cyberattaques et la désinformation, ont annoncé en septembre 2020 les présidents français et lituanien d'une conférence de presse.

12 M. Quéméner, criminalité économique et financière à l'ère numérique, Economica 2015