Hausse des attaques informatiques en période de crise sanitaire

Fiche pratique publié le **22/02/2021**, vu **1470 fois**, Auteur : La zone du droit

Les infractions servant de base légale à la répression de la cybercriminalité ont toutes pour point commun d'utiliser les systèmes et réseaux numériques.

Le coronavirus réduit de plus en plus nos libertés fondamentales et individuelles. Le virus n'en finit plus de faire des victimes et le nombre de décès par jour fait partie du quotidien des populations à telle enseigne qu'elles n'accordent plus d'importance à ces chiffres désolants. Pour rappel, la France a franchi le cap des 80.000 morts le 10 Février 2021.

Depuis le début de cette crise, tous les gouvernements du monde entier ont pris des mesures pour faire face à cette avancée incontrôlable. Ces mesures prises sont drastiques à tel point qu'elles touchent presque tous nos droits fondamentaux et individuels.

C'est le cas de la libre circulation entre les Etats Européens, qui, autrefois constituait un droit pour les populations Européennes, est remise en cause aujourd'hui car considérée par les autorités gouvernementales comme favorisant la circulation du virus entre les Etats. Le port obligatoire du masque est plus que jamais devenu la norme dans tous les Etats par crainte de se faire infliger une contravention pour non-respect des mesures barrières.

Cette situation a par ailleurs, élevé au premier rang les nouvelles technologies qui prennent une place désormais indiscutable au sein de la société. Le numérique est devenu le premier centre d'intérêt dans cette crise tant pour continuer l'activité économique que pour lutter contre ce virus. A titre d'exemple, le télétravail a franchi un seuil considérable dans cette crise. Et qui dit télétravail, dit installation de tout un système informatique chez soi.

Ainsi, la fraude informatique est-elle une préoccupation majeure que connaissent tant les particuliers, les administrations, que les entreprises. Elle s'attaque à des victimes extrêmement variées, par des moyens différents et provoque de graves préjudices.

Les infractions servant de base légale à la répression de la cybercriminalité ont toutes pour point commun d'utiliser les systèmes et réseaux numériques tantôt en tant qu'objets de l'infraction, tantôt encore en tant que supports de l'infraction, tantôt enfin en tant que moyens de l'infraction.

Qu'est-ce-que la cybercriminalité ?

« La cybercriminalité », également appelée criminalité informatique, consiste en la réalisation de délits commis à l'aide d'équipements informatiques et d'Internet. Parmi les exemples classiques de cybercriminalité, il est possible de citer la diffusion de virus informatiques, le téléchargement illégal, les actes de phishing, le vol d'informations personnelles telles que des données bancaires ou données à caractère personnelles. (1)

En outre, la cybercriminalité est une délinquance protéiforme, dont l'ampleur reste difficile à évaluer. Ses auteurs comme ses victimes présentent des profils variés : de simples particuliers, des organisations criminelles, des États peuvent être impliqués. Il est cependant certain que la cybercriminalité représente une menace croissante en raison de la place grandissante qu'occupe le numérique dans nos économies et nos sociétés.

Lorsque les systèmes et réseaux numériques sont l'objet de l'infraction, les atteintes aux systèmes de traitement automatisé de données, les infractions en matière de fichiers ou de traitements informatiques et enfin la cryptologie constituent aujourd'hui le cœur des incriminations.

En 2019, il y a eu 54 signalements d'incidents empêchant la victime d'accéder au contenu de ses fichiers pour demander une rançon. En 2020, ce type d'attaque est monté à 192. Les groupes cybercriminels ciblent désormais davantage les collectivités locales, du secteur de l'éducation, du secteur de la santé et les entreprises de services numériques.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié un rapport qui alerte à propos de cette progression, et explique ses causes. Selon ce rapport, aucun secteur ni zone géographique n'est épargné. (2)

I) Typologie des différents cyber – délinquants

A) Le hacker

Il exploite les failles dans une procédure d'accès des données pour casser un système informatique et y dérober ou détruire de l'information. Il va soit voler des informations qui étaient protégées dans un système informatique soit les modifier soit les copier frauduleusement.

A titre d'illustration, des hackers ont procédé à une campagne de ransomware (logiciel de rançon qui crypte des données personnelles) qui a infecté 300 000 ordinateurs en quelques heures et engendré, pour les entreprises victimes, plus d'un milliard de dollars de pertes financières (Cyberattaque WannaCry, Comm. UE, Renforcer la cybersécurité en Europe, 12 sept. 2018).

Aussi, un hacker a-t-il été condamné par le Tribunal Correctionnel de Lyon le 27 mai 2008 pour avoir modifié la page d'accueil du site Internet de la Fédération du Rhône du Front national en le « défaçant » par l'insertion de commentaires décalés (TGI Lyon, ch. corr., 27 mai 2008, obs. É. A. Caprioli, préc.).

B) Les crackers

Le cracker n'est autre qu'un pirate informatique en mesure de couvrir plusieurs domaines de spécialisations. Ses compétences peuvent l'amener à « cracker » les protections diverses d'un ordinateur afin de s'y introduire et ainsi voler des données. Toutefois, cet acte est généralement assimilé à du hacking. Par conséquent, on retient surtout du cracker sa capacité à casser les

multiples protections d'un logiciel ou partagiciel, d'une application ou même d'un système d'exploitation sous licence.

Également, ils sont spécialisés dans le cassage des codes de protection anti-copie des logiciels qui sont sous licence des jeux. Ce qui permet ensuite aux personnes qui téléchargent les jeux ou ces logiciels d'en bénéficier gratuitement alors qu'elles sont sous licence. C'est en gros une sous-catégorie de hacker qui se spécialise sur soit la copie de logiciel voire le cassage de ces codes de logiciels qui seront utilisés gratuitement alors qu'elles sont payantes.

C) Le crasher

Il rentre dans un système informatique afin de le détruire ou de le saboter. Pour cela, il va utiliser deux moyens principaux :

La technique du déni de service ou denial of service : c'est l'arrêt de toute fonctionnalité informatique. Tel a été le cas dans une affaire ayant occupé le parquet de Paris en juin 2018 et qui concernait l'Office des Postes et de Télécommunication de la Polynésie Française (OPT). (3)

Le parquet de Paris a ouvert une enquête pour déni de service affectant depuis le début de l'année 2018 le principal fournisseur d'accès à internet, le fameux OPT. Il s'agissait d'attaque par réflexion qui est une technique servant à usurper une adresse mail pour interroger un certain nombre de serveurs repartis dans le monde et qui répondront légitiment à cette adresse IP.

Cette adresse IP usurpée sera destinataire d'un nombre important d'informations et sous le poids de cet afflux énorme d'informations venant d'autres ordinateurs arrivera à saturation. Ce qui aura pour conséquence une défaillance des serveurs informatiques en Polynésie.

Un internaute sous pseudonyme revendiquait sur internet être l'auteur de cette attaque par déni de service et il justifiait ses attaques du fait des tarifs qu'il considérait comme étant trop élevés. Il y avait une très grande distorsion entre les motivations du délinquant et son pouvoir de nuisance. Il demandait ainsi la somme de 300 dollars de bitcoins pour cesser ces attaques.

Des investigations ont été menées par le parquet de Paris qui a lui-même désigné la DGSI sur les éléments techniques qui lui ont été remis par la société victime de cette attaque et uniquement par les constatations de source ouverte. Le cyber-délinquant a finalement été identifié et interpellé au mois de juillet reconnaissant les faits.

Lors de sa garde à vue et de l'enquête, il a indiqué que pour réaliser cette attaque il avait seulement fait une location du temps avec un hébergement d'internet à hauteur de 60 dollars.

Ce sont des attaques peu coûteuses à réaliser et qui peuvent survenir assez fréquemment, mettant ainsi les entreprises dans un état de vulnérabilité. Le constat est que de grands effets néfastes peuvent être causés par l'utilisation de matériels assez simples et accessibles à tous.

II) D'autres outils peuvent être utilisés par les cybers-délinquants

A) Les chevaux de Troie

Ce sont des logiciels qui permettent d'ouvrir « la porte » dans un ordinateur et qui permettent de prendre le contrôle à distance de cet ordinateur et d'y activer un certain nombre de programmes nocifs que l'on appelle des « Malwares ».

L'outil en lui-même n'est pas nocif mais sera utilisé comme véhicule du programme nocif appelé Malwares. Il est vital pour les entreprises qui font de la cybersécurité de se protéger en concevant des anti-virus et des programmes qui vont permettre de bloquer ces chevaux de Troie.

B) Les logiciels espions

Ces logiciels vont s'introduire dans un système informatique pour recueillir à des fins commerciales le profil d'un utilisateur au vu de sa navigation ou pour recueillir ses informations personnelles. Typiquement, un logiciel espion qui va être sur votre ordinateur ne va pas détruire des informations ni altérer des programmes. Au contraire, il va faire en sorte que tout reste exactement dans l'état précédant l'attaque, tout en lui permettant de lire un certain nombre d'informations confidentielles.

Tel est le cas du logiciel Pegasus qui était un programme de surveillance et qui permettait de prendre à distance le contrôle d'un téléphone et d'y lire les données qui étaient inscrites par son utilisateur.

Comment marche un logiciel espion ? Le téléphone qui est la cible de l'attaque va recevoir une adresse sur laquelle il faudra cliquer et à ce moment-là, le logiciel va par la suite contourner la sécurité du téléphone et s'y engouffrer afin de capter toutes les données de l'utilisateur.

C) Les botnets

Ce sont des systèmes constitués par un ensemble de machines, d'ordinateurs, téléphones et autres appareils. L'ensemble des machines est affecté par un même logiciel malveillant. Et l'ensemble de ses machines vont se connecter à un système de commande et de contrôle.

En vérité aujourd'hui, tous les systèmes de logiciels malveillants vont utiliser cette architecture en botnets qui permet de rapatrier de l'information vers les cybers-attaquants, permettant de transmettre des ordres vers les fameuses machines infectées.

On est tout simplement sur des attaques informatiques qui vont être démultipliées par le nombre de machines infectées. Les différentes informations qui vont être rapatriées vers les cybers-attaquants sont les données qui sont confidentielles et les ordres qui sont transmis via cette architecture en botnets sont des ordres d'exécution d'une action sur la machine comme le téléchargement d'une mise à jour de logiciels malveillants.

D) Les virus informatiques

C'est un programme qui inclut en général dans un format de fichiers utilisés et qui est stocké sur un ordinateur à l'insu de son utilisateur. Et ce programme informatique ou ce code informatique est susceptible de s'auto-exécuter à un moment précis ou de s'exécuter lors du lancement de logiciel. Le but de ce virus est de rendre le système informatique hors d'usage en détruisant

certains fichiers ou en saturant les ressources de la machine.

Sur ce point, il convient de s'attarder sur l'utilisation du rançon-logiciel, une fraude informatique largement répandue : les cybercriminels introduisent un logiciel malveillant dans le système informatique d'une entreprise, cryptent les fichiers qui s'y trouvent ou soustraient des données confidentielles puis exigent le paiement d'une rançon pour que la restriction soit levée ou que les données ne soient pas divulguées, à un concurrent par exemple.

Aux termes d'un avis du 1er octobre 2020, le Bureau du contrôle des avoirs étrangers du Trésor américain (Office of Foreign Assets Control) a expressément indiqué que les entreprises qui paieraient une rançon à des cybercriminels faisant eux-mêmes l'objet de sanctions américaines (par exemple, des cybercriminels ressortissants de Corée du Nord ou d'Iran), ainsi que les tiers ayant facilité le paiement d'une telle rançon (assureurs, établissement bancaires, etc.), pourraient se voir infliger de lourdes sanctions. La vigilance est donc de mise pour les entreprises en raison notamment de l'extraterritorialité de la législation américaine.

III) Multiplication des mécanismes d’extorsion

L'informatique est la science du traitement automatique de l'information reposant sur des procédés de recueil, de tri, de conservation, de communication et d'utilisation faisant appel à des programmes d'ordinateurs. Son apparition et son développement ont marqué la criminalité : les matériels, programmes et données informatiques se prêtent, comme objet, produit ou moyen du délit, à des faits aussi divers que le vol, l'abus de confiance, l'escroquerie, le recel, la contrefaçon, la pédopornographie ou encore l'espionnage et, comme élément de preuve, à toute infraction (trafic de stupéfiants, extorsion, blanchiment, etc.) dont les traces de la préparation, de la commission ou du profit qui en est tiré sont susceptibles de s'y trouver imprimées.

Depuis novembre 2019, une tendance qui consiste à faire pression sur la victime en exfiltrant ses données et en la menaçant de les publier sur un site Internet, est en hausse. Cette démarche est appelée la double extorsion, car le chiffrement est précédé d’une exfiltration de données.

En outre, les atteintes intentionnelles à la sécurité des systèmes d'information atteignent des niveaux jamais égalés. Ainsi, une étude de Moody's indique que les cyber-attaques contre les institutions financières ont connu une augmentation de 238 % dans le monde entre février et avril 2020. (4) Les tentatives d'extorsion de données personnelles ont, quant à elles, été multipliées par neuf. Par ailleurs, selon une autre enquête « Enduring from Home : COVID-19's Impact on Business Security », 24 % des entreprises interrogées ont indiqué devoir supporter des coûts imprévus pour faire face à des incidents de cybersécurité depuis le début de la pandémie. (5)

L’extorsion est prévue par les articles 312-1 et suivants du Code pénal. L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque.

L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende. (6)

Les délits d'extorsion et de chantage ont tous deux pour objet d'obtenir, par la contrainte, une signature, un engagement ou une renonciation, la révélation d'un secret ou la remise de fonds, de valeurs ou d'un bien quelconque et se distinguent l'un de l'autre par le moyen de pression utilisé.

L'élément intentionnel de ce délit est défini par la Cour de cassation, comme « la conscience d'obtenir par la force, la violence ou la contrainte ce qui n'aurait pu être obtenu par un accord librement consenti » (Cass. crim., 9 janv. 1991). (7) La Cour engage les juges du fond à vérifier si

la remise de fonds a été déterminée par l'existence d'une contrainte exercée en connaissance de cause sur la victime (Cass. crim., 3 nov. 2016, n° 15-83.892 : Bull. crim. n° 287, préc. n° 10). (8)

Si cette intention frauduleuse est caractérisée, les mobiles sont indifférents, selon la tradition du droit pénal français, au moins en ce qui concerne la constitution de l'infraction. Peu importe, notamment, que l'auteur ait agi dans un but légitime.

A noter pour finir que face à la multiplication des cyberattaques, Le Président Emmanuel Macron a présenté le jeudi 18 Février 2021 la stratégie française en matière de cybersécurité, après un échange par visio-conférence avec les directeurs des hôpitaux de Dax et Villefranche-sur-Saône, récemment victimes de rançongiciels, a annoncé l'Elysée.

Le chef de l'Etat annoncera une enveloppe d'un milliard d'euros, dont 720 millions de fonds publics, pour renforcer la filière et tripler son chiffre d'affaires à 25 milliards d'euros en 2025. (9)

Sources :

La cybercriminalité (https://www.murielle-cahen.fr/cybercriminalite/)

Les attaques informatiques avec extorsion ont triplé par rapport à l'année dernière (https://www.francesoir.fr/societe-science-tech/les-attaques-informatiques-avec-extorsion-ont-triple-par-rapport-lannee)

Organiser un exercice de gestion de crise cyber (https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/)

Moody's Investors Service, Sector in-depth, 8 juill. 2020, p. 3.

Malwarebytes, Enduring from Home, COVID-19's Impact on Business Security, p. 5.

L’extorsion est prévue par l’article 312-1 et suivant du Code pénal.

L'élément intentionnel de ce délit est défini par la Cour de cassation, comme « la conscience d'obtenir par la force, la violence ou la contrainte ce qui n'aurait pu être obtenu par un accord librement consenti » (Cass. crim., 9 janv. 1991).

La Cour engage les juges du fond à vérifier si la remise de fonds a été déterminée par l'existence d'une contrainte exercée en connaissance de cause sur la victime (Cass. crim., 3 nov. 2016, n° 15-83.892 : Bull. crim. n° 287, préc. n° 10)

Cybersécurité : Macron présente la stratégie française (https://www.francesoir.fr/actualites-france/cybersecurite-macron-presente-la-strategie-francaise)