Vos données personnelles en otage, puis chantage

Vos données personnelles en otage, puis chantage

Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité

Quel mode opératoire ?

Le mode opératoire est toujours sensiblement le même :
Un individu parvient à s'introduire dans le système informatique d'une entreprise ou d'un particulier. en extrayant les données y étant stockées.
Dans un second temps, l'internaute ou l'entreprise victime se voit réclamer le versement d'une rançon.
A défaut de paiement, ces informations personnelles seront diffusées sur la toile.
L'exemple le plus significatif en la matière est le cas du site de rencontres extraconjugales canadien ASHLEY-MADISON.COM, victime d'une cyberattaque le 15 juillet 2015.
Un groupe de « hackers » se faisant appel « The Impact Team » a réussi à pénétrer sur les serveurs du site et à en récupérer les données relatives à ses 37 millions d'abonnés de par le monde.
La fermeture du site a alors été exigée, son éditeur se voyant menacé d'une publication en ligne de l'intégralité de ses données. Précisons que cette menace a été mise à exécution au cours du mois d'août 2015.
Une fois ces informations rendues publiques, certains (anciens) clients du site se sont vus demander la remise de fonds, à défaut de quoi leurs informations personnelles seraient adressées directement à leurs proches ou à leurs relations professionnelles.
Autant dire que l'image de l'entreprise victime est ternie, la sécurité de son système informatique étant clairement remise en cause.
Les abonnés voient également des informations (très) personnelles dévoilées publiquement, telles que leur lieu de résidence, leurs coordonnées bancaires, leurs loisirs et habitudes de consommation, leurs fantasmes et désirs sexuels.

Dans une moindre mesure, les particuliers peuvent être individuellement les cibles de phénomènes de ce type.

Pour ces derniers, il prendra la forme d'un programme informatique malveillant appelé « rançongiciel », dérivé de l'anglicisme «ransomware » et, précisons-le, contraction des termes « rançon » et « logiciel ».
Ce programme chiffre ou crypte les données de l'internaute, présentes sur le disque dur de son ordinateur.
Si il souhaite les récupérer ou éviter leur divulgation, il devra là encore payer la rançon exigée.
Une variante consiste à arborer le logo d'une unité de police de type INTERPOL, en accusant l'internaute de détenir illicitement des œuvres protégées par le droit d'auteur ou bien des vidéos ou photographies pédopornographiques.

Quelles Infractions pénales ?

Le chantage et l'extorsion

« Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, 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. » (article 312-10 du Code pénal)
Ce délit est puni de 5 ans d'emprisonnement et de 75.000,00 Euros d'amende.
« Lorsque l'auteur du chantage a mis sa menace à exécution, la peine est portée à sept ans d'emprisonnement et à 100.000 euros d'amende. » (article 312-11 du Code pénal)
La menace sera mise à exécution, à partir du moment où les données sensibles seront publiées en ligne ou communiquées à des tierces personnes.
« 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. » (article 312-1 du Code pénal)
En la matière, la contrainte ne reposera pas sur la force physique, mais sera purement morale ou psychologique.

L'intrusion dans un système informatique

L'accès et le maintien frauduleux dans un système

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. » (article 323-1 du Code pénal)

L'entrave au fonctionnement d'un système

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-2 du Code pénal)
Le chiffrement ou le cryptage de données entrave nécessairement le bon fonctionnement d'un sytème informatique.

La suppression ou la modification frauduleuse de données

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-3 du Code pénal)

Les atteintes à la vie privée

« Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.» (article 226-1 du Code pénal)
« Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l' article 226-1.» (article 226-2 du Code pénal)
L'atteinte à l'intimité de la vie privée sera ainsi caractérisée, lorsque l'objet du chantage consistera en des photographies ou des vidéos représentant des personnes dans un lieu privé.

La violation du secret des correspondances (électroniques)

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. » (article 226-15 du Code pénal)
Le délit de violation du secret des correspondances est pleinement constitué, dès lors que la menace porte sur la teneur de courriers électroniques, d'emails ou de messages privés échangés entre abonnés ou utilisateurs d'un site.

Les infractions à la législation sur les données personnelles

Le traitement illicite de données personnelles
« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »(article 226-16 du Code pénal)
La collecte frauduleuse de données personnelles
« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226–18 du Code pénal)
Le défaut de sécurité des données
La particularité de cette dernière infraction est qu'elle vise, non pas l'auteur de l'attaque, mais bel et bien sa victime directe, le responsable du traitement des données.

En effet, les personnes, entreprises, organismes et collectivités, en charge du traitement des données de leurs utilisateurs ou de leurs usagers, sont tenus de mettre en œuvre toutes les mesures nécessaires, afin d'assurer la sécurité et la confidentialité desdites données.
A défaut, ils engageront leur responsabilité civile et pénale sur le fondement des articles 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et 226–15 du Code pénal:
« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » (article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226-15 du Code pénal)

Au cas par cas, d'autres infractions peuvent également être constituées, telles que les délits d'escroquerie, d'usurpation d'identité (numérique), voire même d'usurpation de fonctions, dans la situation où le cyber-délinquant se fait passer pour une unité de police, afin de se faire remettre des fonds.

Quelles solutions ?

La plainte pénale

Que l'on soit une entreprise, une collectivité ou un particulier victime de ce type d'agissements, le premier réflexe est de déposer plainte auprès des services de police ou de gendarmerie ou bien directement auprès du Procureur de la République.
Ce dernier se réservera le droit d'engager des poursuites ou bien de procéder à un classement sans suite de la plainte, faute notamment de disposer d'éléments suffisants afin d'identifier et de localiser précisément le ou les auteur(s) des faits.
En cas de classement sans suite, la victime disposera alors de la faculté de se constituer partie civile auprès du doyen des juges d'instruction, ce qui déclenchera automatiquement des poursuites pénales.

Le retrait de contenus illicites

Si les informations personnelles sont publiées sur un site internet en particulier, leur retrait peut être demandé directement auprès de son éditeur.
A défaut de réponse de sa part ou si il n'existe aucun moyen de le contacter, la suppression des contenus illégaux devra être alors demandée à l'hébergeur du site, en application de l'article 6-I-5 de la loi n°2004-575 pour la confiance dans l'économie numérique.

Le déréférencement et la désindexation des moteurs de recherche

Lorsque le nom et le prénom d'une personne sont tapés sur un moteur de recherche, la liste des résultats de recherche peut faire apparaître des liens renvoyant vers les informations frauduleusement obtenues et divulguées.
Dans ce cas, il est envisageable de demander la désindexation de ces liens directement auprès du moteur de recherche et, le cas échéant, par voie judiciaire.

Réagissez à cet article

Source : *Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité – Maître thibault prin*
Thibault PRIN AVOCAT
Avocat inscrit au Barreau de PARIS