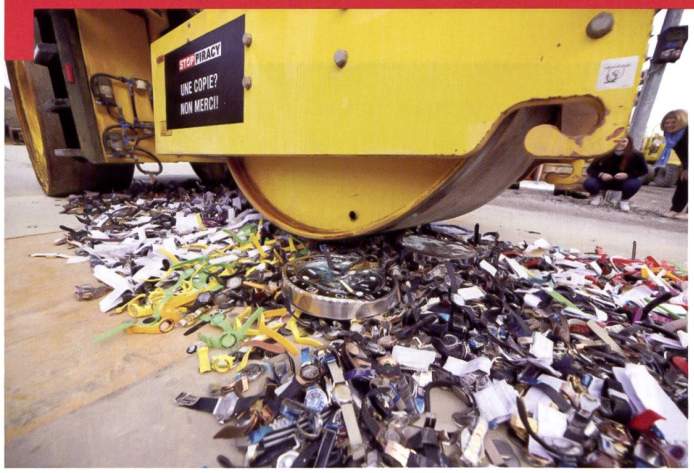
Piratage et contrefaçon au temps du coronavirus



Police

Piratage et contrefaçon au temps du coronavirus

Lena Ebener
Rédactrice RMS

Déjà en 2018, 10'000 emplois disparaissaient du marché du travail helvétique en raison du commerce de contrefaçon. Alors que la crise sanitaire entraîne une crise économique dont les répercussions se font sentir sur le marché de l'emploi, la situation pourrait encore se péjorer en raison de l'augmentation des attaques cyber, du piratage et de la contrefaçon. Chaque année, les entreprises suisses perdent plusieurs milliards. Pour la première fois, des chiffres concrets sont disponibles, ils ressortent de la nouvelle étude réalisée par l'Organisation de coopération et de développement économiques (OCDE), publiée fin mars 2021, sur mandat de l'Institut fédéral de la propriété intellectuelle (IPI).[1] Les données sont édifiantes alors même qu'elles sont antérieures à la crise sanitaire et les failles sécuritaires qu'elle a engendrées (voir encadré). En 2018, des consommateurs du monde entier ont déboursé plus de 2 milliards CHF pour des produits « suisses » contrefaits, pensant acheter un original, ce qui menace la bonne réputation des entreprises.

En l'absence de contrefaçon, 2 milliards CHF se seraient ajoutés au chiffre d'affaires de l'industrie horlogère et bijoutière du pays, au lieu de finir sur les comptes de faussaires. L'industrie des machines, des équipements électriques et des métaux est touchée à hauteur de plus de 1 milliard CHF. Des marques de vêtements et chaussures « Swiss made » sont elles aussi impactées, tout comme l'industrie pharmaceutique. La perte totale dépasse les 4,5 milliards et exclut les cas où les consommateurs étaient conscients d'acheter une contrefaçon en raison de son prix bas notamment, ce qui n'a en général pas remplacé l'achat d'un produit original.

Car oui, nous risquons parfois de payer le prix fort pour un article de luxe contrefait, qui se retrouve en boutique après avoir été mélangé dans la chaîne de distribution officielle. Ce qui s'explique par la complexification des chaînes d'approvisionnement et la multiplication des intervenants sur un marché mondialisé. Surtout que la contrefaçon est un domaine très lucratif. Le business de la contrefaçon de médicaments arrive même en tête des trafics illicites, devant celui de la drogue. Dans cette branche, pour 1'000 US$ investis, un criminel peut générer entre 200'000 et 500'000 US$, contre seulement 20'000 US$ avec le trafic d'héroïne.[2]

La veille comme premier outil

Pour savoir comment lutter contre la contrefaçon, il faut déjà comprendre d'où elle provient. Le lieutenant-colonel Daniel Donnet-Monay, PDG de *Vici Swiss Competitive Intelligence SA*, détaille ses observations : *« Les plans des articles contrefaits peuvent provenir de plusieurs facteurs. 1. De la trahison à l'interne, en général pour des raisons pécuniaires, mais cela peut aussi être par vengeance ou idéologie. 2. Des erreurs liées à l'utilisation des applications gratuites comme Facebook, Snapchat, TikTok et compagnie. Par exemple, le collaborateur qui prend un selfie devant les plans d'une nouvelle machine et l'envoie à une amie sur une messagerie instantanée, ou la femme de ménage qui, le soir dans les locaux vides, se filme en chantant devant des pièces de la prochaine collection. 3. Le vol des données. Nous nous sommes penchés sur les incidences sécuritaires de l'utilisation d'internet au bureau et, surtout, dans le cadre du télétravail. 100% des entreprises sont concernées ».*

Alors que le réflexe pourrait être de mettre en place une authentification forte ou un accès limité aux seuls appareils préautorisés, installer un pare-feu, Daniel

1 Etude de l'OCDE : « Contrefaçon, piratage et l'économie suisse. »

2 Article : « Comment mieux combattre la contrefaçon », Laurence Duarte, Harvard Business Review.

Donnet-Monay, passionné d'histoire militaire, use de la métaphore pour faire comprendre que ça n'est pas la meilleure tactique selon lui : *« Le meilleur outil contre la fuite de données, c'est la veille stratégique. Depuis 20 ans, les entreprises s'entourent de professionnels en cybersécurité, qui leur ont fabriqué des châteaux forts. C'est humain de se sentir rassuré quand la forteresse est haute et épaisse, mais même la plus imprenable a ses failles, il faut bien faire entrer l'eau et éliminer ses déchets. La plupart des stratégies cyber sont à l'image des constructions du maréchal Sébastien Le Prestre, marquis de Vauban, qui a construit les plus grands ouvrages sous Louis XIV. Vici se positionne en tant que forces spéciales, en amont et en aval du château, pour voir ce qui va rentrer, les attaques qui se préparent, et ce qui va sortir comme les mots de passe. Sinon c'est comme construire un bunker et laisser la clé sur la porte, ça ne*

Les failles du tout virtuel

La pandémie a entraîné une augmentation du commerce en ligne, mais pas seulement. Le coronavirus a modifié nos habitudes : nous vivons littéralement sur internet, Skypéro, réunions sur Zoom, livraison de nourriture, télétravail, combien de brèches ce transfert du réel au virtuel a-t-il généré ?

En utilisant un ordinateur non dédié pour travailler et surfer sur internet en parallèle, les risques de laisser fuiter son adresse mail et ses codes d'accès professionnels sont élevés. Le problème peut venir du matériel utilisé. Par exemple, en Grande-Bretagne, 61 % des sondés par la firme norvégienne Promon admettent utiliser leur ordinateur privé pour travailler et se connecter au réseau d'entreprise,[1] 66 % ont répondu n'avoir reçu aucune recommandation sur les questions de cybersécurité de la part de leur employeur les 12 derniers mois, 77 % disent ne pas s'être inquiété des risques potentiels. Le problème peut également venir des sites visités, certains employés ont même surfé sur des sites pornographiques dans un onglet à côté de celui de livraison de pizza, de leur compte bancaire, des réseaux sociaux, d'un concours pour gagner un smartphone, tout ça en travaillant sur des dossiers importants.

Pour se faire une idée de l'ampleur du problème, il n'y a qu'à voir le récent scandale lié à Facebook, une vulnérabilité dans le système a permis le vol des données de 533 millions d'utilisateurs en 2019.[2] C'est récemment que ces informations qui permettent de lier une adresse mail à un numéro de téléphone ont commencé à circuler librement sur des forums utilisés par des *hackers*. Elles concernent des utilisateurs de 109 pays dont la Suisse et, nous exposent à un plus grand risque d'attaque, notamment parce-que les pirates peuvent, dès lors, utiliser le multi-facteur par SMS que l'on retrouve sur de nombreuses plateformes d'authentification ou pour récupérer un mot de passe. Ces données peuvent être exploitées pour une usurpation d'identité puis, extorquer de l'argent à des tiers.

Il est possible de savoir si notre compte a été compromis en entrant son mail ou son numéro de téléphone sur le site https://haveibeenpwned.com/, une référence en la matière. Si tel est le cas, il est recommandé de changer de mot de passe, mais une fois que le mal est fait, mieux vaut ne pas rester seul face au problème et s'entourer de professionnels.

Quant à savoir s'il est légal d'agir ou non, Daniel Donnet-Monay est catégorique : *« Une attaque qui viendrait de Suisse toucherait uniquement des serveurs basés en Suisse, ça serait une affaire à régler devant les tribunaux. Mais il n'y a aucune base légale qui légifère internet, d'autant que la question du for juridique serait problématique. Les pirates fonctionnent par ricochet. Une attaque dont l'auteur se situe en Chine sera déclenchée du Népal ou de Mongolie. On ne va pas envoyer un courrier recommandé au Nigéria pour demander aux criminels d'arrêter leur activité illégale, ils vous riraient au nez, pourtant on doit quand-même agir, c'est de la légitime défense et, la meilleure défense c'est l'attaque ».*

1 https://promon.co/security-news/two-thirds-of-remote-workers-in-uk-given-no-cybersecurity-training-from-employers-in-past-year.

2 Article : « Les données personnelles volées à 533 millions d'utilisateurs de Facebook ont été mises en ligne », Business Insider, 3 avril 2021.

sert à rien ». Pour se prémunir contre la fuite de données, effectuer une veille sur Internet est le premier pilier.[3] Dans la lutte contre la contrefaçon, il existe d'autres axes importants.

Sensibiliser ou désinformer

La coopération entre tous les acteurs est essentielle, une entreprise ne peut pas gagner la bataille seule. Les organismes gouvernementaux doivent s'impliquer et le font, les autorités et le secteur économique collaborent dans la lutte contre la contrefaçon, comme le démontre l'IPI en ayant commandité l'étude de l'OCDE, et en consentant à fournir des efforts encore plus importants à l'avenir, pour inscrire des standards dans les accords de libre-échange, en vue de faire respecter les droits de propriété intellectuelle. Les consommateurs ont également leur rôle à jouer, c'est pourquoi des campagnes de sensibilisation sont mises sur pied. C'est d'ailleurs la tâche principale de la plateforme suisse de lutte contre la contrefaçon, STOP PIRACY, qui publie des sujets intéressants sur son site www.stop-piracy.ch, par exemple en présentant une famille sans histoires, dont les membres soutiennent, par leurs achats, ces organisations criminelles. Autre action, STOP PIRACY s'est associé à des influenceurs pour qu'ils sensibilisent leurs *followers*, mais l'intervention ne s'arrête pas là. « *Ces dernières années, nous nous sommes focalisés sur les intermédiaires qui jouent un rôle dans la chaîne de distribution des contrefaçons. Parmi eux se trouvent les services de paiement, les entreprises de logistique, qui ne violent pas les droits de la propriété intellectuelle, mais sont un maillon qui permet aux contrefacteurs de gagner de l'argent avec leur activité illégale. C'est pour cela que nous cherchons le dialogue* avec eux » explique Juerg Herren, avocat et chef du service juridique droit général, designs et mise en œuvre du droit à l'IPI. « *Notre troisième pilier d'activité est l'échange au niveau international, dans le cadre des organisations comme l'Observatoire européen des atteintes aux droits de la propriété intellectuelle* » précise-t-il.

Sachant que l'erreur humaine est un facteur important de fuite, des mesures de sensibilisation au sein de l'entreprise doivent être mises en place. « *Une fois les failles identifiées, les collaborateurs sensibilisés, la personne qui a l'habitude de se prendre en photo devant des données sensibles peut continuer à le faire, mais devant des faux plans, pour pousser les contrefacteurs à commettre des erreurs* » confie le PDG de l'agence de cyber renseignements et cyber protection Vici. « *Il faut perturber, désinformer les criminels, si on pratique le contre-renseignement et qu'on leur tend des pièges, ils vont perdre du temps à usiner des mauvaises pièces* ».

L. E.

3 https://www.vici-agency.com/fr/cyber-renseignement.