Cybercriminalité

Source
Le Figaro
Cyril Coantiec
23 décembre 2014

1. Piratage de Sony : le rappel des faits date par date

Depuis le vol et la divulgation en masse de données informatiques du studio de cinéma le 25 novembre dernier, de nombreux événements ont secoué la société. Retour sur l'affaire.

25 novembre 2014 : le piratage des studios Sony est revendiqué

Sony Pictures est victime d'un piratage massif. Le groupe de hackers, à l'origine de l'attaque, se fait appeler GOP, Guardian of Peace (les Gardiens de la paix). Le groupe a piraté la plupart des ordinateurs des employés du studio de cinéma. « Nous avons obtenu toutes vos données internes incluant des secrets. Si vous n'obéissez pas, nous publierons ces données. Vous avez jusqu'au 24 novembre à 23h pour décider », pouvait-on lire sur le message qui bloquait les machines. Selon le site Web *The Next Web*, ils contiennent notamment des informations financières, mais certains sont protégés par des mots de passe. Sony a indiqué qu'une enquête avait été ouverte. Les ordinateurs des employés ont été immédiatement déconnectés d'Internet.

1er décembre 2014 : diffusion illégale de cinq longs métrages et possibilité que l'attaque vienne de Corée du Nord envisagée

Les hackers, les Gardiens de la paix, ont mis en ligne illégalement cinq films, *Annie*, *Mr. Turner*, *Still Alice*, *To Write Love On Her Arms* et *Fury*, distribués par la société. En quelques heures, le long métrage, avec Brad Pitt, était le second film le plus téléchargé sur Pirate Bay.

Sony Pictures évoque la possibilité que cette attaque vienne de Corée du Nord. L'agression de ces hackers serait liée au film *L'interview qui tue!*, qui sort en février en France et à Noël aux USA et dont Sony Pictures est le distributeur. D'ailleurs, parmi les révélations faites à la suite du piratage, on a retrouvé sur la Toile les cachets des acteurs du film : James Franco et Seth Rogen. Cette comédie met en scène un journaliste télé, incarné par James Franco, et son producteur, joué par Seth Rogen, qui projettent d'assassiner le dictateur nord-coréen Kim Jong-Un. Une comédie qui ne plaît pas à tout le monde, à commencer par la Corée du Nord.

Dans une interview accordée au *Telegraph*, Kim Myong-chol, le directeur du Centre d'éducation pour la réunification, avait exprimé sa colère. « Il y a une ironie particulière dans cette histoire qui montre le désespoir du gouvernement et de la société américaine. N'oublions pas qui a tué le Président Kennedy - les Américains. Le Président Obama devrait faire attention, dans le cas où son armée voudrait également le tuer ». Contacté par *le Figaro*, Sony Pictures France considère que l'attaque, d'ampleur mondiale, nécessitera « plusieurs semaines de réparation pour rétablir le système ».

3 décembre 2014 : Sony Pictures fait appel au FBI

Sony Pictures s'est attaché les services d'une société de sécurité indépendante, Mandiant, en contact avec le FBI, pour rétablir le système. Son responsable Kevin Mandia s'est exprimé dans un message destiné à Michael Lynton, chef de la direction de Sony Pictures. Il ne cache pas l'ampleur du travail à accomplir pour faire face à cette cyberattaque encore jamais vue.

« C'est un crime sans précédent, bien planifié, mené par un groupe organisé face auquel ni Sony, ni d'autres entreprises auraient pu se préparer. Le malware utilisé est indétectable par les logiciels antivirus standards, et assez dangereux et exceptionnel pour que le FBI lance une alerte en vue de prévenir les autres entreprises de cette menace. La portée de cette attaque diffère de tout ce qu'on a pu voir par le passé. Son but était à la fois de détruire des informations et de dévoiler des données au public. »

9 décembre 2014 : la Corée du Nord nie son implication dans le piratage de Sony Pictures

La Corée du Nord a récusé toute responsabilité dans l'attaque informatique massive qui a visé Sony Pictures. La Commission de défense nationale nord-coréenne a dénoncé les « fausses rumeurs » impliquant la Corée du Nord dans l'attaque contre Sony, tout en la qualifiant d' « acte légitime de partisans et de sympathisants de Pyongyang ».

11 décembre 2014 : la riposte de Sony sur les sites hébergeant des données piratées

D'après les informations du site spécialisé Re/Code, Sony Pictures a lancé des attaques contre les sites Internet ayant publié des données appartenant à la société. Le but est de ralentir la vitesse de téléchargement pour empêcher les internautes d'accéder aux fichiers.

Parmi les informations mises en ligne, outre les films inédits diffusés le 1er décembre dernier, on retrouve un annuaire des salariés, ainsi que des scripts de futurs épisodes de séries. On compte aussi des copies de pièces d'identité d'acteurs, comme Cameron Diaz et des commentaires peu flatteurs à propos de certains artistes, comme ceux concernant Angélina Jolie. Le salaire des dix-sept responsables les mieux payés du studio a été révélé, avec en tête les trois millions de dollars annuels touchés pour le PDG Michael Lynton et la coprésidente Amy Pascal. On tombe également sur des pseudonymes utilisés par des célébrités pour réserver leurs chambres d'hôtel. Le préjudice pourrait s'élever à plusieurs dizaines de millions de dollars.

Un échange de courriels, entre la coprésidente de Sony Pictures Amy Pascal et le producteur Scott Rudin, a aussi été diffusé. La responsable explique ce que le Président des États-Unis aimerait produire comme film, citant *Django Unchained*, *Twelve Years a Slave* ou *Le Majordome*, des longs métrages qui font référence à des personnages de couleur noire. Amy Pascal a présenté ses excuses après la publication de cette discussion. « Le contenu de mes courriels était déplacé et sans aucun égard, mais ne reflète pas ce que je suis. Bien qu'il s'agisse d'une correspondance privée qui a été espionnée, je prends la totale responsabilité de tout ce que j'ai écrit et je m'excuse auprès de tous ceux que j'ai blessés », a-t-elle déclaré dans un communiqué envoyé au magazine *Variety*.

15 décembre 2014 : le scénario de James Bond et la tristesse de George Clooney révélés

EON Productions, société qui produit les films de James Bond, a confirmé, dans un communiqué, qu'une première version du scénario de *Spectre* a été diffusée. En novembre, cette version a été envoyée par courriel à plusieurs dirigeants de Sony pour être révisée. D'après le siteGawker,les dirigeants concèdent que le film est « globalement bon » et que «les 100 premières pages sont fantastiques». Mais ils déplorent « une fin décevante ». Celle-ci serait «ennuyeuse» et pourrait être raccourcie de « vingt pages ».

Jonathan Glickman, président de la société de production et de diffusion MGM, Hannah Minghella, coprésidente de la production de Columbia Pictures, filiale de Sony, et Elizabeth Cantillon, productrice de Sony, ont également porté de sévères remarques tout au long du scénario. Le méchant, dont le nom est dévoilé, ne serait pas assez « convaincant » et le scénario manquerait de « rebondissements ».

Dans un autre registre, le même jour apparaissaient les courriels écrits par George Clooney, confiant son abattement à la coprésidente de Sony Pictures, Amy Pascal, après la sortie de son dernier film, *Monuments Men,* boudé par la critique internationale. Le comédien y racontait ne pas supporter pas les critiques négatives : « Je n'ai pas dormi depuis 30 heures... Cela empire. J'ai besoin d'être protégé de toutes ces critiques. Faisons-en juste un succès. »

16 décembre 2014 : Sony Pictures promet de « survivre à l'attaque informatique »

Les dirigeants de Sony Pictures ont promis que le studio de cinéma survivrait à l'attaque informatique massive dont il a fait l'objet fin novembre. Le directeur général de Sony Pictures Entertainment, Michael Lynton, et la coprésidente, Amy Pascal, se sont exprimés à propos du piratage informatique. M. Lynton a déploré une opération « criminelle » qui a ciblé des « victimes innocentes ». Au total, 47'000 personnes auraient été ciblées par l'attaque, leurs données personnelles

y compris leurs adresses, courriels, numéros de sécurité sociale ayant été dérobés.

Amy Pascal, la coprésidente de Sony Pictures, a affirmé, de son côté, que les employés étaient « la colonne vertébrale de ce groupe ». Le FBI et Sony n'ont donné aucun détail sur les pistes d'investigation, se contentant de dire qu'une « enquête mondiale est toujours en cours ». Contacté par *Le Figaro*, Sony Pictures France a réaffirmé sa volonté de « survivre à la cyberattaque » et «ne pas se laisser faire», même si les salariés ne peuvent toujours pas utiliser leurs ordinateurs de travail. Les pirates à l'origine de la cyberattaque, les Gardiens de la Paix, ont proféré de nouvelles menaces pour Noël.

17 décembre 2014 : l'avant-première de *L'interview qui tue!* annulée à New York après de nouvelles menaces des hackers

Après de nouvelles menaces proférées par les hackers qui ont piraté le système informatique de l'entreprise américaine, le groupe de salles de cinéma américain Landmark Theatres a annoncé que l'avant-première du film *L'Interview qui tue!*, qui devait se tenir jeudi prochain, a été annulée.

Dans un nouveau message, le groupe GOP annonce le début d'un « cadeau de Noël », avec la mise en ligne de nouveaux extraits de courriels personnels du directeur général de Sony Pictures Entertainement, Michael Lynton. Ce récent message en forme de menace, rappelant le souvenir tragique des attentats du 11 septembre 2001, menace ceux qui voudraient voir la comédie satirique, relayant un peu plus les spéculations sur une attaque de la Corée du Nord.

« Nous allons vous montrer clairement dans tous les lieux où *L'interview qui tue!* sera diffusé, notamment lors de l'avant-première, à quel destin tragique sont voués ceux qui cherchent à se moquer de la terreur », est-il écrit dans un mauvais anglais dans le message du groupe de pirates informatiques. « Rappelez-vous le 11 septembre 2001. Nous vous recommandons de vous tenir à distance de ces endroits *[où le film sera diffusé]*. Et si votre maison est à proximité, vous devriez partir. Tout ce qui va se passer dans les prochains jours sera dû à la cupidité de SPE. Le monde entier dénoncera Sony » peut-on lire dans le message.

La comédie satirique *L'interview qui tue!* accumule les déboires, après la décision d'annuler l'avant-première à New York. Les interviews des deux acteurs principaux Seth Rogen et James Franco, prévues dans le cadre de la promotion du film, ont également été supprimés de leur agenda. L'avant-première de *L'interview qui tue!* Interview) à Los Angeles, qui s'est tenue jeudi dernier, s'est déroulée sans prise de parole des deux comédiens. Le groupe de salle de cinémas américains Carmike ont aussi annoncé, mardi dernier, qu'ils ne voulaient pas diffuser le film dans leurs salles.

Source
Le Monde
20 décembre 2014

« The Interview » : la capitulation de Sony et d'Hollywood

Edito du « Monde ». Téléguidés par la Corée du Nord, les pirates informatiques remportent une victoire sans pareille dans l'histoire de la guerre cybernétique.

La firme Sony Pictures Entertainment vient de créer un précédent dangereux. Cédant à l'agression de pirates du cyberespace, téléguidés par la Corée du Nord, le studio a annoncé, mercredi 17 décembre, qu'il renonçait à sortir un film, *The Interview*, en salles ou sous tout autre support. Cette capitulation marque une date noire pour la liberté d'expression dans un monde qui vit à l'heure du numérique.

Les pirates informatiques remportent une victoire sans pareille dans l'histoire de la guerre

cybernétique. Ils font reculer Sony, qui comptait amortir un investissement de 80 millions de dollars dans ce film en en programmant la sortie pour les fêtes de Noël. Le studio « a fait une erreur » en annulant la sortie du film, a regretté, vendredi soir, Barack Obama, juste après que le FBI eut pointé la main du régime de Pyongyang dans les actes de piratage dont Sony a été victime.

Maraudant en toute liberté dans les ordinateurs de Sony, les pirates se sont emparés des mails de la direction, parfois d'une vulgarité consommée, de courriels éminemment privés, de scripts de films et autres documents censés être plus ou moins confidentiels. Ils ont rendu l'ensemble public et promis d'en mettre davantage encore en ligne s'ils n'obtenaient pas gain de cause : le retrait du film.

Déjà dure à encaisser pour la réputation de la direction et, plus encore, pour les tiers ayant pensé pouvoir correspondre avec elle par courrier électronique en toute sécurité, cette agression est allée plus loin. Les pirates – ils se font appeler « The Guardians of Peace », « Les Gardiens de la paix » – ont menacé de perpétrer des attentats dans les salles qui présenteraient le film. Les employés du studio ont eu la surprise, en allumant cette semaine leurs ordinateurs, d'y trouver le message suivant : « Le monde sera plein d'effroi si *The Interview* est distribué. Souvenez-vous du 11 Septembre… »

Hollywood avait déjà cédé. Avant même la décision de Sony, les plus grands réseaux de distribution avaient renoncé à accueillir *The Interview*. Le film relate le projet de deux journalistes qui, désireux de recueillir un entretien avec Kim Jong-un, sont recrutés par la CIA pour assassiner le chef du régime nord-coréen.

Si la thèse américaine est vraie – Pyongyang nie toute implication –, elle veut dire qu'un Etat peut faire chanter un journal, une maison d'édition, des producteurs de théâtre ou de cinéma pour obtenir le retrait d'un article, d'une enquête, de toute œuvre qui lui déplaît. Elle veut dire que tous les coups sont permis ou presque dans cet espace d'échanges – Internet – qui est au cœur de la vie quotidienne de l'époque. Elle confirme, hélas, qu'une forme de guerre est déjà bien engagée dans le vaste espace numérique, où plus rien n'est protégé.

Il y a vingt-cinq ans, le Guide de la République islamique d'Iran, l'ayatollah Ruhollah Khomeyni, prenait un « décret » religieux enjoignant aux musulmans du monde entier d'assassiner le grand écrivain britannique Salman Rushdie. Motif ? L'un de ses romans, Les Versets sataniques, aurait été insultant pour l'islam. L'affaire de *The Interview* représente le même type de menace. Comme le suggère notre confrère britannique The Financial Times, Sony doit répliquer en usant à son tour du Web : rendre le film The Interview accessible à tous ceux qui veulent le voir… en le mettant en ligne.

Source
Futura Tech
Fabrice Auclert
16 avril 2019

2. Triton, le malware industriel frappe à nouveau

En s'attaquant aux systèmes de protection de grands complexes industriels, les pirates peuvent causer des dommages mortels.

Les virus informatiques et autres malwares évoquent rarement l'idée d'un réel danger pour l'être humain. Ces mots désignent la plupart du temps des programmes qui affichent des publicités, envoient du courrier indésirable ou ralentissent les ordinateurs personnels. Cependant, il existe des programmes qui visent directement des sites industriels sensibles, comme Stuxnet découvert en 2010, qui aurait été développé par la NSA et Israël pour forcer l'arrêt du programme nucléaire iranien. En 2016, ce sont les virus Black Energy et CrashOverride qui ont attaqué les installations électriques en Ukraine.

Jusqu'à présent, les rares malwares qui ont attaqué les sites industriels n'ont pas cherché à faire de victimes, mais dernièrement un groupe inquiète les chercheurs avec des objectifs bien plus meurtriers. Le groupe de hackers Xenotime tente de compromettre des sites industriels plus dangereux, avec pour mission la destruction physique des installations. Le virus utilisé par le groupe a été découvert pour la première fois en 2017 dans la raffinerie Petro Rabigh en Arabie Saoudite. Le programme a été baptisé Triton, ou Trisis.

Un virus qui s'attaque directement aux dispositifs de sécurité

Une des particularités de Triton est de s'attaquer au système de sécurité Triconex de Schneider Electric. Ces automates sont conçus pour faire face aux défaillances ou aux pannes du système de production. Une telle attaque aurait pu permettre la libération de gaz de sulfure d'hydrogène, hautement toxique, ainsi que des explosions dues à des températures ou pressions élevées. Des arrêts de fonctionnement inexpliqués ont permis de détecter Triton, ainsi que de nombreux autres

malwares.

Une chance qui a certainement évité la catastrophe, mais les hackers ont probablement amélioré leur stratégie depuis. Cette infiltration, qui aurait pu passer inaperçue, ainsi que l'étendue des dégâts potentiels inquiètent beaucoup les spécialistes. D'autant plus que des tentatives d'intrusion ont été détectées notamment dans les raffineries et usines pétrochimiques aux États-Unis.

Une seconde victime et un mode opératoire

FireEye, une société de cybersécurité qui était intervenue en Arabie Saoudite, a déclaré lors d'un sommet organisé par Kaspersky, avoir été engagée en 2018 pour le compte d'une seconde victime qui n'a pas été nommée pour des raisons de confidentialité. Les experts ont pu donner des informations sur les attaques menées par Xenotime, qui serait lié au Kremlin. Le groupe a un mode opératoire qui rend la détection plus compliquée, car ils utilisent des programmes malveillants adaptés à chaque site visé. Pour cela, ils modifient des virus et malwares courants qui servent à contourner la sécurité et créer des portes dérobées, voler des mots de passe et prendre le contrôle des systèmes.

Les hackers de Xenotime sont également très patients, et prennent beaucoup de temps pour infiltrer entièrement les installations. Le groupe opérerait depuis 2014, ce qui suggère qu'ils pourraient avoir implanté du code sous forme de bombe à retardement dans des sites industriels à travers le monde. Les industriels devront donc analyser toutes les installations utilisant le matériel Triconex, à la recherche de fichiers spécifiques ou de flux réseaux suspects.

3. Une ville plongée dans le bleu éternel

Source
letemps.ch
Stéphane Benoit-Godet
1er juin 2019

Des hackers bloquent les systèmes informatiques de Baltimore. Plus de 20 cités américaines font l'objet d'attaques similaires depuis le début de l'année. Ironie de l'histoire, c'est un vers développé par la NSA qui est à l'œuvre.

Que peut l'informatique d'une ville face à une attaque de hackers qui utilisent l'arme la plus puissante qui soit ? Baltimore doit répondre à cette question. La cité du Maryland se voit complètement bloquée depuis le 7 mai, date à laquelle ses employés ont vu apparaître sur leurs écrans une demande de rançon. Leurs équipements ne répondent plus de rien depuis qu'un ver a pris possession de leur machine. Il n'est désormais plus possible de payer sa note d'électricité, de créer sa société ou d'interagir avec l'administration.

Baltimore doit faire face à une de ces attaques dont on entend de plus en plus parler. Le phénomène s'accroît notamment parce que les infrastructures publiques, dans lesquelles les investissements ne sont pas suffisants, représentent des cibles idéales pour les pirates du web. Rien que cette année, 24 municipalités américaines ont été attaquées. La grande originalité de ce cas tient toutefois à l'origine du malware, développé par la NSA, l'agence de renseignement technologique. *EternalBlue*, c'est son nom, a rendu de grands services à la bannière étoilée en permettant des opérations d'espionnage dans de nombreux pays. Son nom vient du fait que le dispositif s'attaque aux failles du système Windows de Microsoft qui, quand il crashe, affiche un écran d'un bleu profond.

Microsoft a fourni à ses clients une parade à EternalBlue dès 2017. Rester deux ans sans un patch est une faute grave.

Des pirates du web ont récupéré cette technologie et l'ont retournée à l'expéditeur. *EternalBlue* constitue ce qui se fait de mieux dans la panoplie de la cyberguerre. La NSA n'a pris le temps d'informer Microsoft du monstre qu'elle avait créé que cinq ans après sa création. Microsoft a sorti en 2017 un correctif, mais quelques mois plus tôt des hackers avaient volé, à la NSA elle-même, le code d'EternalBlue. Depuis, ses clones font des ravages un peu partout dans le monde. À l'initiative de la Corée du Nord, *WannaCry* a bloqué le système de santé britannique comme le réseau ferroviaire allemand. *NotPetya*, créé par la Russie pour attaquer l'Ukraine, a contaminé de nombreuses entreprises qui travaillaient sur place. Et des hackers iraniens se sont servis d'une version du malware pour s'attaquer à des compagnies aériennes.

Résultat, des ingénieurs des secteurs privé comme public se retrouvent aujourd'hui à pied d'œuvre à Baltimore pour tenter de la sortir du bleu éternel. Mais trois semaines après le premier message, la ville n'a pas pu reprendre la main. Ses représentants estiment que cet assaut va leur coûter au moins 18 millions de dollars. Tout ça pour une arme qui ne vient ni de Chine ni de Russie mais d'un organisme fédéral qui se trouve – ironie de l'histoire – à une trentaine de kilomètres de là.

Source
Europe 1
26 mai 2020

4. Une cyberattaque tous les trois jours dans les hôpitaux : « Il est temps pour les États d'agir »

Ces deux derniers mois, une cyberattaque visant les systèmes informatiques du secteur de la santé a eu lieu tous les trois jours dans le monde. Une tribune internationale, signée par plusieurs prix Nobel de la paix, des anciens présidents, des présidents d'ONG, appelle mardi les États à renforcer leur lutte, particulièrement problématique en ces temps de pandémie.

Entre mars et avril 2020, 18 cyberattaques ont été répertoriées dans le secteur de la santé. À plusieurs reprises, l'OMS reçoit des emails de phishing pour obtenir des données sur les vaccins et les traitements du coronavirus. Le 16 mars, le Health and Humans Services Department, aux Etats-Unis, est victime d'une attaque par « une autre organisation étatique » qui vise à l'affaiblir. Plusieurs hôpitaux espagnols sont à leur tour touchés, le 23 mars, juste avant le système de santé canadien, visé le lendemain.

Une tribune internationale publiée mardi et signée par plusieurs prix Nobel de la paix, des anciens présidents, des responsables d'ONG, ou encore par le patron de Microsoft, appelle à mettre fin aux cyberattaques sur les hôpitaux, et rappelle aux États leurs obligations de protection, particulièrement en ces temps de pandémie. « Il est temps pour les États d'agir, et de travailler ensemble pour protéger ces services dont tout le monde a besoin », affirme au micro d'Europe 1 Stéphane Duguin, président du Cyberpeace Institute, signataire de la tribune.

Opérations chirurgicales reportées et patients réorientés

L'attaque la plus impressionnante de ces dernières semaines a eu lieu mi-mars en République Tchèque, à l'hôpital de Brno, en pleine crise du coronavirus. Un logiciel infecte alors tous les ordinateurs et réclame une rançon. Le système informatique est planté, des opérations chirurgicales urgentes doivent être reportées, les patients réorientés. Les répercussions durent près d'une semaine. En novembre dernier, le CHU de Rouen avait vu 6.000 de ses ordinateurs infectés en quelques secondes. Le centre hospitalier avait marché au ralenti pendant plusieurs jours, l'attaque ralentissant de fait la prise en charge des patients.

Ces derniers mois, une attaque a eu lieu tous les trois jours dans les hôpitaux du monde entier. « Si des groupes armés entraient une fois tous les trois jours dans des hôpitaux, il est fort possible que la communauté internationale réagirait différemment... », soupire Stéphane Duguin.

Un « labyrinthe juridique » laissant de l'espace aux cybercriminels

« Il y a des difficultés financières, géopolitiques et technologiques à sécuriser le secteur de la santé. Ce qui laisse beaucoup d'espace aux cybercriminels », pointe Stéphane Duguin. Pourtant, ajoute-il, « le cadre juridique international permet de mettre à mal ces attaques illégales", citant notamment la charte des Nations unies, le droit humanitaire international et la convention de Budapest contre la cybercriminalité. Reste que cette réglementation éclatée, ce « labyrinthe juridique » dit Stéphane Duguin, profite finalement aux cybercriminels.

Lui et les autre signataires appellent désormais les États à "tout mettre en oeuvre" pour sécuriser leurs systèmes de santé, en y allouant des ressources technologiques et financières suffisantes. Et à se doter d'un « système judiciaire performant » pour que les cybercriminels soient « conduits devant la justice ».

Source
siecledigital.fr
Valentin Cimino
18 septembre 2020

5. Une femme décède au cours d'un ransomware dans un hôpital allemand

C'est une triste nouvelle que nous apprenons ce matin. Une femme est morte au cours d'une cyberattaque qui a touché l'hôpital universitaire de Düsseldorf, en Allemagne. Selon The Verge, il s'agirait du premier décès directement lié à un ransomware.

Le premier décès lié directement à un ransomware

Les cyberattaques sont fréquentes. Elles sont quand même plus rares contre les hôpitaux, surtout depuis le début de la crise du Covid-19 mais malheureusement certains hackers n'ont pas de pitié.

Alors que de nombreux hackers avaient promis un répit pour les hôpitaux tant que la pandémie de Covid-19 serait là, l'hôpital universitaire de Düsseldorf n'a pas été épargné. Toutefois, selon la presse allemande ce ransomware n'était pas destiné à toucher l'établissement de santé mais visait plutôt l'université voisine. Les hackers ont stoppé leur attaque dès l'instant où ils ont compris qu'ils avaient touché un hôpital.

Malheureusement il était déjà trop tard. Une femme est morte au cours de cette cyberattaque. Les autorités estiment qu'il s'agit du premier décès qui survient directement pendant une cyberattaque. L'hôpital de Düsseldorf n'a pas pu prendre en charge cette patiente à cause justement du ransomware en cours. Cela a contraint la femme à rouler 30 kilomètres supplémentaires pour trouver un autre établissement de santé, mais son état de santé était trop instable.

Les hackers peuvent-ils être tenus responsables ?

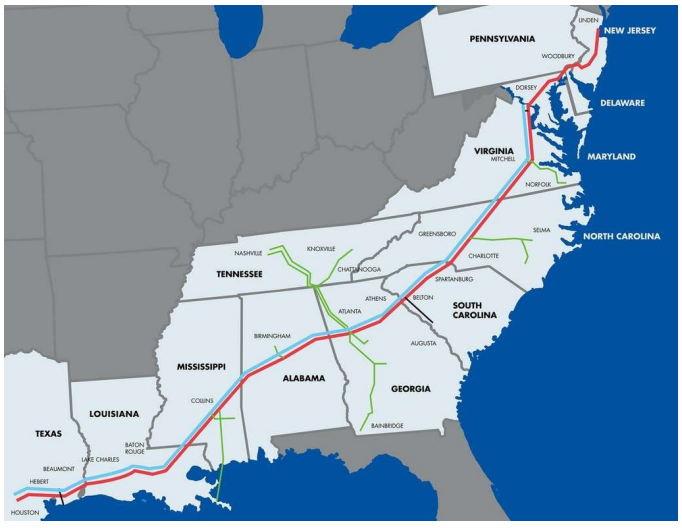
Pour les pirates informatiques, les établissements de soins représentent une cible de choix. Depuis plusieurs années les experts en cybersécurité veillent au grain pour surveiller ces lieux si sensibles. Une immense majorité des hôpitaux ne sont pas préparés à de telles attaques. Une grande partie des équipements est connectée à Internet, comme les équipements de radiologie par exemple.
Sans ces outils, les médecins ne sont pas capables de soigner leurs patients. Cette vulnérabilité incite les hackers à lancer des ransomwares contre les hôpitaux pensant qu'ils répondront très vite à leurs demandes de rançons. En France, le CHU de Rouen était par exemple victime d'un ransomware l'année dernière. 200 applications de son système informatique avaient été touchées. À l'époque, les patients qui n'étaient pas en situation d'urgence ont été orientés vers d'autres établissements, la prise en charge des patients, les prescriptions, et la gestion des admissions avaient également été perturbées.

De telles attaques peuvent semer une pagaille monstre en quelques minutes seulement. À Düsseldorf, les autorités allemandes ont ouvert une enquête sur la mort de cette femme. La presse allemande précise que si son transfert vers un autre hôpital s'avère être la cause de sa mort, les autorités pourront considérer que cette cyberattaque a causé le décès de cette patiente et pourront donc traiter cette affaire comme un homicide.

Source
Futura
Louis Neveu
9 mai 2021

6. États-Unis : une cyberattaque impacte un oléoduc et menace d'une pénurie de carburant

C'est la plus grosse cyberattaque contre une infrastructure américaine. Elle touche Colonial Pipeline, le plus gros opérateur d'oléoducs de distribution de carburant raffiné aux États-Unis. L'opérateur a dû couper ses lignes principales car ses systèmes sont neutralisés par un ransomware. Certaines régions pourraient connaître une pénurie de carburant.



Après la cyberattaque massive envers SolarWinds visant à mener des opérations de cyberespionnage, la prise de contrôle d'une infrastructure vitale, comme celle d'une unité de

traitement de l'eau, voici que ce sont maintenant les oléoducs de carburant aux États-Unis qui sont ciblés. Ces attaques ont toutes en commun de viser des secteurs stratégiques ou critiques. Cette fois, c'est le plus grand opérateur d'oléoducs, Colonial Pipeline qui a été victime des hackers. Ses 8800 km de conduites acheminent du carburant raffiné (essence, diesel, kérosène) sur tout le territoire américain. C'est cet opérateur qui fournit 45 % du carburant de la côte Est. Et cette fois, la cyberattaque a eu un impact massif immédiat puisque, lorsqu'elle a été identifiée, l'opérateur a mis hors service plusieurs services essentiels pour atténuer son ampleur. Il ne s'agissait pas cette fois de prendre le contrôle du dispositif ou d'espionner, mais sans doute de neutraliser les installations avec un ransomware qui a chiffré les systèmes de l'opérateur.

Une attaque en attente d'attribution

C'est, à ce jour, l'attaque directe la plus importante ciblant un secteur sensible des États-Unis. Elle pourrait engendrer une pénurie de carburant dans plusieurs États du centre et du sud-est du pays selon les déclarations d'un expert auprès de l'AFP. D'après lui, tout va dépendre de la durée de l'arrêt des systèmes. Si elle dépasse les cinq jours, la pénurie va toucher les stations-services et les aéroports régionaux. Cet arrêt commence déjà à avoir des répercutions sur les cours du pétrole en les augmentant. En attendant, Colonial Pipeline est en train de rouvrir ses canaux de distribution et exploite ses lignes secondaires pour remplacer les principales qui restent fermées.

Pour le moment, personne ne s'est encore aventuré à attribuer officiellement l'attaque. Selon les informations de Reuters, il s'agirait d'un groupe de hackers récent, mais très organisé appelé DarkSide. Ce groupe pratique la double extorsion avec une exfiltration des données, puis la menace de les rendre publiques. Sur ses autres attaques, DarkSide cherche habituellement à compromette le contrôleur de domaine, autrement dit, le centre névralgique du réseau. Ensuite, il se déplace dans le réseau avant de déclencher sa charge et de générer l'impact le plus large possible.

Il ne s'agirait donc pas de hackers liés à un État, alors que le mode opératoire par ransomware rappelle celui de NotPetya en 2017. Le ransomware ciblait l'économie ukrainienne pour l'affaiblir et avait touché de grandes entreprises françaises comme Saint-Gobain, Renault ou Auchan. Pour cette attaque, les regards se tournaient alors vers le Kremlin. Dans le cas de SolarWinds, le président Joe Biden a formellement attribué l'attaque aux Russes et a engagé des sanctions contre le pays.

Source
Le Temps
Anouch Seydtaghia
13 mai 2021

6.1. DarkSide, la PME du « ransomware » qui soigne son image

Le piratage de Colonial Pipeline a mis en lumière le modèle d'affaires des hackers de DarkSide, qui défendent une certaine éthique pour tenter de gagner la confiance de leurs… victimes.

Des automobilistes qui se ruent dans les stations-service, bidons en main. Un prix de l'essence au plus haut depuis 2014. Et même deux vols long-courriers d'American Airlines obligés, par manque de kérosène, d'ajouter une étape... Les conséquences du piratage d'oléoducs de la firme Colonial Pipeline a eu un impact très concret sur la côte est des États-Unis. Ce hacking a aussi mis en lumière les pratiques du groupe de pirates DarkSide, semblable à une PME du *ransomware* qui tient à soigner sa réputation.

Si l'approvisionnement en carburant devrait être rétabli en cette fin de semaine aux États-Unis, avec une remise en fonction progressive des installations de Colonial Pipeline, l'affaire risque d'avoir des conséquences à long terme pour DarkSide. C'est en tout cas ce que craint ce groupe, qui publiait en début de semaine ce message sur le darknet, sorte de réseau parallèle au web que nous utilisons : « Nous sommes apolitiques, nous ne participons pas au jeu géopolitique, n'essayez pas de nous lier à un gouvernement défini et à chercher d'autres motivations. Notre objectif est de faire de l'argent, et non de créer des problèmes pour la société. »

La défense d'une éthique

Ce communiqué est publié alors que les États-Unis accusent la Russie d'utiliser DarkSide à des fins de déstabilisation – ce qu'a immédiatement contesté Moscou. D'après de nombreux analystes, c'est l'implication du FBI dans l'enquête, au vu des enjeux majeurs en lien avec l'approvisionnement énergétique, qui a poussé les hackers à réagir. Désormais dans le viseur des autorités américaines, DarkSide veut faire profil bas. D'autant que dès son apparition, en août 2020, il a voulu défendre une certaine « éthique de travail » : pas d'attaque d'écoles, d'entreprises incapables de payer une rançon

ou d'établissement de santé. En octobre 2020, le groupe était allé jusqu'à annoncer des dons à deux ONG, The Water Project and Children International pour un montant de 20 000 dollars en bitcoins volés. Ces dons avaient été rejetés.

DarkSide a aussi levé le voile sur son modèle d'affaires, dans son communiqué : « A partir d'aujourd'hui, nous introduisons la modération et vérifions chaque entreprise que nos partenaires veulent attaquer pour éviter les conséquences « sociales » (sic) dans le futur. » Le groupe ne se contente pas de mener lui-même des attaques et d'en récolter les bénéfices sous forme de rançon ou de vol de données. Il loue aussi ses logiciels et prélève une commission (au pourcentage inconnu) sur les montants extorqués par d'autres hackers. C'est le modèle dit SAAS en jargon informatique, soit « software as a service ».

Une question de… confiance

Mais désormais, DarkSide doit faire attention. « Par le passé, [des groupes comme DarkSide] ont réussi à mener leurs activités sans que les gouvernements leur accordent une attention particulière, et aucune sanction n'a été imposée aux pays qui les hébergent, déclarait cette semaine Brett Callow, analyste auprès de la société de cybersécurité Emsisoft, au site spécialisé Quartz. Et cela pourrait être sur le point de changer. Cette attaque est d'une telle ampleur qu'elle ne peut vraiment pas rester sans réponse. »

Impossible de dire si DarkSide est proche du Kremlin. Impossible aussi de savoir si ce groupe a attaqué lui-même Colonial Pipeline, ou s'il s'agit de l'œuvre d'un sous-traitant. Une chose est sûre, pour les hackers, la réputation devient importante. C'est « une manière pour eux d'être identifiés comme un acteur sérieux, professionnel, et auquel on peut faire « confiance » lorsqu'on paie la rançon », estime Dmitry Galov, de la société de cybersécurité Kaspersky, cité par France 24. Les hackers, qui d'après les spécialistes exigent une rançon de 200 000 à 2 millions de dollars par attaque, voudraient ainsi garantir que le paiement de ces montants permet aux victimes de retrouver l'accès total à leurs machines. Car souvent, les entreprises piratées paient, mais ne récupèrent ensuite pas le contrôle de leurs ordinateurs.

Suisses touchés

Le business du *ransomware* semble en constante augmentation. Selon une étude publiée le mois dernier par la société de sécurité Sophos, 37 % des entreprises au niveau mondial ont été confrontées à ce fléau en 2020, avec une proportion allant jusqu'à 46 % en Suisse. Le montant le plus communément payé, sur la planète, serait d'environ 10 000 dollars, et la moyenne se situerait autour des 170 000 dollars. En Suisse, ces derniers mois, les entreprises Stadler Rail, Swatch Group, Meier Tobler ou encore Amag ont été touchées par un *ransomware*.

Source
Le Temps
Anouch Seydtaghia
14 mai 2021

6.2. Oléoduc piraté : les États-Unis auraient payé une rançon de 5 millions de dollars

Colonial Pipeline aurait accepté l'extorsion réclamée par le groupe de hackers russe DarkSide, selon des médias américains. Ce versement risque de créer un précédent pour toutes les attaques de « ransomware ».

C'est une nouvelle qui aura sans doute un impact considérable dans le monde du crime organisé sur internet. Colonial Pipeline aurait accepté de verser une rançon de 5 millions de dollars aux pirates du groupe DarkSide. C'est grâce à cela que ses oléoducs auraient été remis en service en cette fin de semaine. Paralysées par un *ransomware,* ses activités n'ont ainsi pu redémarrer que via un versement parti des États-Unis à destination de pirates suspectés d'être proches du pouvoir en Russie. Le piratage de l'oléoduc avait conduit à des pénuries d'essence sur la côte Est, ainsi qu'à des modifications de plans de vol d'avions d'American Airlines, obligés d'effectuer des escales supplémentaires.

Cette information, révélée tant par CNN que par Bloomberg, qui citent chacun deux sources proches du dossier, n'a pas été confirmée par Colonial Pipeline. Interrogé à ce sujet jeudi, le président américain, Joe Biden, n'a pas voulu faire de commentaires. Selon Bloomberg, l'entreprise gérant un immense réseau d'oléoducs a payé cette rançon avec une cryptomonnaie seulement quelques heures après l'attaque, survenue il y a près d'une semaine. L'objectif de Colonial Pipeline semble avoir été de restaurer ses activités le plus rapidement possible, et à n'importe quel prix.

Toujours selon le média américain, 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. Mais l'outil proposé était si lent à fonctionner que Colonial Pipeline a continué à utiliser ses propres sauvegardes pour aider à restaurer le système, toujours selon Bloomberg.

Message ambigu

La société, avec l'aide d'experts en cybersécurité du secteur privé et de représentants du gouvernement américain, a réussi à récupérer les données les plus importantes qui avaient été volées, selon CNN. Selon une source citée par le média américain, une partie des données n'a pas été récupérée auprès des pirates, mais en tirant parti de l'utilisation par les attaquants de serveurs intermédiaires aux États-Unis pour stocker les informations volées. Il y aurait donc eu, très tôt, une collaboration entre le secteur privé et les autorités.

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 lundi, Anne Neuberger, principale responsable de la cybersécurité à la Maison-Blanche, a refusé de dire si les entreprises devraient payer des cyberrançons lors d'un briefing en début de semaine : « 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 récupérer les données », a-t-elle déclaré lundi.

Mieux vaut payer…

De manière schématique, ce sont donc les États-Unis qui auraient versé cette rançon à la Russie, DarkSide étant très proche du Kremlin, selon des officiels américains. Moscou a nié ces accusations cette semaine. De son côté, DarkSide, qui loue ses logiciels de *ransomware* à d'autres groupes de pirates, a publié cette semaine un communiqué indiquant qu'il allait vérifier quel sous-traitant allait attaquer qui. Il est ainsi possible que ce ne soit pas directement DarkSide qui ait attaqué Colonial Pipeline, mais un plus petit groupe de hackers moins expérimenté, selon des médias américains.

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 Barracuda, 15 % des services municipaux visés aux États-Unis les mois précédents avaient accepté de payer des sommes allant de 45 000 à 250 000 dollars. « Toutes les municipalités étudiées qui ont effectué des paiements avaient une population inférieure à 50 000 habitants, et elles ont jugé que le coût et la main-d'œuvre associés à la récupération manuelle des attaques de *ransomware* étaient trop élevés », avait estimé la société californienne.

6.3. L'extorsion numérique, cette activité si ordinaire

Source
Le Temps
Anouch Seydtaghia
14 mai 2021

L'explosion du nombre de versements effectués après des attaques par «ransomwares» doit nous alerter : les agressions contre des infrastructures critiques vont se multiplier .

Bienvenue dans un nouveau monde. Un nouveau monde où hôpitaux, oléoducs et stations d'épuration sont devenus des cibles privilégiées des pirates informatiques. La paralysie du pipeline acheminant 45 % du carburant sur la côte Est des États-Unis était déjà un événement majeur en soi. Mais ce n'était rien par rapport à l'annonce du versement d'une rançon de 5 millions de dollars.

Cette tentative d'extorsion réussie a fait basculer le hacking par *ransomware* – ou rançongiciel – dans une nouvelle dimension. Ce type de piratage devient une activité (presque) comme une autre, un business avec ses règles et ses acteurs – les pirates informatiques –, qui tiennent à se montrer dignes de confiance pour être payés. En Suisse, de Swatch Group à Stadler Rail, des dizaines d'entreprises ont été attaquées ces derniers mois.

Que l'opérateur d'un oléoduc majeur aux États-Unis ait accepté de payer 5 millions à des hackers, malgré l'aide du FBI et de ses spécialistes, en dit long sur le degré de sophistication de ces attaques. Pour Colonial Pipeline, mieux valait payer plutôt que passer des semaines, voire des mois, à tenter de restaurer ses systèmes. Les hackers sont devenus des hommes d'affaires efficaces, en réussissant même, parfois, à proposer leurs logiciels d'attaque sous licence, et en récupérant des commissions lors de chaque piratage.

L'extorsion numérique est donc devenue une activité industrielle. Peut-être les pirates sont-ils en majorité Russes, comme l'affirment les Américains. Mais laissons de côté la guerre des mots entre Joe Biden et Vladimir Poutine. Ce qui compte, désormais, c'est de prendre conscience de la nécessité

de mieux protéger nos infrastructures critiques. Sans vouloir tomber dans le catastrophisme, il serait sans doute prudent pour les exploitants de lignes ferroviaires, de barrages, de compagnies aériennes ou de centrales nucléaires d'accroître leur niveau de sécurité. Car personne n'est désormais à l'abri de pirates devenus redoutables, qui gagnent de plus en plus d'argent grâce à toutes les attaques qui réussissent.

Mais nous avons la mémoire un peu courte. Souvenons-nous de WannaCry, le rançongiciel qui avait paralysé des centaines de milliers d'ordinateurs sur la planète il y a pile quatre ans. Cette attaque massive, lancée tous azimuts, aurait dû être un signal d'alarme pour qu'entreprises, administrations et particuliers protègent davantage leurs infrastructures. Manifestement, l'alerte n'a pas été assez entendue.

Source
Courrier International
5 juin 2021

7. La Corée du Nord et son armée de hackeurs de l'ombre

Pyongyang forme depuis plusieurs décennies des pirates informatiques de très haut niveau, chargés de missions d'espionnage, mais aussi de cyberattaques destinées à renflouer les caisses exsangues du pays.

"C'est à la fin des années 1990 que la Corée du Nord a commencé à faire parler d'elle pour ses capacités de hacking. *Tout a commencé quand le Bureau de la stratégie du Parti du travail [au pouvoir] a fait venir des spécialistes du décodage d'ex-URSS. En 1997, l'université Moran a vu le jour à Pyongyang et a accueilli une dizaine d'élèves parmi les meilleurs du pays. La première génération de hackeurs nord-coréens est née ainsi*", témoigne Joo Seong-ha, réfugié nord-coréen devenu journaliste auprès de **Dong-a Ilbo,** quotidien sud-coréen de la droite conservatrice.

D'après lui, depuis 2009, la gestion de ces ressources humaines d'un type quelque peu particulier relèverait de l'armée. Notamment de son Bureau général de reconnaissance, un service de renseignements sur lequel le dirigeant suprême du pays, Kim Jong-un, veillerait personnellement, avec un intérêt accru pour la cyberguerre. Le Bureau est régulièrement cité comme un organe qui supervise des groupes de hackeurs connus sous le nom de Lazarus ou APT38.

Les meilleurs informaticiens, donc des hackeurs potentiels, seraient formés, selon Joo Seong-ha, d'abord dans la section informatique d'une école d'élite de Pyongyang appelée Kumsong, puis à l'université Kim Il-sung ou à l'université de technologie Kim Chaek. Selon des réfugiés, l'université Mirim est également réputée enseigner la façon de neutraliser Windows et de fabriquer des virus, précise **Boan News,** journal sud-coréen en ligne spécialisé dans les questions de sécurité nationale.

Formés en Inde ou en Chine

La communauté internationale s'intéresse de plus en plus aux capacités de la Corée du Nord dans ce domaine. Celles-ci seraient cependant souvent "*exagérées*", écrit Joo Seong-ha en se fiant aux témoignages des informaticiens qui ont fui le pays. Alors que le ministère de la Défense sud-coréen estime le nombre de hackeurs nord-coréens à 6 800 dans son livre blanc de 2020, il précise que "*les hackeurs portant l'uniforme sont au nombre de 400 environ, dont une cinquantaine seulement de très haut niveau. On compte en effet beaucoup d'enfants de cadres pistonnés qui veulent profiter de ce tremplin pour entrer au parti".*

D'après Joo Seong-ha, l'histoire de la formation des meilleurs hackeurs nord-coréens – à laquelle la Corée du Sud a certainement contribué, bien malgré elle – ne manque pas d'épisodes cocasses. "*Entre 2002 et 2005, par l'intermédiaire de l'Unesco, la Corée du Sud a offert à la Corée du Nord un fonds pour la doter d'informaticiens. Une soixantaine de Nord-Coréens ont ainsi pu être formés en Inde",* raconte-t-il, toujours *au Dong-a Ilbo. "Par ailleurs, en 2000, Samsung Electronics s'est lancé dans la coopération intercoréenne et a créé à Pékin le Centre intercoréen du développement de logiciels, en collaboration avec le Centre nord-coréen de l'informatique, et y a investi 3,25 millions de dollars [environ 2,68 millions d'euros] jusqu'en 2004."*

Une équipe expulsée de Bulgarie en 2016

Des informaticiens et des hackeurs nord-coréens travailleraient à l'étranger "*avec la mission de rapporter des devises étrangères au régime en mal de ressources à cause des sanctions internationales*". Outre la Chine, la Malaisie aurait servi de base jusqu'à ce que, en 2017, Kuala Lumpur expulse les expatriés nord-coréens à la suite de l'assassinat de Kim Jong-nam, frère de Kim Jong-un. Une équipe d'informaticiens nord-coréens a également été expulsée de Bulgarie en 2016.

Seule la Chine continuerait à en accueillir – ils y seraient un millier aujourd'hui. L'institut de technologie de Harbin, en Chine, est par ailleurs cité par *Boan News* comme l'un des lieux de formation privilégiés pour les Nord-Coréens.

La justice américaine a inculpé en février trois Nord-Coréens accusés d'avoir mené plusieurs cyberattaques qui leur auraient rapporté au total 1,3 milliard de dollars (1,07 milliard d'euros). L'un d'entre eux, Pak Jin-hyok, avait déjà été inculpé en 2018 pour avoir été impliqué dans une cyberattaque en 2014 contre Sony Pictures, société vivement critiquée par Pyongyang pour avoir produit et diffusé *The Interview*, le film parodique sur l'assassinat du leader de la Corée du Nord. Les trois auraient agi entre 2015 et 2019 contre des banques et des entreprises situées au Vietnam, au Bangladesh, à Taïwan, au Mexique, à Malte, dans des pays africains, etc., afin d'obtenir de l'argent, mais aussi des informations sensibles. Par exemple, en mai 2017, ils auraient créé le rançongiciel WannaCry 2.0 et l'auraient utilisé pour extorquer 6,1 millions de dollars (environ 5 millions d'euros) à un établissement bancaire pakistanais. De telles inculpations auront-elles un effet ? Joo Seong-ha en doute. "*Sans la volonté de Pékin, nous ne serons jamais à l'abri des hackeurs nord-coréens.*"

Source
letemps.ch
Anouch Seydtaghia
30 mars 2022

8. Les données médicales de milliers de Neuchâtelois ont été mises en ligne

Les pirates qui avaient attaqué deux cabinets médicaux ont mis leur menace à exécution, révèle « Le Temps ». Jamais des données suisses d'une telle sensibilité n'avaient été publiées sur le darknet. Plusieurs spécialistes commentent ce piratage.

C'est une nouvelle étape franchie dans les cyberattaques qui ravagent la Suisse depuis des mois. Il y eut des données personnelles sur les habitants de Rolle et des employés de la commune en août 2021. Il y eut ensuite des déclarations d'impôts mises en ligne en novembre 2021 après le piratage d'une fiduciaire en Suisse alémanique. Aujourd'hui, ce sont des données encore plus sensibles qui ont été mises en ligne sur le darknet : des informations médicales personnelles.

Comme a pu le constater *Le Temps*, les pirates informatiques qui avaient attaqué deux cabinets médicaux dans le canton de Neuchâtel ont mis leur menace à exécution. Ce mardi, ils ont publié sur le darknet des données médicales sur des milliers d'habitants du canton. Les hackers avaient affirmé mi-mars que si leur demande de rançon n'était pas satisfaite, ils mettraient ces données en ligne le 29 mars. Et c'est ce qu'ils ont fait. Dans la journée de mercredi, ces données ont ensuite été retirées du darknet, sans que l'on puisse l'expliquer. Selon le compte à rebours affiché, elles pourraient être à nouveau publiées ce jeudi.

Détails sur les maladies

D'après nos investigations, ce sont au total 43 651 fichiers médicaux qui sont désormais disponibles sur le darknet, représentant plusieurs gigaoctets de données. Il y a au moins quatre fichiers contenant des listings de patients de ces deux cabinets situés dans les Montagnes neuchâteloises contenant des informations sur respectivement 994, 1207, 3259 et 4458 personnes. On y voit le nom des patients, leur adresse postale, leur date de naissance, leur numéro de téléphone (fixe et mobile), leur date de naissance et leur profession.

Ces informations sont visibles, mais il y en a aussi sur les examens médicaux effectués, les pathologies et les traitements. Ainsi, l'on constate qu'un patient est séropositif. Un autre est consommateur de drogue. Un troisième est dépressif suite à un accident. Des milliers de Neuchâtelois voient ainsi leurs données médicales intimes mises en ligne. Ce sont ainsi des dossiers médicaux complets qui ont été publiés, certains extrêmement récents, d'autres remontant jusqu'à 1998.

Des craintes en 2021

D'après ce que nous avons vu, aucune de ces informations n'est protégée : les données ne sont pas chiffrées et aucun fichier n'est verrouillé par un mot de passe.

L'un des deux cabinets piratés s'inquiétait justement, fin 2021, pour sa sécurité informatique, d'après ce que nous avons constaté. En septembre dernier, une responsable d'un cabinet écrit un e-mail à son prestataire informatique disant : « Depuis quelques mois nous nous questionnons sur la sécurité informatique dans notre cabinet », citant aussi le précédent de Rolle. Point par point, le prestataire informatique répond au cabinet médical concernant les bonnes pratiques à avoir, les

sauvegardes qui sont effectuées chaque soir, l'importance d'avoir des mots de passe robustes ou encore des logiciels de protection mis à jour.

Toujours dans cette correspondance, un élément datant de novembre 2021 indique que le risque d'un piratage avait été clairement identifié. On y lit ceci : « Le phishing représente le 90 % des hackings. Le risque est par exemple d'avoir un logiciel malveillant qui crypte les données. Ainsi, si on n'a pas de sauvegarde, on perdrait toutes les données, les hackers peuvent demander une rançon ou alors ils peuvent mettre les données sensibles sur le darkweb. Ex.: administration de Rolle. » Le pire était craint, et c'est ce qui s'est finalement produit.

Porte d'entrée

Mercredi, ni les cabinets médicaux touchés, ni la société de cybersécurité qui les assiste n'ont souhaité s'exprimer. Plusieurs plaintes ont été déposées auprès de la police neuchâteloise. Selon nos informations, la cyberattaque a pu être commise à cause d'un logiciel mal installé, qui aurait offert une porte d'entrée aux hackers. « Les cabinets médicaux ne protègent pas suffisamment leurs données, comme d'ailleurs la plupart des PME, estime Jean-Gabriel Jeannot, médecin à Neuchâtel et spécialiste des outils numériques. Mais le problème est probablement encore plus important avec les cabinets médicaux en raison de la valeur des données. Leur divulgation peut avoir des conséquences graves mais la perte de ces données, qui pourrait avoir des répercussions importantes sur la prise en charge médicale du patient, probablement encore plus. »

Que peuvent faire les patients ?

De nombreuses questions se posent. Les cabinets, qui savaient depuis des jours qu'ils avaient été piratés, auraient-ils dû en informer leurs patients ? « Il n'y a aujourd'hui pas d'obligation légale d'annoncer les violations de la sécurité aux personnes concernées. Une partie de la doctrine déduit néanmoins du principe général de la bonne foi une obligation d'informer dans des cas particuliers », répond Sylvain Métille, avocat et professeur en protection des données et droit pénal informatique à l'Université de Lausanne. La nouvelle loi sur la protection des données, qui doit entrer en vigueur le 1er septembre 2023, changera les choses. « Le préposé fédéral à la protection des données devra être informé de toute violation de la sécurité des données représentant un risque et les personnes concernées devront aussi l'être lorsque cela est nécessaire à la protection des personnes », poursuit Sylvain Métille.

Autre question brûlante : les patients lésés peuvent-ils attaquer les cabinets médicaux ? « Une action en responsabilité des patients est tout à fait envisageable et n'est pas seulement théorique. Pour que le cabinet médical soit condamné, il faudrait néanmoins prouver que des mesures suffisantes n'ont pas été prises et l'existence d'un dommage, qu'il s'agisse de dommages-intérêts ou d'un tort moral. Il faudra en plus démontrer un lien de causalité adéquate, c'est-à-dire que le dommage est survenu à cause de la négligence du cabinet médical », répond Sylvain Métille.

Des cibles trop faciles

Sans se prononcer sur ce cas précis, Sergio Alves Domingues, responsable technique de la société de cybersécurité SCRT, estime que «les attaques sont souvent causées par des mauvaises pratiques : logiciels pas à jour, failles non corrigées, absence d'authentification forte... Une bonne hygiène de sécurité permet de prévenir quantité d'attaques. De nombreuses attaques sont assez simples ». Selon le spécialiste, « bien sûr, la sécurité à 100 % n'existe pas. Mais toutes les entreprises peuvent augmenter fortement leur sécurité avec des actions simples. Mais malgré toutes ces attaques, certains ont l'impression que cela n'arrive qu'aux autres et qu'ils ne sont pas des cibles intéressantes. C'est faux : les pirates sont opportunistes et attaquent partout où l'occasion se présente ».

Source
letemps.ch
Anouch Seydtaghia
15 avril 2022

9. Données volées, le cauchemar d'une famille de Nyon

FICTION Les cyberattaques se multiplient en Suisse, nous touchant de plus en plus dans notre intimité. Mais le pire du pire n'est-il pas à venir ? Voici un récit-fiction de quelques jours d'une famille imaginaire de Nyon, dont la vie devient un enfer à la suite de multiples piratages.

La porte claqua violemment. Alice sursauta, manquant de renverser le verre d'eau posé à côté de son ordinateur. Elle soupira. Encore une soirée difficile en perspective avec sa fille. Depuis des semaines, Cléa rentrait d'humeur massacrante de l'école, s'enfermant immédiatement dans sa

chambre. « Moi aussi, quand j'avais 17 ans, j'étais une peste avec mes parents », sourit-elle. Elle se leva, toqua à la porte de la chambre de sa fille.

– Cléa, c'est moi. Tu as eu des soucis à l'école ? Viens, on va en parler.

– Laisse-moi, lâcha Cléa. Je ne veux pas te parler.

– Mais dis-moi, quel est le problème ?

– Non, laisse-moi tranquille.

Alice leva les yeux au ciel et retourna travailler à son bureau. Ce soir, elle laisserait son mari gérer son ado de fille. Elle avait assez donné à ce sujet ces derniers jours.

Une heure plus tard, Marc rentra.

– Bonsoir tout le monde ! Alors, que voulez-vous que je vous cuisine de bon pour ce soir ?

– Commence plutôt par voir ta fille, dit Alice.

– Ha ha, encore une crise d'ado ? rigola Marc.

D'un coup, Cléa ouvrit la porte de sa chambre.

– Ah oui, c'est moi l'ado ? Vraiment ?! Mais tu es trop nul ! Nul !, hurla Cléa, en lui tendant son téléphone.

Surpris, Marc attrapa nerveusement ses lunettes dans son blouson et plongea son regard de presbyte sur le smartphone de sa fille. Très vite, il blêmit. Sur l'écran, en grand, le logo de Pornhub, l'un des principaux sites X de la planète. Et juste à côté, son nom et son adresse e-mail, au milieu d'une liste sans fin égrainant les coordonnées de milliers d'autres personnes.

– Mais c'est quoi ce truc ? s'étouffa Marc. Et de toute façon, ce n'est pas moi, j'ai un nom commun, c'est un homonyme… Tu as trouvé ça où ?

Cléa s'assit, dépitée, le regard dans le vague.

– Ah oui, et ta date de naissance écrite à côté ? lâcha-t-elle.

Marc baissa les yeux. Il avait vaguement entendu parler, il y a quelques jours, du piratage de Pornhub et de la fuite de données. Mais il avait complètement oublié qu'il avait lui-même créé un compte il y a quelques années sur cette plateforme, pour accéder à des vidéos payantes. Il avait donné ses véritables coordonnées à Pornhub, y compris les informations pour sa carte de crédit. Mais comment sa fille est-elle tombée sur ces données ? Cléa ricana, Alice était consternée.

– C'est Rodrigo, le type dans ma classe qui va des fois sur le darknet. Il m'a dit que ça ne lui avait pris que quelques minutes pour retrouver les fichiers volés. Il a cherché des noms en Suisse et il t'a trouvé. Papa, c'est trop la honte pour moi à l'école…

Le soir, le souper se déroula dans une ambiance pesante. Une fois, puis deux fois, le téléphone fixe sonna. La troisième fois, excédé, Marc se leva et empoigna le combiné.

– Quoi ?!, hurla-t-il.

– Euh Marc, c'est Agathe, lui dit sa mère, un peu surprise. Écoute, j'ai un souci. J'ai perdu un peu d'argent je crois… Toi qui es dans la banque, tu pourrais m'aider, tu penses…?

Trois mois plus tôt, la commune de Payerne avait été victime d'une cyberattaque. Rien de grave, avait assuré le syndic, les hackers n'avaient réussi qu'à voler quelques fichiers sans importance. « Aucune donnée sensible n'a été exfiltrée, nous avons tout fait juste », avait-il promis. Seuls un fichier Excel contenant les coordonnées des habitants de la commune et quelques dossiers communaux avaient été dérobés. Habitant Payerne depuis vingt-quatre ans, Agathe avait ensuite lu le tout-ménage envoyé par la municipalité, ce qui l'avait rassurée.

– Marc, j'ai versé il y a quelques jours 1350 francs à une entreprise, enfin à des types louches, il me semble que c'était une arnaque, poursuivit Agathe. J'ai cru que c'étaient les services industriels de Payerne qui m'écrivaient des e-mails pour des factures impayées. Je trouvais bizarre qu'ils ne m'écrivent pas des lettres avec une facture, comme d'habitude… Mais ils semblaient savoir tant de

choses sur moi… Si je te transfère les e-mails, tu pourras récupérer l'argent ?

– Ah mais non, tu t'es fait avoir, soupira Marc, se souvenant du piratage de Payerne. Tu ne vas jamais revoir ton argent, maman, tu n'as pas été assez prudente, les pirates t'ont eu avec du *phishing*…

– Du quoi..?, répondit Agathe.

Epuisé, Marc raccrocha brutalement. « Enfin, je suis assez mal placé pour donner des conseils, moi…», pensa-t-il.

Le lendemain, Alice décida de retourner au bureau pour échapper à l'atmosphère électrique qui régnait chez elle. Arrivée dans les locaux de sa fiduciaire à Genève, elle fut surprise par l'accueil glacial reçu. « Alors, plutôt Maldives ou Seychelles pour les prochaines vacances ? », lui lança une collègue. « Dis donc, il t'aime bien le patron, non ? », renchérit un autre.

– Non, mais vous parlez de quoi ?, répondit Alice, désarçonnée.

– Ha ha excuse, Madame est bien au-dessus de tout ça, répondit une collaboratrice. Tiens, lis ça, ça pourrait t'intéresser.

Elle jeta un paquet de feuilles sur son bureau. Alice s'assit et lu. Face à elle, toutes les fiches de paye des 46 employés de sa fiduciaire sur les trois dernières années. Alice venait d'obtenir une augmentation importante fin 2021. Elle se savait beaucoup mieux payée que le reste de son équipe.

– Mais… mais comment c'est sorti tout ça ?, bredouilla-t-elle.

– Séance générale immédiatement dans la grande salle !, coupa sa cheffe en passant en trombe.

La fiduciaire venait de se faire pirater et toutes ses données avaient été mises en ligne. Les hackers avaient même poussé le vice jusqu'à envoyer le dossier « salaires » à tous les collaborateurs, en fichier compressé par e-mail.

– Nous avons joué avec les pirates et on a perdu, annonça la directrice. On a été attaqués hier soir, tout est allé très vite. Notre informatique a été paralysée, on n'avait accès à plus rien. Notre prestataire informatique m'a dit que nos sauvegardes étaient insuffisantes. Tout a été perdu. Les pirates nous ont réclamé une rançon de 250 000 francs, mais c'était beaucoup trop. On a tenté de négocier. Sans succès.

Les employés sont choqués, certains pleurent. Alice écoute, impassible. La directrice marque une pause, puis poursuit.

– Au milieu de la nuit, notre prestataire informatique nous a dit qu'il avait une solution. Alors on a envoyé balader les pirates. On pensait pouvoir récupérer rapidement les données. Mais ça n'a pas été le cas. Fâchés, les hackers ont publié les données de l'entreprise sur le darknet… et ont juste maintenu en fonction notre système de messagerie pour envoyer à tous la liste des salaires. Je suis désolée… Rentrez chez vous, on vous téléphonera quand vous pourrez à nouveau travailler…

Effondrée, Alice se dirige vers la gare. Mais son train n'arrive pas. Encore sous le choc de ce qu'elle vient d'entendre, elle regarde, hébétée, un employé des CFF qui l'aborde.

– Madame, vous vouliez prendre le train pour Nyon ? Alors désolé, mais les trains ne circulent plus, on a été victimes d'une cyberattaque, à ce qu'ont dit les chefs. Aucun train ne circule actuellement en Suisse, mais on va les remplacer par des bus. Attendez là, l'un d'eux va venir dans une heure ou deux.

Pendant ce temps, Marc prenait sa pause-café sur la terrasse de sa banque. « Mais quel idiot j'ai été avec PornHub, je suis vraiment un crétin », ruminait-il en ouvrant machinalement l'application LinkedIn sur son iPhone. « Étrange », se dit-il, en constatant que le mot de passe préenregistré n'était pas reconnu. Au bout de trois tentatives infructueuses, il ouvrit sa boîte e-mail privée. « Accès suspect à votre compte, veuillez vérifier vos paramètres de sécurité », lui avait écrit LinkedIn. Marc commença à transpirer.

– Encore un petit souci ?, rigola l'un de ses collègues.

– Je ne sais pas, LinkedIn n'est plus accessible, grommela Marc.

– Ah, c'est peut-être dû au *leak* de la semaine passée.

– Le quoi ?

– La fuite de données, il y a une immense base de données avec les mots de passe des utilisateurs qui se balade sur le Net. Tu as dû te faire piquer ton compte. Tu n'avais pas activé la double authentification ?

Non, trop paresseux, Marc ne l'avait jamais fait. Une fois ou deux, il avait songé à mieux protéger ses comptes en ligne en ajoutant l'envoi d'un code reçu par SMS au mot de passe traditionnel. Mais il ne l'avait jamais fait. « Ooops, d'ailleurs il me semble que j'ai le même mot de passe pour Netflix et LinkedIn », se dit-il.

Soudain, son téléphone se mit à sonner. « Bizarre, je ne connais pas ce numéro », se dit Marc. Il hésita, avant de décrocher.

– Bonjour, je suis le médecin de votre fille. Je n'arrive pas à la joindre sur son téléphone, alors je vous contacte vous. Je dois vous dire que…

– Oui oui ça va, interrompit sèchement Marc, elle est fâchée à cause de ma connerie sur Pornhub, c'est bon !

– Monsieur, je ne sais pas de quoi vous parlez, mais ce n'est pas ça, répondit calmement le médecin. Non, je me dois de vous dire, par correction, que nous avons un petit souci technique. Il semblerait que notre système informatique central ait subi récemment une intrusion. Et il est possible que le dossier médical de votre fille soit divulgué. Et comme elle m'a consulté récemment à deux reprises pour me parler d'un possible changement de sexe, je voulais que votre fille sache que cette information risque de se retrouver sur internet. Voilà, je lui enverrai un courrier standard pour l'informer directement. Bon après-midi.

Pour Marc, c'était trop. Il descendit à l'épicerie en bas de sa banque pour s'acheter une bouteille de vodka. Il but trois gorgées au goulot et observa, du trottoir, l'immeuble de sa banque. « Non, je ne peux pas y retourner cet après-midi, je rentre, ça suffit pour aujourd'hui », se dit-il en se dirigeant vers le parking.

Il s'approcha de sa Tesla et tira sur la poignée. Rien. « Ha ha, ma voiture est devenue trop intelligente, elle a déjà activé l'éthylomètre ! », pensa-t-il. Mais non. Impossible d'accéder à l'habitacle. Marc sortit le téléphone de sa poche, ouvrit l'app Tesla. « Trois messages d'erreur », soupira-t-il. « Suite à un incident de sécurité mineure, l'accès aux habitacles de nos voitures est momentanément impossible au niveau mondial. Nous regrettons cette indisponibilité et nous vous remercions pour votre confiance. »

De retour chez elle, Alice sirotait un Red Bull en lisant un livre de management. La sonnette retentit. « Ah, enfin une bonne nouvelle, ça doit être Antoine », se dit-elle. Elle ouvrit la porte et pris son fils dans les bras.

– Alors, c'était comment cette semaine à Madrid ?

– Trop cool maman. On a fait la fête presque tous les soirs. Je suis vanné.

– Tu n'as pas publié de photos sur Insta cette semaine, tu étais trop occupé pour en poster ?

– Euh non, je crois que j'ai eu un souci. Je n'arrive plus à accéder à mon compte depuis que j'ai été surfé sur le réseau wi-fi d'un Starbucks. Je ne sais pas trop ce qui s'est passé.

– Ah, mais tu n'as pas activé le VPN, comme je t'avais dit ?

– Non, j'ai oublié…

Alice prit le téléphone de son fils et l'examina. Des applications qui s'ouvraient moins vite que d'habitude, certaines qui activaient la localisation sans raison, Instagram inaccessible… Le téléphone d'Antoine avait certainement été piraté lorsqu'il avait utilisé ce réseau wi-fi non sécurisé et des hackers avaient injecté du code dans son téléphone pour en prendre le contrôle.

– Eh bien tu as du travail, soupira Alice. Ça tombe bien, il pleut. On dirait que ton téléphone a été hacké. Allez, toi qui crois être un crack de la tech, réinitialise ton smartphone et change tous tes mots

de passe, c'est plus prudent. Pour une fois que je te dis de passer des heures devant ton Android…

Après le souper, Alice s'installa sur le canapé et saisit son téléphone, passant de Snapchat à *Candy Crush* durant de longues minutes. Puis elle éclata de rire.

– Enfin un truc drôle ?, lui demanda Marc, d'un air fatigué.

– Pas pour elle, en tout cas, lui répondit Alice en lui tendant son téléphone.

Sur l'écran, une carte de Fribourg, avec une nuée de points dans le centre-ville et en périphérie. Depuis des semaines, des collègues d'Alice travaillant dans la succursale fribourgeoise s'agaçaient de l'attitude d'une collaboratrice, qui prenait jusqu'à trois heures de pause à midi. Pour en savoir plus, un collaborateur avait décidé de coller une balise d'Apple, un AirTag, derrière la plaque minéralogique de sa voiture. Et depuis, ses collègues pouvaient suivre à la trace ses déplacements à midi pour tenter de retracer ses activités.

– Euh, mais c'est légal ce que vous faites ?, demanda Marc, amusé.

– Je ne sais pas, sourit Alice. Sans doute pas. Mais on s'en fiche un peu, du moment qu'Apple nous permet de suivre quelqu'un sur nos téléphones, pourquoi s'en priver ? Et puis de toute façon, c'est pour la bonne cause, on se demande bien ce que fait cette cruche durant ses pauses de midi.

Le lendemain matin, à l'heure du petit-déjeuner, Alice s'impatienta.

– Antoine, viens, tu vas être en retard pour l'école. Et tu as un test de math aujourd'hui, je te rappelle.

– Attends, j'arrive, je regarde juste un truc, répondit son fils à travers la porte de sa chambre.

Allongé sur son lit, Antoine regardait une vidéo sur son ordinateur, sa sœur à côté de lui.

– Vous faites quoi ?, leur demanda Alice.

Sans quitter l'écran des yeux, Cléa lui répondit. Rodrigo, son copain de classe, était parvenu à mettre la main sur des flux de webcams d'Amazon. Trois semaines plus tôt, le géant américain avait reconnu l'existence d'une faille de sécurité dans sa caméra de surveillance, pressant ses utilisateurs de mettre immédiatement à jour leur logiciel. Le risque était élevé que des hackers prennent le contrôle de ces webcams et accèdent à des enregistrements vidéo.

– Ha ha maman regarde, on peut voir dans l'appartement de Monsieur Richard, notre prof de philo. Il nous avait dit tout fier qu'il utilisait des webcams pour surveiller son chien, mais il en a même mis dans sa chambre à coucher. C'est chaud !, pouffa Antoine.

Alice soupira et retourna à la cuisine pour y finir son café. Elle regarda son chat, qui rentrait, l'air satisfait, d'un tour à l'extérieur. « Prépare-toi Caramel, à cause de ton collier GPS, tu seras sans doute le prochain à te faire pirater », sourit-elle.

Source
Le big data
Bastien L
22 août 2019

10. Fuite de données : que peuvent faire les hackers de vos informations ?

Quels sont les risques que vous encourez en cas de fuite de vos données personnelles ? Découvrez tout ce que les hackers peuvent faire avec vos différentes informations.

Les fuites de données sont de plus en plus nombreuses et massives. La plupart du temps, toutefois, si les informations liées à leurs coordonnées bancaires ne sont pas compromises, les victimes tendent à relativiser la gravité de la situation.

Pourtant, en réalité, la fuite d'autres types de données personnelles peut avoir des conséquences tout aussi fâcheuses. Découvrez, de façon concrète, ce que peuvent faire les hackers en mettant la main sur vos informations personnelles.

Les informations personnelles identifiables, plus communément appelées « données personnelles », sont les données pouvant être utilisées pour identifier, localiser ou contacter un individu spécifique. En guise d'exemples, on peut citer le nom, la date de naissance, l'adresse, le numéro de sécurité sociale, le numéro de téléphone ou toute autre donnée permettant de distinguer

ou d'identifier un individu.

Ces informations sont les plus fréquemment compromises lors de fuites de données. Une fois obtenues, les cybercriminels peuvent s'en servir de multiples façons. Avec suffisamment de données, il est par exemple possible d'emprunter de l'argent ou de prendre une carte de crédit au nom de la victime. Les informations personnelles identifiables peuvent aussi être vendues à des entreprises qui les utiliseront à des fins de ciblage publicitaire. Bien souvent, ces données se retrouvent aussi en vente libre sur le Dark Web...

Les données financières

Les informations financières sont les données liées aux activités financières d'une personne. Il s'agit par exemple des coordonnées bancaires, des informations d'assurance ou toutes autres données pouvant être utilisées pour accéder à des comptes ou effectuer des transactions financières.

Le vol de ces informations peut avoir des conséquences terribles. Un cybercriminel peut les utiliser pour payer ses factures, effectuer des transactions en ligne frauduleuses, ou tout simplement se servir dans le compte bancaire de la victime. Les criminels organisés peuvent aller jusqu'à créer des cartes de crédit contrefaites à partir de ces données.

Les numéros de carte bancaire

Dans la veine des informations financières, les numéros de carte bancaire sont le numéro, la date d'expiration ou encore le numéro de sécurité présents sur les cartes de crédit et de débit.

Comme vous le savez sans doute, si une personne met la main sur ces données, elle peut les utiliser immédiatement pour effectuer des achats ou des transactions en ligne. Il est donc impératif de surveiller que les sites sur lesquels vous les utilisez sont totalement sécurisés, et d'ajouter une sécurité supplémentaire à l'utilisation de votre carte bancaire comme l'authentification à deux facteurs.

Les données de santé

Les données de santé sont celles utilisées par un individu pour accéder aux services médicaux tels que les séjours à l'hôpital ou l'assurance médicale. Tout comme les données personnelles, ces informations peuvent permettre d'identifier très facilement une personne.

Par ailleurs, les données de santé peuvent être utilisées par un criminel pour acheter des médicaments délivrés uniquement sous ordonnance. Elles sont donc particulièrement convoitées par certains toxicomanes.

Les données d'éducation

Les données d'éducation sont celles qui relatent le parcours scolaire d'une personne telles que ses diplômes ou ses résultats. En cas de fuite, ces informations peuvent être utilisées à des fins de chantage ou d'extorsion.

Elles seront alors utilisées pour faire pression sur la victime afin d'obtenir ce que l'on veut d'elle. En outre, les cybercriminels peuvent utiliser ces données pour effectuer des attaques de type phishing en se faisant passer pour des étudiants ou des représentants d'une institution.

Les identifiants de sites web

Les identifiants de sites web sont les noms d'utilisateurs, adresses email et mots de passe que vous utilisez pour vous connecter aux différents sites web et autres applications mobiles. Si un cybercriminel s'en empare, il pourra se connecter à votre compte sur tous les sites où vous les utiliser.

Le pire qui puisse vous arriver est la compromission d'une adresse email, car les différents sites web vérifient généralement l'identité d'un utilisateur en lui envoyant un mail de confirmation. Ainsi, un criminel qui s'en empare pourra même changer vos mots de passe sur les différents services que vous utilisez.

En outre, les comptes de réseaux sociaux et les adresses email peuvent être utilisés pour orchestrer des attaques de phishing ou des spams publicitaires. Certains criminels peuvent aussi s'en servir pour vous espionner, ou pour voler la propriété intellectuelle de votre entreprise.

Les numéros de sécurité sociale

Il n'est pas rare que des numéros de sécurité sociale soient compromis lors d'une fuite de

données. C'est notamment ce qui s'est passé, récemment, lors du Data Leak de la banque américaine Capital One. On estime que 140'000 numéros de sécurité sociale ont été compromis lors de cet incident.

Or, en s'emparant de votre numéro de sécurité sociale, les cybercriminels peuvent éventuellement profiter de services publics à votre place. La tâche sera plus aisée pour les hackers aux États-Unis et au Canada ou le numéro d'assurance sociale (NAS) fait figure de sésame pour tous les programmes et services gouvernementaux, mais c'est aussi possible en France et dans les autres pays d'Europe.

Au Canada, un NAS valide peut permettre à un usurpateur d'identité d'obtenir un emploi à votre nom. Ainsi, le criminel pourra recevoir un salaire... mais c'est vous qui payerez les impôts pour lui ! Il est aussi possible de combiner une identité volée avec de fausses déclarations fiscales pour profiter d'avantages sociaux tels que des chèques de remboursement.

Toujours en Amérique, notamment aux États-Unis, il est possible d'utiliser les données d'autrui pour profiter de soins médicaux à ses frais. Un tel usage peut avoir des conséquences encore plus néfastes, puisque le malfaiteur risque d'ajouter ses propres données de santé à votre dossier médical !

Une identité usurpée peut également permettre à un criminel de vous faire porter le chapeau pour ses méfaits. Vous pourriez ainsi vous retrouver accusé d'infractions au Code de la route ou autres infractions sans même le savoir...

Le numéro de téléphone

Si un cybercriminel parvient à mettre la main sur votre numéro de téléphone et à s'octroyer une carte SIM, il sera capable de surveiller tous les appels et messages textuels que vous recevez.

De plus, il convient de rappeler que le téléphone est souvent utilisé pour l'authentification à deux facteurs. Ainsi, les malfaiteurs seront en mesure d'accéder à vos comptes sur d'autres services tels que votre compte bancaire via la plateforme en ligne de votre banque ! Il ne lui restera plus alors qu'à réinitialiser votre mot de passe pour pouvoir vider votre compte en toute quiétude.