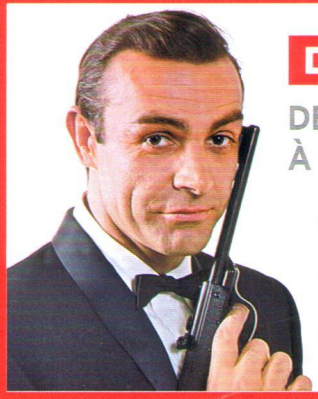
Septembre 2016
N°427
3,90 €

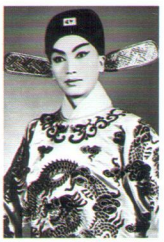
ça M'INTÉRESSE

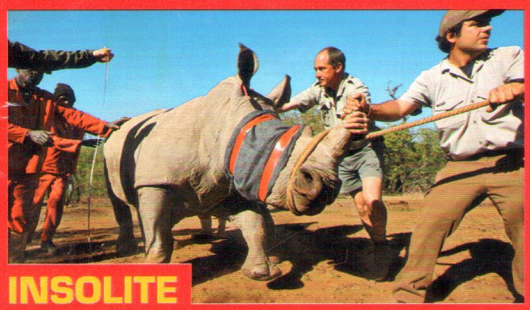


DOSSIER SPÉCIAL

DE IAN FLEMING
À JOSÉPHINE BAKER

15 HISTOIRES D'ESPIONNAGE ROCAMBOLESQUES





INSOLITE
Dans ces fermes, on élève des rhinos pour leurs cornes

ENQUÊTE
Énergie solaire, éolien, géothermie... Pourquoi la France est à la traîne

ÉCONOMIE
Combien rapporte une vigne bio dans le Sud-Ouest ?

Ostéopathie, réflexologie, shiatsu...

LA SANTÉ PAR LE TOUCHER

STIMULER LE CERVEAU,
RÉDUIRE LE STRESS,
VAINCRE LA DOULEUR...

BANC D'ESSAI
12 TECHNIQUES À LA LOUPE

www.caminteresse.fr

PRISMA MEDIA
M 01237 - 427 - F: 3,90 € - RD

BEL : 4,40 € – CH : 8 CHF - CAN : 7,50 CAD – D : 5,50 € - ESP : 4,50 € - GR : 4,50 € - ITA : 4,50 € – LUX : 4,40 € – PORT.CONT. : 4,50 € – DOM : Avion : 5,80 € ; Surface : 4,30 € – GUYANE : 7 € - MAY : 8.50€ - Maroc : 40 DH – Tunisie : 4.8 TND – Zone CFA Avion : 4 500 XAF ; Bateau : 3 500 XAF – Zone CFP Avion : 1 400 XPF ; Bateau : 700 XPF.

EN FÉVRIER, LA BANQUE CENTRALE DU BANGLADESH A PERDU 71,5 MILLIONS

HACKERS De quoi sont-ils

Dans notre monde ultra-connecté, le pouvoir de ces pirates informatiques s'étend. Et la marge entre fiction et réalité se resserre.

Texte Sébastien Porte
Illustrations Antoine Levesque

Cette nuit-là, dans la centrale de Chai Wan, à Hong Kong, tout a l'air sous contrôle. Les ingénieurs surveillent d'un œil tranquille les cadrans dans la salle des réacteurs. Quelque part ailleurs, un homme saisit un code sur son PC et appuie sur la touche *enter*. Il vient de lâcher un virus malveillant qui commence alors sa course folle. À l'échelle du nanomètre, on le voit filer le long de câbles puis entrer dans le système de refroidissement de la centrale, provoquant une fissure dans un caisson et faisant exploser le cœur du réacteur. Cette attaque d'une violence inouïe n'est heureusement qu'une fiction. C'est la scène d'ouverture du film *Hacker*, de Michael Mann (2015). Dans la vie réelle, jusqu'où les hackers peuvent-ils aller ? Surtout les *black hats* (« les chapeaux noirs »), ceux qui cherchent à voler de l'argent ou à déstabiliser des industries ou des institutions en faisant fuiter des données (comme dans le piratage de Sony Pictures, fin 2014, attribué à la Corée du Nord).

En une journée, 20 incidents de sécurité touchent les entreprises

Face à ce risque, les administrations et les entreprises s'organisent. La France a ainsi créé en 2009 une agence, l'Anssi (Agence nationale de la sécurité des systèmes d'information), qui les aide à se protéger. « Les compétences des hackers peuvent être achetées par n'importe qui sur le *dark net* [un réseau Internet parallèle, sans législation, ndlr] », rappelle Philippe Trouchaud, auteur de *Cybersécurité, au-delà de la technologie* (éd. Odile Jacob). « Mais les moyens humains et financiers pour les contrer restent faibles. Les entreprises subissent en moyenne 20 incidents de sécurité par jour, dont 70 % pourraient être évités avec des mots de passe plus solides ou par une mise à jour des systèmes. » ■

Bloquer une voiture à distance

OUI Télépéage, wi-fi, GPS, caméras, etc., nos voitures sont de plus en plus connectées avec l'extérieur. Tous ces gadgets sont autant de portes d'entrée possibles pour les cybercriminels. Entre 2010 et 2014, le nombre de points de vulnérabilité logicielle sur les véhicules serait passé de 4 258 à 7 038. L'an dernier, avec un simple ordinateur, des chercheurs américains ont pu agir à 10 km de distance sur les essuie-glaces, la climatisation, mais aussi la direction et la vitesse d'une Jeep Cherokee qui roulait. Ils s'étaient infiltrés sur Uconnect, l'ordinateur embarqué du véhicule, *via* son adresse IP. D'autres, en Allemagne, se sont amusés à ouvrir à distance les portières d'un millier de BMW. Pire encore, des experts ont fait la démonstration que l'on pouvait forcer une voiture à foncer contre un mur, malgré son radar anticollision. « Le "véhicule étendu" permet d'effectuer des diagnostics à distance et d'anticiper les pannes grâce à un serveur où transitent les données de la voiture, explique Amar Cheballah, consultant indépendant. Ces modèles ne représentent encore que 3 à 4 % du parc, mais ils vont se généraliser à partir de 2020. Or, dès que l'on est capable d'interroger à distance les calculateurs un par un, on est capable de les reprogrammer. Un hacker pourra donc entrer dans le système central du véhicule et en faire un engin de mort. » Qu'adviendrait-il si un *black hat* piratait un semi-remorque rempli de carburant ? Le rêve de la voiture « intelligente », qui conduit seule, pourrait virer au cauchemar.

D'EUROS À CAUSE D'UNE CYBERATTAQUE

vraiment capables ?

En juin dernier, d'après le journal *Libération*, la banque BNP-Paribas cherchait à recruter un pirate informatique éthique pour tester son propre système.

Contrôler les écrans d'une ville

DIFFICILEMENT

Pirater les messages des panneaux de signalisation routière serait un jeu d'enfant. Facile aussi, pour un bidouilleur doué, de s'inviter sur une pub numérique. Certains l'ont fait sur Times Square, à New York, en approchant des écrans un émetteur branché sur smartphone. D'autres ont remplacé le logo d'un soda sur la place de Brouckère, à Bruxelles, par une tête de troll. En revanche, hacker en même temps tous les écrans d'un réseau est une autre paire de manches. « Nous avons mis en place plusieurs barrières », explique Norbert Maire, de Media Transports, la société qui gère les publicités numériques dans les gares et le métro à Paris. « Le logiciel utilisé pour transmettre nos images est développé en interne avec plusieurs langages. En plus, nous empruntons une portion du réseau RATP qui est une boucle très haut débit extrêmement sécurisée pour faire face au risque terroriste. Il faudrait que le hacker soit quelqu'un de chez nous, qui connaisse nos logiciels. Il serait obligé de placer un fichier sur notre serveur central avant de donner l'ordre d'attaquer la RATP, puis les gares. » Impossible aussi de parasiter les écrans à distance, comme à Times Square, car ils ne sont pas reliés à la 3G ou à la 4G : « Le réseau ressemble plutôt à un gros intranet », précise Norbert Maire. La seule manière, c'est de se brancher à l'arrière des écrans, « sur le port USB destiné à la maintenance ». Mais avec 1 500 dispositifs à Paris, la tâche est titanesque.

Pirater les données d'un hôpital

OUI Imaginez un laboratoire qui voudrait lancer un médicament contre le diabète, et qui réussirait à mettre la main sur une cartographie listant les coordonnées des diabétiques de France. Un tel document lui permettrait de réaliser des bénéfices considérables ! Voilà pourquoi les hôpitaux sont devenus des cibles prisées des hackers. Ils viennent piller des données sur les patients qu'ils revendent ensuite sur le *dark net*, ce marché en ligne illégal où s'échangent aussi bien de la cocaïne que des armes ou des images pédophiles. « C'est le quartier chaud d'Internet, résume Vincent Trély, fondateur de l'Apssis (Association pour la promotion de la sécurité des systèmes d'information de santé). Un dossier médical s'y vend entre 30 et 200 $. » Les établissements de santé français auraient essuyé 1 300 incidents de sécurité en 2015, dont une quarantaine d'intrusions malveillantes sophistiquées. Le but ? La revente de fichiers, mais aussi l'espionnage, voire le chantage. C'est ce qui est arrivé à Labio, un laboratoire de biologie qui s'est fait siphonner des centaines de bilans et d'analyses sanguines : les cyberescrocs exigeaient 20 000 € de rançon en échange de leur non-publication. Le labo n'a pas cédé. Reste que, dans un milieu où l'informatisation a explosé, des efforts considérables sont à accomplir pour sensibiliser le personnel aux bonnes pratiques. « Quand vous êtes dans un service d'urgence, avec trois ordinateurs pour 80 personnes, les médecins ne comprennent pas qu'il faille perdre dix minutes à utiliser une carte sécurisée », déplore Vincent Trély.

Provoquer un crash

DIFFICILEMENT Dans le transport aérien, aucun scénario n'est écarté, même les pires. Exemple : un passager qui réussit à modifier la poussée des réacteurs en s'immisçant *via* la console de divertissement, comme l'ingénieur Chris Roberts a déclaré l'avoir fait l'an dernier. « En réalité, Roberts s'était branché sur un boîtier sous le siège avec un câble bricolé », corrige Jean Carlioz, responsable cybersécurité à la DGAC (Direction générale de l'aviation civile). « Rien ne prouve qu'il ait agi sur les commandes. Son mérite est d'avoir montré que le système opérationnel et le système de divertissement en cabine pouvaient être connectés. » Le défaut aurait été corrigé sur les Boeing et sur les Airbus A350 et A380. « Mais on n'est pas sûr que le lien ait été sécurisé sur 100 % des appareils », admet le spécialiste. Autre hypothèse : un pirate au sol réussit à s'insérer sur les fréquences radio entre l'avion et la tour de contrôle. La DGAC reconnaît qu'il n'y a pas de risque zéro : « Le cas s'est déjà produit il y a dix ans, avec un individu qui connaissait le vocabulaire. Le pilote a compris que quelque chose clochait et a repris la main. Sans voix, il y a d'autres moyens d'établir le contact. Et les pilotes sont formés pour atterrir à vue. » Y compris de nuit ? « Il faudrait qu'une organisation brouille les contacts radio, l'imagerie radar, coupe l'alimentation de l'éclairage des pistes... » Un scénario qui reste plausible, en théorie. Mais peu probable dans la réalité.

Dévaliser un compte bancaire

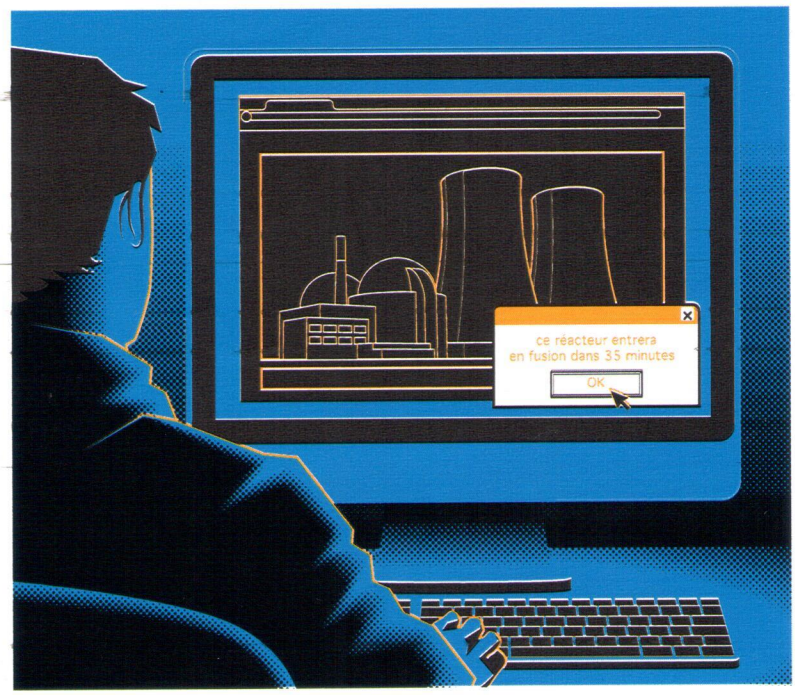
OUI C'est un classique. Les Arsène Lupin du Net profitent des failles de certains sites marchands pour aspirer des listes entières de numéros de cartes bleues, avec codes secrets, dates d'expiration… Bref, le kit nécessaire pour vider votre compte à votre insu. Soit ils les utilisent pour effectuer des achats en ligne (et se font livrer incognito à des points relais). Soit ils les revendent par paquets de dix sur des forums privés. « Le plus ravageur, c'est quand ils s'introduisent directement sur le compte de nos clients et font des virements à l'extérieur », confie un banquier, responsable de quinze agences dans un important groupe français, qui reconnaît que sa clientèle est régulièrement victime d'attaques. « Les hackers prennent la main à distance sur les ordinateurs, et il est très difficile de les neutraliser. »

Quelles parades alors adopter ? La banque peut demander au client de valider les virements par SMS. Sauf que, souvent, le hacker possède le numéro de téléphone de sa victime, et peut donc valider à sa place. Au final, le client ne s'en tire pas si mal : « On rembourse toujours », avoue le banquier. Une charge qu'il compare à celles que supportaient les banques « à l'époque où il y avait des hold-up ».

Prendre le contrôle d'une centrale nucléaire

IMPOSSIBLE DE SAVOIR

« On est ici dans un axe de cyberguerre », explique un club d'experts en cybersécurité. D'où l'extrême difficulté à récolter des infos sur ce type de risque. Du côté d'EDF, qui exploite les 19 centrales nucléaires françaises, le discours se veut rassurant : « Les systèmes numériques de pilotage de la centrale ne sont à aucun moment connectés avec les réseaux extérieurs comme Internet. De plus, à tout moment, les agents en salle de commande peuvent arrêter la réaction nucléaire. » Mais d'après l'institut britannique Chatham House, cette prétendue isolation des circuits d'information dans le nucléaire relèverait du mythe. Une enquête publiée en 2015, portant sur sept pays, dont la France, s'inquiète du risque croissant d'une cyberattaque sérieuse. Selon elle, Internet serait entré dans les centrales *via* les VPN (réseaux virtuels privés). Qu'en est-il de cette porosité dans les centrales françaises ? « On ne souhaite pas parler d'un secteur en particulier pour ne pas donner d'informations à des attaquants potentiels », élude l'Anssi. Elle nous explique juste que le nucléaire relève du champ des opérateurs d'importance vitale (OIV), rassemblant plus de 200 entreprises, dont la liste est tenue secrète, et, qu'à ce titre, la loi leur impose de renforcer leurs règles en matière de cybersécurité. Pendant ce temps, les virus comme le célèbre Stuxnet, forgé dans les années 2000 par Israël et les États-Unis pour nuire au nucléaire iranien, continuent de se propager dans le monde. Et les hackers s'en inspirent pour tailler de nouvelles armes, toujours plus intrusives.



Plonger une ville dans le noir

OUI La ville intelligente, ou *smart city*, est le nouveau concept à la mode. Et comme toute technologie naissante, c'est une proie facile pour les hackers. À Nice par exemple, qui se veut pionnière en la matière, lampadaires, bancs, poubelles et trottoirs sont bardés de capteurs, ce qui permet de moduler l'éclairage public en fonction des besoins ou d'envoyer les éboueurs avant que les ordures débordent des poubelles. Les automobilistes peuvent aussi consulter en temps réel, sur leur smartphone, les places de parking disponibles, et payer à distance. Moderne, mais non sans risques : un an après l'inauguration, en juin 2013, de leur premier boulevard connecté, un hacker a révélé aux Niçois qu'il a réussi à éteindre les réverbères et à pirater le système de stationnement. En cause : des données non cryptées et sans certificat d'authentification transmises par wi-fi. Mais au-delà de ces nuisances ponctuelles, la question qui se pose est celle de l'extinction généralisée. Un scénario pris au sérieux par de nombreux États, dont la France. Le concept de *smart city* repose effectivement sur celui de *smart grid* (un réseau unifié où les infrastructures électriques s'échangent une masse de données chiffrées) depuis les sites de production jusqu'au très contesté compteur intelligent Linky, en cours de déploiement. Le piratage d'un seul compteur pourrait même entraîner la paralysie de tout un quartier… « Le nombre d'objets interconnectés va croissant et concerne une grande majorité des équipements nouveaux dans les villes », analyse Yves Jussot, de l'Anssi. « Or, plus la surface de vulnérabilité est importante, plus il est facile pour un hacker d'attaquer. »