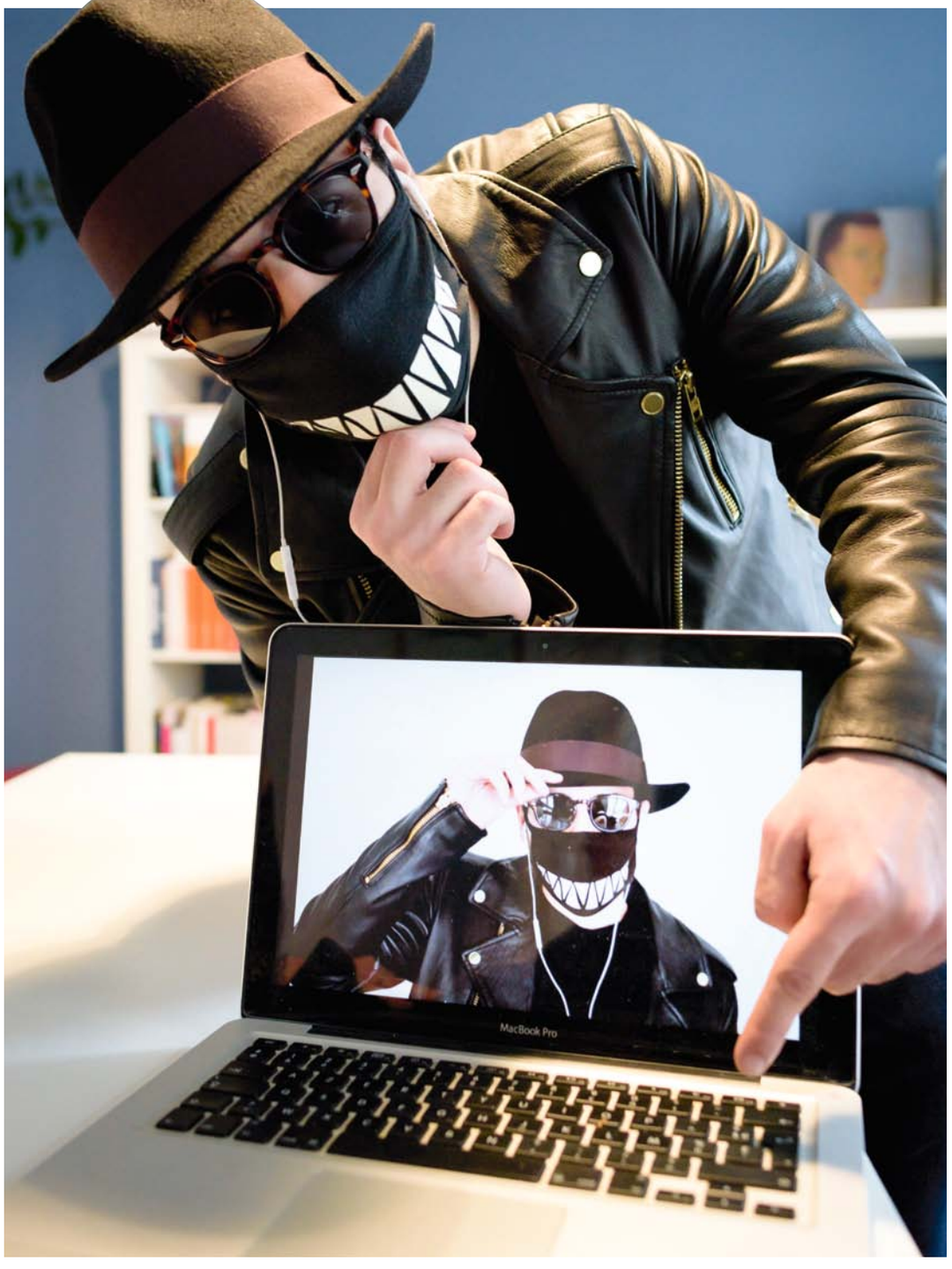
matchdocument



LES CONFESSIONS D'UN HACKEUR

Il se fait appeler « Rabbin des bois ». C'est l'un des pirates français les plus renommés sur le Net.

Il a « craqué » les sites des plus grandes entreprises, des plus grandes écoles, et s'est fait pas mal d'argent. Mais son rêve, c'était d'intégrer l'Ena pour devenir président. Brillant, voire génial, ce jeune homme de 23 ans nous a reçus, masqué, et casse nos dernières illusions sur une quelconque protection possible des données. Amer sur notre système élitiste et se présentant néanmoins comme un lanceur d'alerte, il publie aujourd'hui un livre. Son témoignage donne des frissons.

PAR **MARIANA GRÉPINET**
PHOTOS **PHILIPPE PETIT**

Le Cyberlab de Thales qui forme les équipes des clients du groupe et où sont testés leurs réseaux pour en détecter les failles.

S'il était identifié, ses confessions pourraient l'envoyer à l'ombre pendant quelques années. Alors le jeune homme, arrivé avec une heure de retard, se confond en excuses mais se montre prudent. Pendant les trois heures passées avec lui, il ne quittera pas le masque de tissu qui lui couvre le nez et la bouche. Tout de noir vêtu, il fait presque peur. Mais sa voix trahit sa fébrilité. Et sa fierté d'être écouté. Il parle vite, trop vite. Mais se montre pédagogue, quitte à rappeler ce qui semble, pour lui, des évidences. On le sent sûr de ses capacités intellectuelles, de ses analyses, et fragile à la fois. « J'étais un enfant solitaire et très triste aussi », glisse-t-il. Il finira pas admettre qu'il l'est resté.

Il a, dit-il, essayé pendant des années de s'intégrer dans notre monde. « Mais il n'est pas honnête, pas juste et surtout pas rentable. »

Il emprunte le vocabulaire de la saga Harry Potter pour nous désigner, nous qui sommes éloignés de la magie du numérique, comme des « moldus ». A tendance à exagérer : « Dans votre vie, j'ai envie de me défenestrer à cause de l'administration, je ne sais pas comment vous faites, la Caf, les trucs, les machins… » Ce Rabbin des bois, qui admire « le légendaire et mythique Robin des bois », est croyant, juif, comme son pseudonyme le laissait présager. « C'est une histoire d'assimilation et d'adaptation mais pas une revendication », assure-t-il. Il se passionne pour la politique – il rêvait d'être président ! – mais refuse de dire pour qui il a voté à la présidentielle. On devine qu'il s'agit de Macron. Lorsque ce dernier était encore ministre, il l'avait contacté, persuadé qu'il serait candidat, pour lui donner « deux ou trois idées ». Il avait fini par correspondre, juste une fois, avec son bras droit, Ismaël Emelien. Sur Internet, toutes les barrières sont abolies.

Paris Match. Comment avez-vous commencé ?

Rabbin des bois. Ma mère est morte quand j'avais 13 ans, des suites d'une longue maladie. Je me suis retrouvé seul avec mon père, dans une tour HLM de Chevilly-Larue, en banlieue parisienne. J'ai réalisé que j'étais pauvre et que j'avais perdu toute foi dans le système. Je me suis replié sur moi-même et l'écran est devenu un refuge… J'y passais mes journées.

Pour jouer et pour gagner de l'argent, vous montez vos premières arnaques…

C'était en 2010, grâce au service de paiement en ligne PayPal. Je postais des annonces sur Leboncoin ou eBay pour vendre un iPhone ou un iPad que je n'avais pas et, quand quelqu'un mordait à l'hameçon et envoyait son paiement sur le compte indiqué, je faisais basculer cette somme vers d'autres comptes. PayPal indemnisait la victime et revendait sa dette à une société d'assurances qui tentait de nous retrouver. En vain. Avec mon copain, ça nous rapportait 1 200 euros par mois. On a arrêté lorsque cela n'a plus fonctionné. Plus que voler, j'aimais trouver la faille dans le système. Après, j'ai découvert plus rentable.

Quoi par exemple ?

BlackBerry venait de lancer sa première tablette tactile, le BlackBerry PlayBook, pour essayer de concurrencer l'iPad d'Apple. Sans avoir moi-même de tablette, j'arrivais à m'en faire livrer une gratuitement en faisant croire au service client que la mienne était défectueuse, et je la revendais ensuite. Puis j'ai réalisé que ça pouvait produire de l'argent à l'infini parce que chaque pays avait son propre support informatique. Sur Evolution, l'hypermarché des délits du darknet où s'échangeaient drogue, hack, armes, j'ai vendu ma méthode pour 2 000 euros. C'est parti comme des petits pains. Jusqu'au jour où BlackBerry a annoncé la fin du support pour le PlayBook, officialisant la fin de vie de cette tablette. On peut dire que j'ai coulé le produit… Puis je me suis mis à la data.

Quel intérêt de récupérer de la data ?

La data représente de l'information. Et l'information, c'est le pouvoir. Moi, je la vendais. Et pas très cher : 300 euros pour un million d'adresses e-mail, 10 centimes pour 100 "combos" (nom d'utilisateur + mot de passe ou e-mail + mot de passe). Celui qui achète ça essaie ensuite d'en tirer profit. Il envoie à ces gens un message qui va infecter directement leur ordinateur ou un e-mail avec un lien "phishing" les invitant à se connecter à un faux site, celui des impôts par exemple. Les "combos", eux, sont utilisés pour s'introduire sur des comptes PayPal, Amazon ou encore Netflix, qui vont ensuite être vidés, s'il y a de l'argent dessus, ou revendus. Aujourd'hui, ta vie vaut moins que les données que tu produis, il faut s'y faire.

QU'EST-CE QU'UN HACKEUR ?

« Etre un hackeur, c'est voir un truc cassé et ne pas pouvoir s'empêcher de faire quelque chose. Soit tu l'exploites, soit tu le répares, mais impossible d'ignorer ce dysfonctionnement et de le laisser comme tel. »

Rabbin des bois

Combien tout cela vous a-t-il rapporté ?

Beaucoup. Je suis millionnaire en bitcoins. J'ai un peu moins de 200 bitcoins, soit 1,5 million d'euros. Mais le bitcoin, après avoir pris de la valeur, en a perdu beaucoup. La difficulté consiste à faire entrer cet argent dans le système légal. Il faut le blanchir ou accepter de payer 60 % d'impôts dessus. Ou alors faire un montage financier et résider pendant six mois à Malte. Un jour, je récupérerai cet argent, mais pas pour l'instant. Je n'aspire pas à être riche. Quand j'avais 13 ans, je pensais qu'en gagnant 10 000 euros par mois, je pourrais tout faire. J'ai fini par gagner ça en un mois. Puis en un jour. Et j'ai réalisé que ça ne représentait plus rien. Je ne cherche plus à avoir mais à être…

Aujourd'hui, vous vous êtes un peu rangé. Que s'est-il passé ?

A la base, je voulais être maître du monde. Quand j'ai réalisé que ce n'était pas possible, j'ai voulu être président. Et, pour le devenir, il faut faire l'Ena et, avant cela, passer par Sciences po. J'étais bon élève. Après un bac + 3, j'ai essayé d'intégrer cette école. Je me suis fait recaler deux fois. Pour la troisième, début 2017, j'ai voulu mettre toutes les chances de mon côté. J'avais repéré sur le site de l'école des failles informatiques permettant de mettre la main sur de nombreuses données personnelles, dont quelque 220 000 adresses e-mail et des milliers de mots de passe d'étudiants. D'ailleurs, ce sont sûrement ces failles qui sont à l'origine des "MacronLeaks", qui ont mis en ligne le contenu des boîtes mail de six responsables de la campagne d'Emmanuel Macron. J'ai pensé que révéler ces défaillances à Sciences po pourrait valoriser ma candidature. J'ai contacté l'école et j'ai parlé pendant deux heures à son directeur de la sécurité informatique. Mais ils ont porté plainte contre X et dit que j'avais demandé mon admission en rançon. C'est complètement faux.

La police a-t-elle débarqué chez vous ?

Oui, il y a eu une perquisition et j'ai été placé en garde à vue. Je risquais jusqu'à deux ans de prison et 100 000 euros d'amende, mais je n'ai écopé que d'un rappel à la loi. C'était la fin d'une époque pour moi. J'ai arrêté mes activités illégales. D'ailleurs, comme je parle dans mon livre des vulnérabilités de grandes écoles comme Normale sup ou l'Ecole de journalisme de Lille, de l'université Lyon 2 ou d'un CHU, j'ai contacté l'Agence nationale de la sécurité des systèmes d'information (Anssi) pour l'avertir. C'est un acte bienveillant et citoyen. L'Anssi m'a remercié et a précisé que ça s'inscrivait dans la loi pour une République numérique, promulguée en 2016, et qu'il n'y aurait pas de poursuites.

De quoi vivez-vous aujourd'hui ?

J'ai arrêté le "crime". Je vends des services sur les réseaux sociaux, des "likes" sur Instagram et Facebook, des "followers" sur Twitter. On est nombreux sur le marché, mais je suis le moins cher de France. Deux euros les 1 000 followers : un clin d'œil à Xavier Niel et à son forfait Free Mobile à 2 euros. J'aspire à devenir le Xavier Niel des réseaux sociaux… Twitter est le réseau social où il y a le plus de "bots" (robots informatiques) : environ 15 % de Twitter, soit 50 millions de comptes, sont de faux profils. Je vais à l'encontre des règles d'utilisation de ces réseaux sociaux, mais ça reste légal. Parmi mes "clients", il y a aussi bien des gamines de 14 ans qui veulent des "likes" sur leurs photos que des marques de vêtements, de boissons ou même de BTP. Les réseaux sociaux peuvent faire une carrière ou la détruire… L'influence est un business juteux ; je gagne environ 5 000 euros par mois. Je hacke aussi sur commande des noms d'utilisateurs…

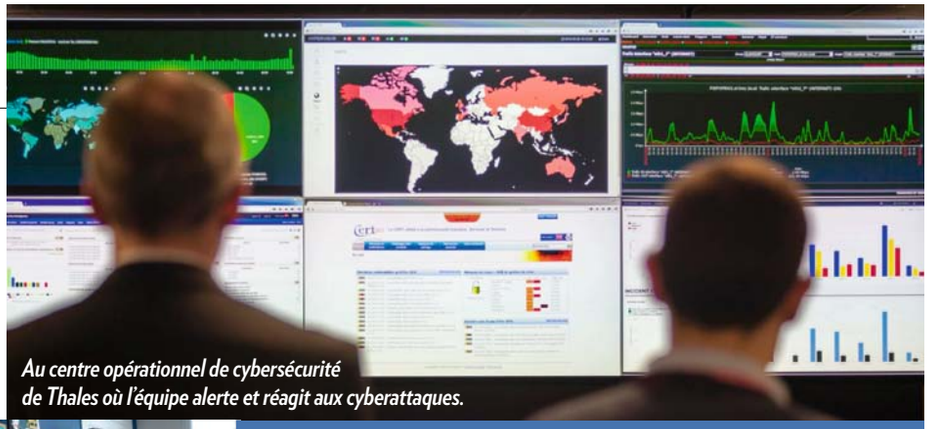
Comment ?

Par exemple vous, Paris Match. Sur Instagram, votre compte, c'est @parismatch_magazine. Mais la propriétaire du compte @parismatch est une jolie jeune fille avec 77 abonnés… D'un point de vue commercial, vous prenez une gifle. Je peux récupérer ce pseudo en hackant le compte et vous le rendre. De nombreuses marques me contactent ainsi pour retrouver leur Instagram. Je vends ce service entre 5 000 et 10 000 euros. Pour une grande marque, ce n'est rien. Parfois, je repère moi-même de faux comptes, comme ceux créés au nom des deux enfants de Cyril Hanouna. Il ne sait sûrement pas qu'ils existent. Je pourrais lui proposer de les lui redonner. *(Suite page 126)*

DES CYBERATTAQUES PLUS ÉLABORÉES ET PLUS DESTRUCTRICES

C'est un record. « L'année 2017 aura été marquée par de nombreuses attaques informatiques, inédites par leur ampleur et leur sophistication », rapporte l'Agence nationale de la sécurité des systèmes d'information (Anssi). Dans son rapport annuel, elle recense 2 435 signalements de sécurité informatique. Pour son directeur, Guillaume Poupard, les récentes attaques ont montré une dimension nouvelle : « Mieux élaborées, plus destructrices », elles touchent désormais « toute la société, du citoyen à la grande entreprise… et même notre démocratie ». Et d'ajouter : « Le risque cyber n'est plus l'affaire des autres, mais un enjeu actuel, prégnant. » Ivan Fontarensky, responsable cyberdéfense et threat intelligence chez Thales, nuance la prise de conscience du côté du secteur privé. « Les grosses sociétés du Cac 40 ont pris la mesure du danger, mais, pour les plus petites, ça paraît encore mystérieux », explique-t-il. Fraudes au président, ransomware (rançongiciel), piratage de données, les attaques se multiplient. « En mai dernier, le rançongiciel WannaCry a infecté en un week-end 300 000 ordinateurs », rappelle Fontarensky. Pour lui, il faut intégrer la cybersécurité dès la conception des nouveaux appareils.

Si la plupart des attaques ont un objectif lucratif, certaines sont de pures opérations de sabotage. Comme NotPetya en juin 2017. « L'attaquant n'a pas frappé directement les victimes, mais le fournisseur d'un logiciel de comptabilité très utilisé en Ukraine », explique l'Anssi. Les entreprises implantées en Ukraine utilisatrices de ce logiciel ont pu être touchées et, par effet boule de neige, de nombreuses autres sociétés, en France et dans le monde, liées à ces premières victimes. Dans l'Hexagone, ce virus a fait perdre 250 millions d'euros à Saint-Gobain, qui a vu son activité bloquée pendant dix jours. A qui profite le crime ? Les gouvernements britannique et américain ont publiquement accusé la Russie d'être derrière ce logiciel malveillant. M.G.



Au centre opérationnel de cybersécurité de Thales où l'équipe alerte et réagit aux cyberattaques.

En dehors de Sciences po, vous avez essayé d'intégrer d'autres grandes écoles, en vain…

J'ai été recalé à Louis-le-Grand, l'Essec, Normale sup. Chaque fois que j'ai essayé d'avoir une admission académique, je me suis fait rejeter à l'oral, si ce n'est à l'écrit. Ces écoles n'intègrent pas des gens différents. Je ne rentre pas dans leurs codes, je ne suis pas formaté ni prêt à l'être. Mais j'aurais adoré suivre ce type d'études. Je vais peut-être d'ailleurs retenter Normale sup l'an prochain.

Quid de 42, l'école de Xavier Niel ?

Elle n'a aucune portée élitiste académique, ça ne m'intéresse pas. J'ai eu des offres d'emploi dans la sécurité informatique, mais j'ai refusé. Je peux faire mieux. Si j'avais une offre d'un très grand groupe, Apple, Facebook ou Google, là, ce serait autre chose.

Qui sont vos modèles ?

Le programmeur Aaron Swartz, une figure iconique du milieu et un des esprits de la plateforme de discussion Reddit. Poursuivi par le FBI, il s'est suicidé avant son procès. J'admire aussi Edward Snowden, qui a échangé sa vie contre un enfer pour avertir les gens. Il devait être l'élément déclencheur d'une prise de conscience massive. Mais, en cinq ans, rien n'a changé. C'est triste. Côté français, je suis impressionné par Cyril Paglino, qui travaille aux Etats-Unis et a fondé Tribe, une application de messagerie vidéo instantanée, une sorte de nouveau Skype qui marche bien mieux.

Votre grand-père fut déporté. "A chaque fois que je vois son visage, ça me rappelle que vivre à travers un écran n'est pas sensé", écrivez-vous…

Quand je le regarde, je sais que je me trompe. La vraie vie est dans le partage. Moi, je suis seul à Paris. Je passe dix heures par jour devant mon écran. Je n'ai pas de vie sociale et je ne peux plus en avoir. Je suis détruit, je ne raisonne plus comme les autres, je ne suis plus dans votre monde. Quand je vois quelqu'un prendre un selfie, je tourne la tête. Mes meilleurs potes sont des lignes sur un écran, des mecs que je n'ai jamais vus.

Pourquoi ce livre ?

Pour avertir les gens, les inciter à développer une conscience numérique. Leur faire comprendre qu'on est dans une cyberguerre numérique mondiale. Elle est déjà en train de se dérouler. Les entreprises, les gouvernements, les hackeurs essaient d'accumuler le plus d'informations, de datas possible. En Ukraine, en décembre 2015, une cyberattaque utilisant le malware BlackEnergy a réussi à couper l'électricité à près de 80 000 foyers pendant plusieurs heures. Le risque est réel. Je pense qu'il est possible de hacker un avion. D'ailleurs, dans une récente interview, Guillaume Poupard, le directeur de l'Anssi, admet que l'attaque informatique d'un avion est une hypothèse que son agence prend en compte. Des pirates peuvent s'en prendre aux opérateurs d'importance vitale (OIV) qui gèrent les infrastructures liées à la santé, à la gestion de l'eau, à l'énergie, aux transports. A partir du moment où c'est relié à Internet, ça peut taper partout : les avions, le pétrole, mais aussi l'assainissement des eaux. En Iran, en 2010, le virus Stuxnet a affecté le programme nucléaire iranien et détruit des centrifugeuses. On a désormais la preuve qu'il s'agissait d'une opération conjointe des Américains et des Israéliens.

Faut-il se méfier des objets connectés ?

COMMENT SE PROTÉGER ? LES 10 CONSEILS D'UN HACKEUR ET D'UN EXPERT EN SÉCURITÉ INFORMATIQUE

1. Définissez un nom d'utilisateur et un mot de passe différent pour chaque compte ou chaque objet connecté.

2. Assurez-vous de donner une bonne entropie à ces mots de passe (c'est-à-dire de les rendre difficiles à cracker) avec un chiffre, un symbole, une majuscule et plus de 8 caractères.

3. Ne communiquez pas vos mots de passe.

4. Vérifiez si vos identifiants ont été compromis dans des vols de données récents via le site haveibeenpwned.com.

5. Ayez un minimum d'« hygiène informatique » : ne cliquez pas sur un lien si vous ne connaissez pas son expéditeur, n'imaginez pas que votre P-DG s'adresse pour la première fois à vous par mail en vous demandant des informations sensibles, etc.

6. Pensez à mettre à jour votre ordinateur. « Ça vaut tous les produits de sécurité », assure Ivan Fontarensky, chez Thales.

7. Séparez le monde du travail de votre vie personnelle et évitez les liens entre les deux. N'installez pas de jeux piratés sur votre ordinateur professionnel.

8. Listez tous vos comptes mails et centralisez-les en un seul.

9. Mettez un sparadrap sur votre webcam. « Si Zuckerberg le fait, il y a peut-être une raison », plaisante Rabbin des bois.

10. Faites passer ces conseils à vos amis.

Ça va être un fléau incroyable. A partir du moment où il y a le mot "Smart", cela signifie que l'objet est connecté à Internet et qu'il peut donc être hacké, infiltré. En septembre 2016, un botnet, un réseau de bots, appelé Mirai, et composé quasi exclusivement de caméras de surveillance et de babyphones, a été utilisé dans une attaque sur Internet, un DDOS (attaque par déni de service), qui a fait tomber l'hébergeur français OVH ainsi que Netflix, Airbnb, Reddit. C'était le plus gros botnet du monde. Dans les dix prochaines années viendra aussi la domination de la "voix", qui se développe via les quatre "cavalières de l'Apocalypse" : Siri, Alexa, Cortana et Home. ■

Interview Mariana Grépinet @MarianaGrepinet

« Lève-toi et code. Confessions d'un hacker », par Rabbin des bois, éd. La Martinière, parution le 16 mai.