Que cherchent les hackers ?

Par **Julie GOMMES**
Cognizant

Introduction

Internet est devenu un nouveau territoire de combats internationaux, fragmenté, disséminé sur des millions de serveurs ; des entreprises et commerces ont pignon sur rue dans ce que Quemener et Ferry appellent des « cyberparadis ». Nous sommes bien loin de l'Internet imaginé par Perry Barlow en 1996, qui espérait ce territoire déconnecté de toute activité physique et obéissant à ses propres règles, définies et changeant au gré des choix des utilisateurs. Ce territoire, miroir déformé du monde physique, est aussi peuplé de personnes qui en connaissent les codes, à tous les sens du terme, et capables de s'en accommoder, voire de s'allier pour en tirer profit, peu importent leurs motivations.

La frontière historique entre *blackhats* (les mauvais hackers) et *whitehats* (les gentils hackers) n'a jamais été aussi poreuse. Il est parfois difficile de cartographier qui sont et surtout ce que veulent ces hackers : au sein de chacun des groupes que nous avons identifiés, évoluent des personnes aux compétences, aux idéaux et aux niveaux techniques variés. Ce n'est plus une frontière manichéenne qui différencie les pirates, ni leur niveau de compétence, mais leurs motivations.

Des motivations bien distinctes

L'appât du gain

Les criminels sont les pirates qui ont fait beaucoup parler d'eux ces dernières années, retombées médiatiques obligent. Ils piratent avant tout pour le profit.

L'argent

De grosses sommes

L'attaque dite de la « fraude au président » est une des plus communes ces dernières années. Les hackers jouent souvent de ce que l'on appelle le Social Engineering[(1)], l'ingénierie sociale, comprenez les techniques de hacking adaptées au mode physique. L'attaquant, souvent après plusieurs mois de recherche d'informations sur l'entreprise et de contacts variés avec des employés, appelle le service comptabilité en se faisant passer pour le chef d'entreprise. Là, il demande un virement en urgence sur un compte hébergé à l'étranger ou la modification des coordonnées bancaires d'un prestataire. Pris par l'urgence de la demande, stressé par le comportement anxiogène du faux président, le comptable transfère l'argent… qui ne restera pas longtemps sur le compte et sera rapidement blanchi ailleurs, grâce à la coopération de certaines banques en ligne (Gueye, 2018). Entre 2010 et 2016, 2300 plaintes relatives à ce type d'attaque ont été déposées en France et le ministère de l'Intérieur estime leur préjudice sur cette période à 485 millions d'euros. De grands comptes français tels que Michelin (1,6 M€) ou Pathé (19 M€) ont d'ailleurs été victimes de ces criminels, mais les attaquants s'en prennent aussi à de petites structures.

(1) Les pratiques d'ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou des organisations pour obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).

(Beaucoup) de petites sommes

Autre extorsion dans l'air du temps, les cryptolockers [2] permettent à des hackers de demander des rançons sous forme de très petites sommes en Bitcoin, pouvant aller de 5 à 50 euros, contre la promesse d'un déchiffrement des serveurs et ordinateurs de l'entreprise ou du particulier attaqué.

Ces malwares [3] circulent au gré des pièces jointes ou fausses publicités en ligne sur lesquelles nous cliquons sans faire attention. Ils se répandent vite et facilement et certains chefs d'entreprise voient l'ensemble de leur parc bloqué et croient ne pas avoir d'autre choix que de payer. Or, dans la plupart des cas, l'attaquant récupère l'argent intraçable et n'envoie jamais la clé de déchiffrement permettant de retrouver ses données.

À l'été 2017, une vague de cryptolockers a même bloqué la production de plusieurs grandes entreprises : Vodafone sera touché par WannaCry, à l'instar de FedEx, Renault, Telefónica et la Deutsche Bahn.

Les données

Des numéros de sécurité sociale aux États-Unis, permettant d'ouvrir un compte au nom de la personne et de récupérer à sa place le trop-perçu des impôts, aux numéros de visa en passant par un plan d'aéroport ou la notice de fonctionnement de machines servant à l'extraction du pétrole, les données sont le nouvel or noir des criminels. Pas besoin de grandes qualités techniques pour trouver le plan d'un aéroport ou le dernier *business plan* d'une entreprise cotée. Même si des entreprises gèrent leur sécurité de manière efficiente, des tiers (entreprise de communication, plombier, prestataires divers…) peuvent laisser leur serveur ou un simple disque dur de stockage connecté à Internet, parfois sans le savoir, et sans protection basique de type mot de passe. Des outils qui « scannent » l'Internet à la recherche d'objets connectés de type disques durs, NAS [4], clés USB, serveurs non protégés sont facilement et gratuitement accessibles en ligne. Les hackers n'ont alors qu'à les installer et les laisser tourner pour télécharger et revendre la documentation récupérée à la concurrence, dans le cas de l'espionnage industriel, ou au plus offrant, sur le darknet [5], où des forums donnent accès à d'autres forums et ainsi de suite, jusqu'à atterrir sur les plateformes où se font les échanges les plus importants.

La hiérarchisation des infractions est de moins en moins visible tant au niveau de la gravité que de leur nature juridique (Gueye, 2018) et c'est aussi sur ces plateformes que sont revendues les données volées *via* piratage et nécessitant des compétences plus étendues (intrusion sur un site et vol de la base de données, récupération des informations contenues dans une boîte email, intrusion sur un serveur suite au cassage d'un mot de passe…).

La déstabilisation d'un État

Il est d'autant plus difficile d'anticiper les attaques visant à déstabiliser un État que les modèles de menaces se diversifient. Les attaquants se présentent souvent sous les traits de hackers nationalistes ou ne font pas part de leur motivation réelle, comme dans le cas de Stuxnet [6], le virus destiné à retarder le programme nucléaire iranien (Bonnemaison et Dosse, 2014).

(2) Logiciels malveillants verrouillant les ordinateurs à des fins de demande de rançon.
(3) Logiciels malveillants développés dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
(4) NAS (de l'anglais Network Attached Storage) est un serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.
(5) Les darknets sont distincts des autres réseaux pair à pair distribués car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas dévoilées publiquement) et que les utilisateurs peuvent donc communiquer anonymement. Plus généralement, le « Darknet » peut désigner toutes les technologies et communications web underground, plus communément associées aux activités illégales ou dissidentes.
(6) Stuxnet est un ver informatique découvert en juin 2010 qui aurait été conçu par la NSA en collaboration avec l'unité israélienne 8200 pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium.

Il est toutefois difficile d'établir clairement les liens entre États et groupes de hackers, même si Bannelier et Christakis (2017) affirment, sans les nommer, que certains États entretiennent des liens avec des groupes non étatiques, utilisés comme intermédiaires dans le but de réaliser des actions malveillantes contre un autre État.

Gueye (2018) détaille les impacts de telles attaques (économiques, sociaux, environnementaux ou vitaux) et souligne un « effet dévastateur pour un pays non préparé » en cas de blocage total de la distribution de billets, d'essence ou de produits frais. Faire vaciller un État sans envoyer un seul missile ou sans tirer un seul coup de feu est donc aujourd'hui possible, d'autant plus que l'avènement des télécommunications civiles et d'Internet a permis de transformer un combat asymétrique (7) en combat symétrique sur le terrain cyber.

Ingérence russe

À ce jeu, l'Europe de l'Est est devenue la boîte de Petri de la Russie, ou du moins de hackers nationalistes se revendiquant proches du Kremlin. Les attaques se multiplient et ce, depuis longtemps (Huvert et Razon, 2019) :

- En avril 2007, lorsque le gouvernement estonien a proposé de déplacer la statue d'un soldat symbole de l'ère soviétique, les sites gouvernementaux, ceux de partis politiques, de médias et de banques du pays, subissent des attaques par déni de service (8), rendant par ailleurs les numéros des urgences (pompiers, police) injoignables quelques temps.
- En juillet 2008, c'est la présidence et le parlement géorgien qui sont visés dans l'attaque de 54 sites Internet de partis politiques et de la finance.
- En 2015, les Russes réalisent une cartographie de centrales électriques ukrainiennes qui servira l'année suivante à lancer l'attaque BlackEnergy : les hackers utilisent alors les backdoors (9) laissées sur le système et, pendant une heure, l'électricité est coupée dans la ville de Kiev.
- En mars 2018, des hackers russes, autoproclamés proches du pouvoir, du groupe « ATP28 » aussi appelé FancyBear, ont été identifiés sur le réseau informatique de l'administration fédérale allemande. Les services secrets avaient alors souligné que ces pirates auraient infiltré le réseau un an auparavant et seraient restés sous les radars afin d'accumuler des informations.

Les pirates d'ex-URSS ont souvent le même profil : des ingénieurs, souvent très bien formés, qui ne souhaitent pas travailler en étant sous-payés par rapport à leur niveau de qualification. Ils se tournent donc rapidement vers une manière moins orthodoxe d'utiliser leurs compétences techniques pour gagner leur vie. En Europe, ce sont souvent des jeunes issus de Roumanie, de Russie ou d'Ukraine qui raflent les premières places des "war games" et "capture the flag". Ces compétitions de hacking sont organisées en marge des conférences de cybersécurité. C'est là qu'ils sont repérés par des ministères ou services de renseignement.

La guerre Inde/Pakistan

Les hackers patriotes russes ne sont pas les seuls à reproduire en ligne des conflits existants : Indiens et Pakistanais se livrent une guerre électronique sans fin autour du Cachemire. Ces dernières années ont d'ailleurs été l'occasion de voir certains d'entre eux monter en compétences.

(7) Une guerre asymétrique oppose la force armée d'un État à des combattants matériellement insignifiants. Les guerres asymétriques englobent notamment les guerres d'indépendance, le terrorisme ou la guérilla et se distinguent des guerres entre États.

(8) Une attaque par déni de service (DoS attack pour Denial of Service) est une attaque informatique ayant pour but de rendre indisponible un service. L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriels dans une entreprise.

(9) Dans un logiciel ou un système d'information, une backdoor (porte dérobée) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel ou au système.

C'est le cas du hacker indien Godzilla :

- En 2012, il commence par des défacements [10] grossiers de sites, plus ou moins faciles à attaquer. C'est souvent un exercice pour les débutants et une manière de constituer son "book", montrer ce que l'on sait faire.
- En 2013, il met hors ligne les sites des ministères pakistanais des Chemins de fer, de l'Économie, de l'Intérieur, des Affaires religieuses, de l'Environnement et bien d'autres, publiant au passage la vulnérabilité qui lui avait permis de réaliser cette attaque : trois administrateurs géraient tous les sites gouvernementaux clés, utilisant une base de données commune, accessible *via* le mot de passe « 111111 ».
- En 2014, il rend hors d'usage plusieurs sites officiels pakistanais, ceux du gouvernement, du ministère de la Défense et de la présidence, en attaquant non pas les sites directement mais l'infrastructure qui supporte ces sites. Il a aussi attaqué à quelques reprises le Bangladesh et, à n'en pas douter, il sera à l'origine d'attaques contre les pays qui, à l'avenir, viendraient à se positionner en ennemis de l'Inde.

Le militantisme

Les « hacktivistes » militent pour des sujets politiques depuis les années 1960, rappelle Gicquel (2014), qui cite notamment les Allemands du Chaos Computer Club [11], le L0pht Heavy Industries [12] ou les écrits de Perry Barlow [13]. De nos jours encore, divers groupes militants se servent des techniques de hacking pour porter leurs causes, le hacking n'est donc pas le but recherché, comme pour les nationalistes, mais un moyen de communiquer ou de collecter de l'information.

Anonymous

Le mouvement Anonymous est né en 2006 sur le site 4Chan, mélange de forum, de tchat et de site de partage d'images. Il ne s'agit pas d'un groupe à proprement parler, avec ses codes et ses règles, comme peuvent l'être les nationalistes ou les malfrats, mais d'un mouvement auquel chacun peut se référer (Coleman, 2014). Manquant de cohésion à ses débuts, Anonymous s'est fait connaître *via* de petites attaques :

- En 2006 et 2007, notamment contre le parti nationaliste américain.
- En 2011, des hacktivistes publient les noms de pédophiles en se revendiquant du mouvement et en invitant d'autres hackers à faire de même. L'appel est suivi, il permettra la dénonciation de 1 589 pédophiles.

Gabriela Coleman définit le groupe comme « une myriade de relations, de structures et de positions morales » ayant pour mission l'attaque systématique de qui causerait du tort à l'humain (services de renseignements, Église de Scientologie, etc.).

Au fil du temps, le mouvement s'est recentré sur la communication. Communiquer vite et bien devient un des principaux objectifs : « Anonymous produit autant de contenus que ses membres ont de compétences créatives » (Gicquel, 2014), une capacité mise en œuvre en 2008 contre l'Église de Scientologie ou en 2010, alors que les dons à Wikileaks sont bloqués : Anonymous crée alors

(10) Un défacement est un anglicisme désignant la modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site. Par exemple, afficher le drapeau d'un pays sur la page d'accueil du site gouvernemental d'un autre pays.
(11) Le Chaos Computer Club, que l'on désigne souvent par le sigle CCC, est l'une des organisations de hackers les plus influentes en Europe.
(12) L0pht Heavy Industries (prononcer loft) était un groupe de hackers réputé, basé à Boston, aux États-Unis, entre 1992 et 2000.
(13) Essayiste, militant libertarien, John Perry Barlow (1947-2018) était un des membres fondateurs de *Electronic Frontier Foundation et de Freedom of the Press Foundation*.

des sites miroirs pour diffuser les informations, traduit des câbles diplomatiques pour leur assurer une visibilité plus large et attaque par déni de service les sites de Visa et Mastercard.

Et ces nombreux groupes, travaillant par pôles idéologiques sous la bannière Anonymous, vont faire éclater le mouvement à l'été 2011. En ressortiront de multiples îlots de hackers indépendants, foyers de résistances idéologiques allant de l'opposition à la censure en Tunisie à la lutte contre la culture du viol aux États-Unis. L'infiltration sur les systèmes d'information d'entreprises ne fait plus partie des incontournables *modus operandi* comme au début du mouvement.

Telecomix

Le groupe d'hacktivistes qui s'était constitué autour de la lutte contre le Paquet Télécom au niveau européen en 2009 a toujours eu une forte implication au niveau politique.

En 2011, ils aident les ressortissants des pays du Maghreb et du Moyen-Orient à communiquer pendant les révolutions alors que les connexions Internet sont impossibles :

- En Égypte, alors que les lignes analogiques ne sont pas coupées (l'armée se servant des téléphones fixes pour communiquer), ils ouvrent des lignes analogiques avec l'opérateur français FDN et envoient les numéros et codes d'accès sur plusieurs centaines de fax en Égypte, accompagnés d'une note explicative sur comment s'y connecter avec d'anciens modems 56k [(14)].
- En Syrie, l'idée de départ était de fournir une boîte à outils numériques pour permettre aux révolutionnaires syriens d'améliorer leur anonymat et leur sécurité en ligne.
  - Ils informent dans un premier temps les Syriens par mail, six mille adresses, en leur donnant des liens vers différents outils tels que le proxy Tor.
  - Le lien vers un salon de tchat est aussi partagé, Telecomix les invitant à aller y poser des questions sur l'utilisation des outils d'anonymat.
  - Suivront plusieurs mois d'échanges avec des Syriens pour les aider à communiquer avec l'extérieur et sécuriser leurs communications.
- En parallèle, Telecomix publie des informations techniques sur la surveillance de masse en Syrie et en Libye et organise des campagnes d'envois de modems 56K en prévision d'une future coupure de l'Internet en Syrie (Guiton, 2013).

Des intérêts parfois communs

Entre les « hacktivistes » aux idées libertaires, les criminels cherchant le profit, si possible immédiat, et les nationalistes qui souhaitent aider à asseoir l'influence de leur pays, il peut sembler que d'épais murs se dressent. Toutefois, ces acteurs peuvent « travailler ensemble » à l'occasion de différentes attaques, comme ce fut parfois le cas :

L'attaque de la Géorgie (2008)

L'attaque de la Géorgie [(15)] était attribuée à la Russie, contexte géopolitique oblige. On retrouvait alors :

- une discipline militaire dans l'organisation de l'attaque, attribuée aux nationalistes ;
- le savoir-faire de criminels, payés pour exécuter vite et bien certaines attaques ;
- l'expérience de groupes activistes en termes de communication.

(14) Modems analogiques.

(15) En août 2008, plusieurs sites géorgiens sont bloqués, d'autres piratés. Le site du ministère des Affaires étrangères géorgien affichait alors une caricature du président Mikheïl Saakachvili sous les traits d'Adolf Hitler.

Il est alors très difficile, même si les nationalistes Russes ont géré l'opération, de savoir comment cette attaque a pu débuter. Et ce modèle d'attaque se rapproche de ce que nous voyons de plus en plus. La piste la plus probable reste toutefois le fait que les premiers ont engagé des criminels pour réaliser leur attaque.

Les attaques croisées post-attentat (2015)

La bataille en ligne entre hackers des pays du Moyen-Orient et hackers occidentaux a éclaté très vite suite à l'attentat de 2015 dans les locaux du journal *Charlie Hebdo* et s'est déroulée en plusieurs temps :

- Une première vague de hackers occidentaux a visé des sites en langue arabe, pris au hasard, surtout *via* des attaques de type DDOS [16] ou de défacement sous la bannière Anonymous. Présentées comme un "fight back", ces attaques ne nécessitaient pas de grandes compétences techniques : elles pouvaient être réalisées grâce à des outils disponibles en ligne et dont l'usage est bien documenté.
- Dans un second temps, des attaquants du Moyen-Orient s'en sont pris à des sites en français vulnérables (campings, mairies de villages, petits commerces), souvent développés par des agences de communication ou des développeurs indépendants qui ne prennent pas toujours suffisamment en compte la sécurité. En façade, on observait des attaques assez symétriques avec ce qui avait pu être observé du côté occidental. Or, il ne s'agissait là que d'une première ligne. Une fois les sites Internet infectés, les serveurs rendus accessibles, un autre groupe de pirates, très expérimentés et n'étant pas originaires du Moyen-Orient, allaient plus loin et dérobaient les données afin d'en organiser la revente sur le *black market* [17] (accès à des serveurs, numéros de cartes bancaires…).

Nous avions alors affaire à des attaquants plus chevronnés mais impossible de savoir si l'occasion leur a permis de commettre leurs larcins ou si, en prévision de ce type d'événement, ils avaient déjà « recruté » des hackers moins expérimentés afin de couvrir leurs délits, les techniciens étant occupés à refaire fonctionner les sites ou enlever les traces de défacement au lieu de surveiller les activités suspectes sur les serveurs.

Que voudront les hackers demain ?

Les guerres de demain

Cette association entre hackers aux objectifs différents sur des projets communs a tendance à se développer, ce qui ne facilitera pas le travail des armées. L'OTAN a changé de paradigme et reconnaît depuis la mi-juin le cyber comme un nouveau territoire de guerre, ce qui l'inclut de fait, au même titre que l'aérien, le maritime et le terrestre, dans les zones sur lesquelles les États peuvent attaquer, se défendre ou défendre un autre pays membre de l'organisation. Une décision mûrement réfléchie puisque, en 2014, les chefs d'État des différents pays de l'OTAN pointaient déjà du doigt les déstabilisations qui pourraient survenir dans le monde physique suite à une attaque en ligne. Des hackers pourraient alors jouer différents rôles :

- Un rôle déstabilisateur, à l'instar des actions en Géorgie ou en Ukraine.
- Un rôle recruteur, afin de faire appel de temps à autres à des *script kiddies* [18] pour créer un

(16) Attaque DOS (voir note 8) réalisée à partir de plusieurs sources de type machines zombies. On parle ici de déni de service distribué (en anglais, *Distributed Denial of Service attack*).
(17) Synonyme de *Darknet* (voir note 5).
(18) Un *script kiddie* est un terme péjoratif d'origine anglaise désignant les néophytes qui passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou programmes mis au point par d'autres.

écran de fumée ou à des criminels leur permettant de bénéficier, contre rémunération, de leurs compétences techniques.

Un rôle diversif, permettant d'attribuer des attaques à d'autres (*via* proxys [19], commentaires de codes dans une langue bien particulière…) et ainsi détourner le regard d'un adversaire vers un autre pays.

L'information demain

Les capacités techniques des hackers leur permettent d'organiser rapidement et facilement des campagnes d'information ou de désinformation *via* notamment le défacement de sites web alors que d'autres vont se rapprocher de journalistes et transmettre des données permettant de faire la lumière sur des pratiques plus ou moins légales, à l'instar des révélations d'Edward Snowden ou le partage d'informations recueillies par des hackers avec un consortium international de journalistes ayant lancé l'affaire des Panama Papers [20].

Bibliographie

OTAN (1949, mis à jour le 25/11/2015), Traité de l'Atlantique Nord, Washington
https://www.nato.int/cps/fr/natohq/official_texts_17120.htm

PERRY BARLOW J. (1976), *Déclaration d'indépendance du cyberespace*, Electronic Frontier Fondation
https://www.cairn.info/libres-enfants-du-savoir-numerique--9782841620432-page-47.htm#

HUVERT E. & RAZON B. (2019), *Les Nouvelles Guerres, sur la piste des hackers russes,* Paris, Arte Éditions / Stock.

GICQUEL C. (2014), Anonymous, la fabrique d'un mythe contemporain, Paris, Fyp Éditions.

GUEYE P. (Dr) (2018), *Criminalité organisée, Terrorisme et cybercriminalité : réponses de politiques cybercriminelles,* Dakar, L'Harmattan Sénégal.

QUEMENER M. & FERRY J. (2009), *Cybercriminalité : Défi mondial,* Paris, Economica.

BONNEMAISON A. & DOSSE S. (2014), *Attention : Cyber ! Vers le combat cyber*-électroniquen, Paris, Economica, Collection Cyberstratégie.

BANNELIER K. & CHRISTAKIS T. (2017), « Construire la paix et la sécurité internationales de la société numérique. Acteurs publics, acteurs privés : rôle et responsabilités », Paris, *Les Cahiers de la Revue Défense nationale.*

COLEMAN G. (2014), *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous,* Québec, Lux éditeur.

GUITON A. (2013), *Hackers : Au cœur de la résistance numérique,* Paris, éditions Au diable Vauvert.

(19) Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
(20) Fuite de plus de 11,5 millions de documents confidentiels issus du cabinet d'avocats panaméen Mossack Fonseca, détaillant des informations sur plus de deux cent quatorze mille sociétés offshore et leurs actionnaires de ces sociétés incluant des hommes politiques, des milliardaires, des sportifs de haut niveau ou des célébrités.