ESPIONNAGE

Le FBI souhaite encore débloquer 63 téléphones
Censée être exceptionnelle, la demande du FBI auprès d'Apple pourrait finalement concerner 63 téléphones répartis sur l'ensemble du territoire des États-Unis. Le bras de fer est donc loin d'être achevé...

Apple, défenseur des libertés individuelles ?
« Pour défendre nos libertés individuelles, nous comptons sur une multinationale, est-ce normal ? », s'est interrogé l'ancien analyste de la NSA, Edward Snowden, à propos du duel entre la NSA et le FBI.

La guerre du cryptage n

Agences de renseignement, multinationales et hackers se disputent l'accès aux données numériques. Une guerre en eau trouble

YANN SAINT-SERNIN
y.saint-sernin@sudouest.fr

Des semaines de bras de fer contre Apple. Et, au final, le FBI jette l'éponge, la semaine dernière. Après avoir tenté de forcer le géant du numérique à fabriquer un logiciel pour ouvrir le smartphone de l'auteur de la fusillade de San Bernardino, en Californie, l'agence fédérale américaine l'a obtenu d'un mystérieux tiers. Bienvenue dans la guerre du cryptage. S'y croisent des multinationales, des agences de renseignement, des hackers, des défenseurs des libertés individuelles mais aussi des réseaux criminels. L'enjeu ? Le contrôle de l'accès aux données. « L'affaire Apple contre le FBI est un épiphénomène dans la bataille du chiffrement », prévient François Pellegrini, professeur d'informatique à l'Université de Bordeaux.

Les fondateurs d'Internet n'avaient pas prévu que la vie privée deviendrait un enjeu majeur des technologies numériques. Dès le début des années 1990, la NSA, la puissante agence de renseignement américaine, l'avait, elle, bien compris. Elle avait réclamé l'autorisation d'introduire dans chaque ordinateur ou téléphone fabriqué aux États-Unis une puce pour l'espionner. Un projet stoppé in extremis par l'administration Clinton.

L'âge d'or de la surveillance

Récemment, l'ex-directeur de l'agence Michael Hayden a reconnu que la « confiance des citoyens » née de cet abandon avait créé « des océans de données », soit « les 15 plus belles années de la surveillance électronique ». Et, comme l'a révélé Edward Snowden en 2012, cet espionnage de masse s'est déroulé avec la collaboration d'une partie de l'industrie numérique.

L'affaire Snowden aurait finalement coûté des milliards de dollars à la Silicon Valley. De quoi réveiller un intérêt pour la défense des libertés individuelles... « L'industrie du numérique continue peut-être à collaborer avec la NSA, car son activité est occulte. Mais pas avec le FBI, qui, lui, opère dans un cadre judiciaire et potentiellement public », relève Éric Filiol, hacker et ancien expert en cryptographie à la DGSE.

« À la suite du scandale Snowden, les solutions de chiffrement des données et des communications se sont démocratisées, via des logiciels libres. Les industriels ont dû suivre », souligne Félix Tréguer, cofondateur de La Quadrature du Net, une association de défense des libertés sur le Web.

Autrefois réservées aux militaires, les techniques de chiffrement les plus sophistiquées, dites de « bout en bout » (de l'émetteur au destinataire), sont aujourd'hui très accessibles. Dans ce système, le développeur lui-même ne possède pas la clé (on ne peut donc pas la lui réclamer). Ainsi, le système d'exploitation Tails (logiciel libre) agrège ces dispositifs et un système d'anonymisation des navigations. Un outil « extrémiste », selon la NSA. Mais le « bout en bout » semble avoir de l'avenir. La messagerie instantanée WhatsApp, filiale de Facebook, vient de l'adopter.

« Il est toujours possible de contourner le chiffrement. Mais rendre cela facile serait dangereux »

Illégal auparavant, ce chiffrement « total » a été autorisé en France en 2004 au nom de la protection de la vie privée mais aussi de la sécurisation des données. « Depuis quelques années, sur fond de terrorisme, on voit ressurgir des tentatives de retour en arrière », s'inquiète Félix Tréguer.

Car ces applications sont aussi utilisées par les djihadistes. En 2015, le Premier ministre britannique, David Cameron, préconisait d'interdire le chiffrement. En France, malgré les possibilités déjà offertes par la loi renseignement, des députés ont proposé d'obliger les constructeurs à mieux collaborer avec la justice. Bernard Cazeneuve, en prenant parti pour le FBI contre Apple, a pointé au passage « les messages chiffrés ». La tentation d'imposer des « portes dérobées » dans les systèmes (des failles connues uniquement par la justice) est là. Pour l'instant, l'idée se heurte à de fortes oppositions.

« Plus à perdre qu'à gagner »

« Il est impossible d'affaiblir un système pour des cas particuliers sans le rendre vulnérable pour tous. C'est s'exposer aux cyberattaques. Il y a plus à perdre qu'à gagner. Sans le chiffrement, d'autres techniques seraient employées comme la stéganographie [messages cachés dans des images ou des sons, NDLR]. Là, on serait aveugles », pense Éric Filiol.

Selon une récente étude de l'Université de Harvard, le grand trou noir du chiffrement n'est pas pour demain. Elle relève que les polices n'ont jamais disposé d'autant de traces qu'avec l'avènement du numérique. Elle rappelle d'ailleurs que l'industrie a fondé son économie sur la collecte de données privées. Et qu'à ce titre elle saura ne pas aller trop loin dans la confidentialité...

Les technologies numériques ont décuplé les moyens de surveillance mais aussi de cryptage. PH. T. DAVID

Un million pour une « faille »

« Il est toujours possible de contourner un chiffrement. Mais ça coûte cher et c'est une bonne chose. Car rendre cela facile et bon marché serait dangereux », estime Éric Filiol. « Il est important que cela demande beaucoup d'énergie. C'est ce qui protège une administration de la tentation de le faire à grande échelle », abonde François Pellegrini.

Déceler des failles dans les systèmes de sécurité est devenu un business pour les hackers. C'est sans doute chez eux que le FBI a trouvé sa solution. « Les grandes agences de renseignement ont fait flamber les prix pour s'assurer l'exclusivité de ces trouvailles, indique Éric Filiol. Une bonne faille peut se vendre jusqu'à 1 million d'euros. » Dans ce domaine, la France a son fleuron. La start-up Vupen a déménagé dans le Maryland. Près du siège de la NSA...

« On doit avoir accès a

Selon le député socialiste Yann Galut, les industriels doivent faciliter le travail de la police

Yann Galut : « Dans des enquêtes en cours, nous avons une dizaine de portables qu'on ne peut pas exploiter ». ARCH. AFP

« Sud Ouest ». Vous avez plaidé pour de lourdes sanctions contre les industriels refusant d'apporter leur concours à la justice. Le chiffrement vous inquiète ?

Yann Galut. J'aborde cette question sous l'angle de l'antiterrorisme. On est dans une situation paradoxale. Aujourd'hui, vous pouvez perquisitionner des domiciles ou des véhicules, mais vous ne pouvez plus perquisitionner le téléphone d'un terroriste. On sait qu'actuellement la téléphonie tient une place très importante dans les enquêtes. Dans

L'ancien directeur de la NSA pas si inquiet, finalement…
« Nous aurons accès à moins de contenu. Mais cela ne veut pas dire que nous aurons accès à moins de renseignement », a lancé récemment l'ex-directeur de la NSA, Michael Hayden, prenant acte du développement du chiffrement, et défendant même Apple.

La crainte des « portes dérobées » dans les systèmes de cryptage
« Si vous créez une porte dérobée dans les systèmes de cryptage, comment pouvez-vous vous assurer que les criminels et les terroristes ne l'utiliseront pas ? », a récemment questionné le directeur de l'Agence européenne de sécurité des réseaux et de l'information.

e fait que commencer

BOÎTE À OUTILS

SIGNAL, TELEGRAM…
Sur les smartphones, les applications de chiffrement des communications se sont multipliées après l'affaire Snowden. Les principales (gratuites) sont aujourd'hui Telegram (du magnat russe Pavel Durov) et Signal (réalisée par des hackers américains et financée par des donations).

LE GPG, LE CADENAS À DEUX CLÉS
Pour chiffrer ses messages, Jules César décalait l'alphabet de trois lettres. Problème, il fallait que la clé de chiffrement soit connue par l'émetteur et le récepteur. Donc qu'elle soit transmise. Dangereux ! Dans les années 1970 est né un système révolutionnaire reposant sur l'existence de deux clés distinctes pour le chiffrement et le déchiffrement. L'une est publique, l'autre est privée et n'est jamais communiquée. Pour échanger avec B, A chiffre son message avec la clé publique de B. Pour déchiffrer, B utilise sa clé privée. C'est sur ce principe que fonctionne le logiciel libre de chiffrement des mails GPG. Les clés sont générées sur la base de problèmes mathématiques que les ordinateurs ne savent résoudre.

TOR, L'OIGNON INVISIBLE
Le logiciel libre Tor cherche à anonymiser les navigations sur Internet. Surnommé « technique du routage en oignon », il intercale entre l'ordinateur et le site visité un réseau de machines relais disséminées dans le monde.

Aucune de ces techniques n'est infaillible. Elles sont utilisées dans diverses optiques : se prémunir contre la censure, l'espionnage économique, le commerce de données… Mais sont aussi employées par les réseaux criminels.

Paranos ? Comment ils protègent leur vie privée

Félix Tréguer
Juriste et cofondateur de La Quadrature du Net
« J'opte le plus possible pour des services alternatifs. Je n'utilise Gmail que pour le commerce. Pour le reste, je chiffre mes mails grâce à des clés GPG. J'ai quitté Facebook il y a deux ans. Cela a eu un impact sur ma vie sociale, mais j'ai survécu. J'ai aussi collé un autocollant sur la webcam de mon ordinateur. »


François Pellegrini. ARCH. T. DAVID

François Pellegrini
Professeur d'informatique à Bordeaux, par ailleurs commissaire à la Cnil
« Je chiffre tout, mails et portable, disque dur. J'utilise également Tor pour anonymiser ma navigation sur Internet. Sur mon ordinateur, j'ai installé Truecrypt. C'est un des premiers logiciels libres de cryptage des données. Il était réputé très fiable. Peu après les révélations de Snowden, ses concepteurs ont posté un avertissement annonçant qu'il n'était pas sûr et qu'il valait mieux utiliser le système de Microsoft… Pour moi, c'est le signe, au contraire, qu'il est très efficace ! J'ai aussi installé une application permettant de repérer les IMSI-catchers (1) sur mon téléphone. Pour l'instant, je n'en ai pas découvert. »

Vincent Roca
Chercheur, auteur d'une étude sur la sécurité des smartphones
« J'ai l'impression de moins maîtriser mon téléphone que mon ordinateur. J'essaie d'utiliser le moins d'applications possible et surtout pas de système d'aide personnalisé. J'utilise les SMS régis par la législation française, mais j'évite les systèmes équivalents tombant sous le coup de la loi américaine. Je n'ai pas non plus de connexion 3G ou 4G. Pour aller sur Internet, je préfère mon ordinateur personnel. Je crypte mon disque dur et chiffre mes mails. »

Éric Filiol
Hacker, ancien spécialiste de cryptologie à la DGSE
« J'ai acheté un smartphone sécurisé (700 euros). Je débranche toujours la géolocalisation et je bloque les mouchards. Pour mes mails, j'utilise des hébergeurs qui ne vivent pas du commerce de données. Je crypte mes disques durs avec différents systèmes. Il n'y a pas de solution miracle mais rien ne vaut la variété. Pour les échanges les plus confidentiels, j'opte pour le système hypersécurisé Tails, qui donne des sueurs froides à la NSA. Je ne suis pas parano. C'est une sorte d'hygiène de vie ! »

(1) Matériel d'espionnage utilisé pour l'interception du trafic de téléphonie mobile.

ux téléphones des terroristes »

celles qui sont en cours, nous avons une dizaine de portables que l'on ne peut exploiter car Apple a modifié son système de chiffrement en 2014. Ma demande était simple : tout en garantissant la liberté individuelle, il faut que la justice puisse accéder à ces smartphones, à condition que cela soit encadré par un juge du siège.

Les opposants à cette disposition pensent que les constructeurs vont devoir affaiblir de façon générale la sécurisation des portables. Ce qui aurait un impact sur la sécurité au-delà des affaires de terrorisme…
C'est faux ! Ces grands groupes font des milliards de bénéfices, investissent des sommes colossales en recherche et développement. Ils peuvent trouver un système qui protège de manière générale et qui permette dans des cas particuliers à la justice d'accéder aux informations. Ils en ont les moyens techniques. Ils doivent s'adapter. Il n'est d'ailleurs pas nécessaire que les constructeurs livrent des clés de chiffrement. On peut trouver un système avec lequel les téléphones seraient déverrouillés dans leurs propres laboratoires.

N'est-il pas normal dans une démocratie que le travail de la police soit parfois difficile ?
Non ! Dans une démocratie, le travail de la police doit être facile. En revanche, il doit être contrôlé et encadré.

Il y a quelques années, les services de renseignement eux-mêmes s'alarmaient de la faible culture en matière de protection des données en France…
Je ne demande pas une remise en cause du chiffrement. Je pense d'ailleurs qu'il doit être développé. On autorise les perquisitions dans les maisons, cela ne signifie pas que les portes doivent rester ouvertes tout le temps. Mais si l'on n'a pas de clé pour entrer, on a un gros problème.

Vous-même, quelles sont vos pratiques pour protéger la confidentialité de vos communications ?
Lorsque je dois rencontrer un lanceur d'alerte, je bannis le téléphone ou les échanges par mail. Mon site a été piraté il y a quelque temps, je suis bien conscient des risques. Mais je ne crypte pas mon disque dur, ni mes échanges. Nous n'avons pas de formation à l'Assemblée nationale sur ces questions. Cela manque peut-être…

Le chef de la CIA trahi par ses mails

En matière de protection des communications numériques, aucun système n'est infaillible. Une illustration restera dans l'histoire : la façon dont l'ex-chef de la CIA, le général David Petraeus, est tombé… à cause de ses mails !

Pour communiquer avec sa biographe et maîtresse, Paula Bradwell, David Petraeus utilisait une méthode éprouvée par les terroristes d'al-Qaida. Elle consiste à ouvrir un compte Gmail, partagé uniquement par deux utilisateurs qui communiquent en se laissant des messages dans la partie « brouillons ». Le général n'ignorait pas que la surveillance classique des communications Internet se base sur les flux. Ici, aucun mail n'est envoyé. Pas d'échanges, donc a priori tout reste discret.

Mais, même pour le chef de la CIA, il est difficile de tout prévoir. Paula Bradwell était jalouse de la proximité de son amant avec une autre jeune femme, Jill Kelley, à qui elle a envoyé une demi-douzaine de mails anonymes, lui reprochant d'avoir une liaison avec David. Jill s'en est émue auprès du FBI. Les mails n'étaient bien sûr pas envoyés depuis son ordinateur, mais Paula n'avait pas pris soin d'utiliser un système permettant d'anonymiser sa navigation.

VAUDEVILLE NUMÉRIQUE
Du coup, le FBI a rapidement recoupé. Les mails étaient envoyés depuis des hôtels où séjournait Paula. Les enquêteurs ont ensuite obtenu l'ensemble des boîtes mail de Paula. Et sont tombés sans difficulté sur celle partagée avec David… et se sont régalés de la correspondance entre le patron de la CIA et sa biographe. Ce vaudeville numérique a coûté sa carrière au général.

Aujourd'hui à la retraite, David Petraeus a tout le temps de méditer ce conseil de Julian Assange, le fondateur de WikiLeaks : « Si vous n'avez pas dix ans d'expérience en cryptographie, utilisez la poste… »