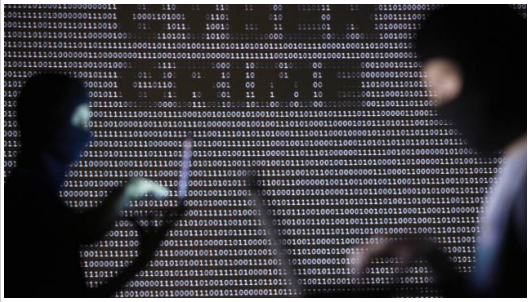
Crainte d’attentats pilotés à partir d’Internet en 2016

Crainte d’attentats pilotés à partir d’Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*

Les opérateurs satellitaires européens nient leur rôle dans la fourniture d’Internet à Daesh

Les opérateurs satellitaires européens nient leur rôle dans la fourniture d’Internet à Daesh

Outil central dans la machine de propagande de Daesh, Internet permet de recruter au-delà des frontières. Pour se connecter, les terroristes utiliseraient les capacités de satellites européens.

Dans une enquête publiée le week-end dernier, le journal allemand Spiegel Online pointe du doigt plusieurs acteurs de l'Internet satellitaire européens (SES, Avanti et le français Eutelsat) pour leur rôle supposé dans la fourniture d'une connexion au Web à Daesh. Alors que les géants du Net Google, Facebook ou Twitter sont appelés à contenir la propagande de l'organisation terroriste, se pose ici la question de son accès au réseau.

Et cette question est centrale dans la lutte contre le terrorisme, car Internet est l'un des vecteurs principaux utilisés par Daesh pour embrigader ses futures recrues. L'organisation diffuse sur les réseaux sociaux grand public ses messages de propagande, qu'elle adapte dans les langues locales, afin de toucher le plus de gens.

Des paraboles turques

Selon le Spiegel, l'organisation terroriste contourne le mauvais état des infrastructures Internet des zones qu'elle contrôle – en Syrie et en Irak – en se connectant par satellite, au moyen de paraboles achetées dans des pays frontaliers, dont la Turquie. En tant que prestataires techniques situés en amont de la chaîne, les opérateurs satellitaires se sont défendus de connaître les clients finaux, voire d'avoir pris des précautions.

C'est le cas d'Eutelsat, seul à avoir réagi publiquement

Le français, contrôlé à 26 % par l'État via la Caisse des dépôts, apporte dans un communiqué deux « clarifications ». Premièrement, il « n'a pas de contact avec des utilisateurs finaux », deuxièmement, « son réseau de distribution n'inclut aucun fournisseur de services en Syrie ». Eutelsat souligne qu'en 2013, il a interdit aux distributeurs de fournir des services Internet en Syrie.

Coordonnées GPS

Pourtant, lorsque les équipements fournis par les FAI se connectent aux satellites, ces derniers reçoivent des coordonnées GPS. Des informations censées permettre, en théorie, de pouvoir remonter la piste. Ainsi selon le Spiegel, de telles connexions sont bel et bien réalisées depuis le territoire de Daesh, dont Raqqa, la capitale autoproclamée, ou encore la ville de Mossoul, en Irak. Mais du côté des opérateurs satellitaires, aucun signal.

L'opérateur luxembourgeois SES a déclaré ne « pas (avoir) connaissance que ses satellites sont utilisés par l'EI ou dans des zones syriennes contrôlées par l'EI » et que si tel était le cas, il mettrait « tout en œuvre pour y mettre fin ». Eutelsat, lui, dit « n'avoir aucune connaissance d'utilisation de ses ressources par Daesh ». Si l'Internet satellitaire était coupé, il enrayerait la propagande, mais aussi les efforts de résistance des civils.

Réagissez à cet article

Source : http://pro.clubic.com/actualite-e-business/actualite-789264-eutelsat-daesh.html

Edward Snowden a-t-il indirectement contribué aux attentats de Paris ?

Edward Snowden a-t-il indirectement aux attentats de Paris vendredi 13 novembre ?

Des responsables politiques et des membres des services de renseignement internationaux accusent les systèmes de communication chiffrés des géants du web de profiter aux terroristes.

Crédit : DENIS CHARLET / AFP Un gendarme de la Brigade Départementale de Renseignements et d'Investigations Judiciaires (illustration)

Edward Snowden a-t-il indirectement contribué aux fusillades meurtrières qui ont balayé l'est de Paris vendredi 13 novembre ?

Certains acteurs de premier plan du renseignement américain ne sont pas loin de l'affirmer. Sans prononcer le nom de l'ancien analyste de la NSA (l'agence nationale de sécurité américaine), le directeur de la CIA John Brennan a clairement laissé entendre la semaine dernière lors d'une allocution à Washington que ses révélations sur les interceptions massives de communications téléphoniques par la NSA en 2013 avaient participé à faire émerger des failles dans la surveillances des réseaux d'extrémistes.

L'ancien directeur de la CIA James Woolsey ne s'embarrasse pas de ces précautions. Selon lui, Snowden a tout simplement « du sang sur les mains ».

À l'époque, ces révélations avaient poussé le Congrès américain à voter la fin du stockage des métadonnées des appels téléphoniques des citoyens américains par la NSA. Elles avaient surtout encouragé les géants du web à adopter des technologies de chiffrement violemment critiquées par la communauté du renseignement.

Depuis le scandale des pratiques d'écoutes de masse par les États-Unis, la protection des données personnelles est devenu un argument commercial pour les sociétés technologiques auprès d'utilisateurs de plus en plus méfiants des services proposés par les entreprises de la Silicon Valley.

Après le rachat de Whatsapp par Facebook, près de 5 millions d'utilisateurs se sont par exemple rabattus sur le service de messagerie sécurisé Telegram, également plébiscité par les terroristes de Daesh.

Apple a développé des systèmes de sécurité de plus en plus draconiens érigeant ses téléphones en véritables forteresses.

Depuis la fin 2014, les emails, SMS et photos de l'iPhone sont chiffrés et personne, pas même Apple, ne peut y avoir accès.

Selon un expert en cybersécurité cité par Les Échos, « la seule manière d'essayer de les récupérer est de décaper le composant avec de l'acide pour ensuite le passer au microscope ». Une opération qui peut coûter plusieurs millions d'euros.

Dans le même temps, Google, Facebook, WhatsApp, Skype ou Twitter n'ont pas ménagé leurs efforts pour sécuriser les données de leurs abonnés. Si bien qu'il est impossible pour les autorités de lire et d'écouter les conversations sur ces services en dehors de réquisitions judiciaires ou d'un accord avec ces entreprises.

Une loi à l'étude au Royaume-Uni

Les autorités et la communauté du renseignement montent régulièrement au créneau pour réclamer un changement de politique des entreprises technologiques.

Le procureur de Manhattan, Cyrus Vance, a répété à plusieurs reprises qu'il a dû abandonner cette année une centaine d'affaires impliquant des meurtriers, faute d'avoir pu accéder aux données de leurs téléphones.

Le directeur du FBI dénonçait en juillet le chiffrement pratiqué par Whatsapp et les entreprises privées, qui permet, selon lui, à des criminels de se mettre à l'abri de la loi.

Au premier rang de leurs revendications figure la création de clés de chiffrement ou de portes dérobées qui leur donneraient accès aux données des utilisateurs quand la situation l'exigerait.

Le débat est également d'actualité de l'autre côté de l'Atlantique. Après les attentats de janvier à Paris, le premier ministre britannique, David Cameron, s'était publiquement interrogé sur les risques de l'existence de données cryptées auxquelles la police ne peut pas accéder. Il souhaite désormais faire figurer dans l'Investigatory Powers Bill, sorte d'équivalent de la loi renseignement française, l'interdiction des méthodes de chiffrement qui n'incluraient pas de porte dérobée permettant aux autorités munies d'un mandat de justice d'accéder aux informations chiffrées. Une nouvelle législation que le locataire du 10, Downing Street justifie par la nécessité de « ne pas créer une situation dans laquelle les terroristes, les criminels et les ravisseurs d'enfants auraient un espace libre pour communiquer ».

Les géants du web rappellent leur attachement au chiffrement

Les géants du net sont fermement opposés à ce type de mesure. Selon eux, leur mise en place reviendrait à introduire une faille dans leurs programmes. Apple, Microsoft, Google, Samsung, Twitter, Facebook et une cinquantaine d'entreprises technologiques regroupées au sein de l'Information Technology Council ont rappelé dans une lettre ouverte que le chiffrement est un outil de sécurité indispensable pour leurs utilisateurs. « Affaiblir le chiffrement quand on a pour but de l'améliorer n'a aucun sens, estiment-ils. Le chiffrement est un outil de sécurité utilisé tous les jours pour empêcher des criminels de vider nos comptes en banque, pour protéger nos voitures et avions des piratages et pour préserver notre sécurité. (…) Affaiblir le chiffrement ou créer des portes dérobées (…) créerait des vulnérabilités qui pourraient être exploitées par les méchants, ce qui causerait certainement des problèmes physiques et financiers sérieux dans notre société et notre économie ».

La France n'a pas encore pris de position claire sur la question. Mi-août, le procureur de la République de Paris, François Molins, a cosigné une tribune du New York Times avec plusieurs responsables internationaux de la lutte antiterroriste pour appeler les géants du web à changer leur politique de chiffrement pour ne pas affaiblir les capacités d'investigation de la justice contre le terrorisme. Adoptée en juin, la loi Renseignement portée par le gouvernement après les attentats de janvier n'évoque pas précisément la cryptologie. Selon Médiapart, le gouvernement avait l'intention de légiférer mais y a finalement renoncé. C'était avant les attentats de Paris. François Hollande a depuis affirmé devant le Parlement réuni à Versailles qu'il souhaitait adapter l'état d'urgence aux évolutions technologiques, sans donner plus de détails.

Les terroristes n'ont pas attendu Snowden

En attendant, il n'a pas été établi à ce stade de l'enquête que les commandos des attentats de Paris ont utilisé un système de communication crypté pour organiser leurs attaques. Le site d'investigation britannique The Intercept a rappelé récemment que les terroristes et les criminels n'ont pas attendu les révélations de Snowden pour se méfier des voies de communication traditionnelles. Les attentats de New York (2001), Bali (2002), Madrid (2004), Londres (2005), Mumbai (2008) et Boston (2013) peuvent malheureusement en témoigner. Le commanditaire des attentats du 11 septembre, Oussama Ben Laden, s'appuyait par exemple uniquement sur un système de messagers humains par crainte d'être pisté par les services de renseignement, notait le Washington Post. Un système qui lui a permis de naviguer en dehors des radars antiterroristes pendant près d'une décennie.

Réagissez à cet article

Source : http://www.rtl.fr/culture/web-high-tech/apple-google-et-les-geants-du-web-entravent-ils-la-lutte-contre-le-terrorisme-7780616618

PAR BENJAMIN HUE

Cyber-terrorisme : un recrutement en 4 phases

Cyber-terrorisme : un recrutement en 4 phases