Nouvelles brèves

Nouvelles brèves

Stuxnet fait entrer le piratage dans une autre dimension

Dans l'avenir, le champ de bataille ne concernera plus seulement les airs, les mers et la terre mais aussi le cyberespace. Depuis quelques années, le piratage informatique fait partie de la panoplie des armes que l'on peut utiliser contre un autre Etat. Tel a été te cas en 2008, lors de guerre russo-géorgienne où des sites gouvernementaux ont été attaqués par des requêtes multiples, provoquant ainsi leur mise hors service.

Rendre inopérant des serveurs Internet en les saturant n'a finalement qu'un intérêt limité, même si cela peut désorganiser ponctuellement l'économie d'un pays, comme par exempte celle de l'Estonie, en 2007. Le vol de renseignements, à l'image de ce qu'a connu, il y a deux ans, l'armée américaine est un autre aspect, non moins intéressant, des opérations que l'on peut mener dans le cyberespace.

Mais le fin du fin reste la capacité à paralyser un réseau électrique ou à pirater les infrastructures industrielles d'un pays. C'est une crainte exprimée notamment par le dernier Livre blanc sur la défense et la sécurité nationale en France. Ce scénario d'ailleurs fait l'objet d'une simulation par un centre d'études politiques indépendant outre-Atlantique en février 2010.

Pour l'instant, aucun cas d'une telle attaque n'a été recensé. Jusqu'à l'apparition du virus inforrnatique Stuxnet. Selon le *Financial Tirnes*, qui a révélé son existence le 24 septembre 2010, ce vers ciblerait des logiciels élaborés par Siemens et utilisés pour contrôler des composants industriels, comme par exemple des valves. En clair, il s'agit de prendre le contrôle d'ordinateurs afin de provoquer des dysfonctionnements au sein d'installations industrielles, voire de les détruire, en faisant exploser une chaudière par exemple. Cela constitue une première.

Concrètement, Stuxnet se propage via une clé USB et s'introduit dans des systèmes informatiques industriels en exploitant des failles dites Zero days, c'est-à-dire qui n'ont pas été encore identifiées. Une fois installté, le virus reste caché dans le système et, une fois qu'il a pris le contrôle de l'automate de programme industriel, il peut ensuite envoyer de nouvelles instructions aux équipements quand certaines conditions sont réunies. Et, cerise sur le gâteau, Stuxnet est capable d'être mis à jour via un module *peer-to-peer*.

Visiblement, l'Iran serait le pays le plus atteint par Stuxnet puisqu'au moins deux tiers des machines infectées s'y trouveraient. Cela donne à penser que le pays des mollahs est directement visé par cette cyber-offensive, qui pourrait cibler son programme nucléaire. L'hypothèse d'une attaque des systèmes informatiques de la centrale nucléaire de Bouchehr, inaugurée l'été dernier, a été avancée. Mais, selon les autorités iraniennes, et même si le chargement du réacteur a pris du retard (officiellement, pour des problèmes de météorologie et sécurité), seuls quelques ordinateurs appartenant à des employés auraient été infectés. L'installation ne fonctionne pas avec des programmes conçus par Siemens.

Une autre piste évoque une attaque contre l'usine d'enrichissement d'uranium de Natanz, qui aurait connu quelques difficultés en 2009, année à partir de laquette Stuxnet aurait commencé à se propager. Cela expliquerait la démission, dans des conditions restées mystérieuses, du patron de programme nucléaire iranien, Gholamreza Aghazadeh'.

Quoi qu'il en soit, du côté de Téhéran, on accuse «des ennemis étrangers d'avoir créé le virus» et on parle de «guerre électronique déclarée par l'Occident contre l'lran.» Le fait est, Stuxnet n'est pas un programme malveillant développé par des *geeks* - fussent-ils brillants - dans un garage. Pour la société spécialiste de la sécurité informatique Symantec, le virus aurait été conçu par cinq à six personnes pendant au moins six ans. Pour Eugene Kaspersky, le concepteur de l'anti-virus du même nom, «une attaque de ce type ne peut être conduite qu'avec le soutien et le financement d'un Etat.»

Dans ces conditions, les regards se tournent vers Israël. D'une part parce que l'Etat hébreu, hostile au programme nucléaire iranien dont un faisceau d'indices montrent la nature militaire, considérerait le sabotage comme un moyen de le perturber. D'autre part, il a développé des capacités en matière de piratage informatique. Ainsi, à la fin des années 1990, le Shin Bet avait réussi à pirater les systèmes de contrôle et de communication, Supervisory Control and Date Acquisition (SCADA) du dépôt de gaz Pi Gliot, situé au nord de Tel Aviv et qui sera visé, en 2002, par une tentative d'attentat qui aurait pu, si elle avait réussi, être très meurtrière.

Seulement, l'idée de pénétrer à l'intérieur du système du dépôt, à des fins de contrôle de routine, en a fait germé une autre. La propagation du virus Stuxnet pourrait en être la conséquence car, depuis dix ans, Israël s'intéresse de près aux moyens offensifs dans le cyberespace, lesquels permettrait d'obtenir des résultats tout aussi importants qu'un raid aérien ou qui aiderait à accomplir ces derniers, comme cela a été le cas pour celui ayant visé une installation probablement nucléaire en Syrie, en septembre 2007.

Cependant, si la thèse est séduisante, il subsiste quelques points qui invitent à la prudence. En effet, les installations industrielles iraniennes n'ont pas été les seules à avoir été infectées par Stuxnet. D'après les spécialistes de la sécurité informatique, d'autres cas ont été recensés en Inde, en Indonésie et aux Etats-Unis. Ces derniers ont également lancé une traque contre ce logiciel malveillant.

Défilé de l'armée iranienne. Source : IRSA.

Nouvelles brèves

Quand la DGSE casse la «crypto» grand public

3 octobre 2010.- «Nos cibles principales aujourd'hui n'utilisent plus le chiffrement gouvernemental ou militaire mais plutôt de la cryptographie grand public, car nous travaillons à 90% sur l'anti-terrorisme. » C'est Bernard Barbier, le directeur technique de la DGSE, qui le dit. Il était l'invité de l'ARCSI à l'occasion de l'excellent colloque de l'association de réservistes.

Comment les grandes oreilles de la DGSE abordent-elles alors Internet et son chiffrement grand public facile, souvent gratuit et surtout très efficace? Pas bille en tête en tout cas, car la DGSE a beau être dotée d'une conséquente puissance de calcul («nous nous chauffons grâce à notre super-calculateur», s'amuse Bernard Barbier), ce n'est pas toujours suffisant. «Je pense qu'avec AES 256 nous sommes arrivés à la fin de l'histoire. Nous ne savons pas le casser par une recherche exhaustive des clés.»

La partie est terminée, alors? Pas vraiment. Car il y a tout un monde entre la qualité intrinsèque de l'algorithme (très bonne) et celle de ses mises en œuvre, notamment au sein de produits grand public (très variable). «L'implémentation d'un algorithme de chiffrement est délicate et donc souvent ratée: la génération de l'aléa est mal gérée ou bien il existe des canaux auxiliaires, par exemple.»

Et même si, par hasard, l'implémentation est du genre solide, la DGSE n'est pas à court de moyens pour autant: «Les mots de passe sont le plus souvent stockés et utilisés sur des systèmes d'exploitation qui ne manquent pas de failles eux non plus», reconnaît le directeur technique. L'approche est donc très pragmatique et certainement efficace: la DGSE récupère les mots de passe directement sur les systèmes ciblés, et elle se constitue au passage un stock de tables de hachage de mots de passe certainement bien alimentées: les fameuses tables arc-en-ciel que l'on trouve aussi dans le commerce, d'ailleurs, mais probablement moins copieusement garnies. On pourrait facilement imaginer la DGSE tel un collecteur de mots de passe particulièrement vorace, essayant frénétiquement des millions de hashes à longueur de journée grâce a un super-calcultateur sous amphétamines.

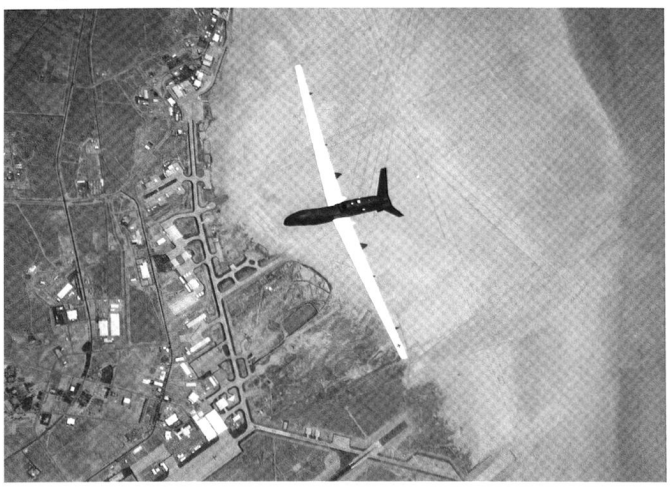
Mais en réalité les espions n'ont finalement pas franchement besoin de chercher les mots de passe. Voire ils se moquent de savoir ce que contient le message intercepté! «Aujourd'hui le contenant est devenu plus important que le contenu. Il y a de plus en plus d'information dans les métadonnées des messages, notamment avec le protocole TCP/IP», explique Bernard Barbier. Ce que raconte la cible est finalement moins important que de savoir à qui elle le raconte. «Nous stockons des années de métadonnées: adresses IP, numéros de téléphones, qui appelle qui, à quelles heures... Et puis nous corrélons.» La DGSE est ainsi finalement un expert du data mining. Et avec à sa disposition le second calculateur le plus puissant d'Europe les perspectives de corrélation sont probablement sans limite. D'autant plus que l'interception de ces métadonnées est facilitée par la forte capillarité des réseaux : « Le routage des communications est totalement mondialisé. Les fibres entre New-York et Miami sont par exemple tellement saturées qu'il revient moins cher à certains opérateurs américains de faire transiter leur trafic entre ces deux villes par l'Europe!»

Ce travail de corrélation permanent ne concerne toutefois pas que les métadonnées des messages IP ou téléphoniques. Vous vous souvenez de ces mots de passe capturés, qui finissent dans une table arc-en-ciel dans l'espoir de retomber un jour sur le même hachage? La DGSE leur a trouvé une autre utilité: elle les corrèle aussi afin de rapprocher des identités a priori différentes. «Quelqu'un qui aurait une double vie aura souvent des mots de passe construits selon le même modèle dans chacune de ses deux vies. Nous faisons tous ça, car la mémoire humaine n'est pas infinie!» Mais si la technique est bien pratique, elle donne aussi l'opportunité à la DGSE de rapprocher deux identités qui, parce qu'elles partagent la même manière de créer leurs mots de passe, peuvent peut-être être la même personne. De quoi faire rêver tous les responsables e-marketing de la planète!

Le renseignement technique a ainsi pris une importance considérable ces dernières années, jusqu'à représenter désormais 80 à 90% de l'activité des services d'après Bernard Barbier, et la France aurait dans le domaine rattrapé son retard au point de jouer en première division. Certes, en tant que directeur technique, l'homme prêche pour sa paroisse, et il serait un peu rapide de balayer le renseignement opérationnel ou humain. Mais effectivement, comme il l'explique, «il est impossible de se promener dans certaines zones tribales du Pakistan ou d'infiltrer certaines cellules.» Le renseignement technique devient donc central et, de ce fait, les progrès réalisés en matière de calcul et surtout de corrélation sont probablement significatifs: «Notre limitation aujourd'hui c'est la puissance électrique.»

http://www.securityvibes.com/people/jsaiz> Jerome Saiz

Grâce à l'*Eurohawk*, en service en Allemagne, les capacités de renseignement européennes ont été sensiblement améliorées.



Nouvelles brèves

«Frenchelon»: la DGSE est en 1e division

Invité par l'Association des réservistes du chiffre et de la sécurité de l'Information, Bernard Barbier de la Direction générale de la sécurité extérieure (DGSE), a levé une partie du voile sur le fonctionnement des *grandes oreilles* de la *grande muette*. On apprend que le renseignement technique (interception des télécommunications, géolocalisation, lutte informatique offensive)
représente 80% à 90% du renseignement, que les réseaux grand public sont la cible principale de la DGSE parce que, pour les terroristes, Internet est un moyen de se cacher.

Nous ne sommes pas des «barbouzes»

Lorsque, à la fin des années 1990, le Parlement européen commença à s'inquiéter de la toute-puissance du système anglo-saxon *Echelon* d'espionnage mondial des communications, les Anglo-Saxons répliquèrent en expliquant que la France disposait, elle aussi, d'un tel système, qu'ils surnommèrent *Frenchelon*. Les autorités françaises n'ont jamais nié l'existence de ce système (dont on ne connaît pas le nom officiel - s'il en a un), mais elles ne s'étaient jamais non plus particulièrement étendu à son sujet.

Inaugurant la nouvelle académie du renseignement, chargée de former les cadres des six services de renseignement français, François Fillon déclarait qu'il fallait «faire en sorte que les Français connaissent mieux les services de renseignements, sachent mieux quelle est leur contribution à leur sécurité quotidienne, et soient plus nombreux à vouloir servir dans leurs rangs (...) Vous le savez, nos services de renseignement ne jouissent pas encore d'une image aussi flatteuse que certains de leurs homologues étrangers. Je pense notamment aux Britanniques. Mais c'est en train de changer. Et pour accélérer ce changement, il faut communiquer davantage (...). Les journalistes, les chercheurs, les historiens doivent pouvoir, plus que cela n'a été le cas, travailler sur le monde du renseignement. C'est utile pour la société française, c'est utile pour les services eux-mêmes.»

Pour la seconde fois, en six mois, le directeur technique de la DGSE est ainsi venu expliquer, devant un public composé de professionnels de la sécurité informatique, l'état de l'art de
son métier: «Je ne vais pas dévoiler de secret d'Etat, mais je vais présenter ce que l'on fait, avec des infos grand public.» Scientifique de haut niveau issu du Commissariat à l'énergie atomique, Bernard Barbier est le directeur technique de la DGSE. Sa nomination marquait la volonté de la DGSE d'investir dans les nouvelles technologies. Son rôle: «rechercher et exploiter les renseignements d'origine technique», donc écouter les télécommunications, mais également mettre en œuvre les satellites d'observation. C'est le patron des *grandes oreilles* et des *grands yeux* de la *grande muette*.

«J'avais beaucoup hésité à m'exprimer publiquement, mais nous ne sommes pas des *barbouzes*, la DGSE a envie de s'ouvrir, notre directeur souhaite que l'on communique, et il est important que les citoyens français connaissent ce que l'on fait.»

Lors de sa première intervention en public, à l'occasion du Symposium sur la sécurité des technologies de l'information et de la communication, en juin 2010, Bernard Barbier avait ainsi expliqué que, si la France faisait partie du *Top 5* (avec les Etats-Unis, la Grande-Bretagne, Israël et la Chine) des pays en terme de renseignement technique, elle avait dix ans de retard pour ce qui est de la lutte informatique offensive. La DGSE, qui emploie 4100 militaires et civils, prévoyait de recruter 100 ingénieurs par an, pendant 3 ans. Pour sa seconde intervention publique, à l'occasion d'un colloque organisé le 30 septembre 2010 par l'Association des réservistes du chiffre et de la sécurité de l'information, Bernard Barbier est revenu sur l'histoire du renseignement technique, mais également sur ce qu'aujourd'hui la DGSE peut faire, ou pas.

Internet est un moyen de se cacher

C'est en cherchant à casser les codes secrets utilisés par les nazis que les Anglo-Saxons bâtirent *Colossus*, le tout premier ordinateur électronique. A l'issue de la guerre, qui avait démontré l'importance du renseignement technique, ils créèrent deux énormes services d'écoute, la National Security Agency aux Etats-Unis et le Government Communications Headquarters au Royaume-Uni. Leur ennemi, l'URSS, était très fermée, entraînant le développement de leur système d'interception des télécommunications Echelon.

Dans le même temps, le terrain de bataille des services français, c'était l'Afrique: le renseignement était essentiellement humain, et non technique... Et il a fallu attendre l'arrivée d'un jeune ingénieur télécom, Henri Serres, en 1983, pour que la DGSE décide de se doter d'une direction technique. La France avait près de quarante ans de retard sur les Anglo-Saxons, «mais aujourd'hui, explique Bernard Barbier, on est en première division.» Lorsqu'il est arrivé à la DGSE, en 1989, l'objectif, c'était le téléphone: des numéros, localisés et limités en terme de relais d'informations (fax, télex ou voix), à bas débit («un million de communications simultanées, c'est pas beaucoup pour nous»), et rarement chiffrés. Le recours à la cryptographie servait d'ailleurs d'alerte, car seuls les diplomates, les militaires ou les services secrets chiffraient leurs communications. «Notre job était de les casser, et on devait traiter entre 100 et 1000 documents par jour.»

A contrario, aujourd'hui, la couverture en téléphonie mobile est quasi-mondiale: on prévoit 4 milliards d'objets connectés en 2013, et les téléphones mobiles sont dotés de centaines de fonctions, applications, et donc d'autant d'identifiants, et l'on peut y faire tout ce que l'on fait sur le Net. Le débit a considérablement changé (de l'ordre de 1 milliard de communications simultanées), et de plus en plus de services et de flux sont chiffrés (*BlackBerry*, *Skype*, *Gmail* -depuis l'attaque des Chinois), sans même que l'utilisateur ne s'en rende compte et, à terme, l'ensemble des télécommunications seront probablement chiffrées, parce que les utilisateurs veulent tout simplement se protéger.

Or, souligne Bernard Barbier, même les méchants se mettent à communiquer : les apprentis terroristes ou talibans, sont souvent jeunes, ont été ou sont encore à l'université. Ils sont donc instruits et, pour eux, Internet est un moyen de se cacher: ils savent qu'ils peuvent être écoutés, ils se cachent donc dans la masse des utilisateurs de l'internet. «Nos cibles principales aujourd'hui n'utilisent plus le chiffrement gouvernemental ou militaire mais plutôt de la cryptographie grand public, car nous travaillons à 90% sur l'anti-terrorisme. Aujourd'hui, nos cibles sont les réseaux du grand public, parce qu'utilisés par les terroristes.»

Autre différence, de taille, par rapport aux écoutes qui prévalaient jusque dans les années 1990: «Le contenant devient plus intéressant que le contenu. Avant, il fallait en effet décrypter les messages chiffrés, parce que l'information

était dans le contenu. Or, "aujourd'hui, ce type d'information est de moins en moins important, et on trouve de plus en plus d'informations dans les métadonnées, surtout en matière d'internet... le tout en clair!»

Car même si les messages sont chiffrés, les *logs*, eux, ne le sont pas, et permettent, par corrélation et *data mining*, de savoir qui communiquent avec qui, quand, pendant combien de temps, voire où, si la communication est géolocalisée. «Toutes ces métadonnées, on les stocke, sur des années et des années, et quand on s'intéresse à une adresse IP ou à un numéro de téléphone, on va chercher dans nos bases de données, et on retrouve la liste de ses correspondants, pendant des années, et on arrive à reconstituer tout son réseau. (...) C'est une transformation énorme de notre métier.» Cette science du secret permet de garantir la confidentialité des communications, mais également de les authentifier. Le monde a bien changé: du temps du téléphone fixe, les particuliers n'avaient pas accès aux outils de chiffrement, alors qu'aujourd'hui, «tous les apprentis terroristes utilisent la crypto.» Et pas seulement: les internautes sont ainsi de plus en plus nombreux à faire de la crypto comme Monsieur Jourdain faisait de la prose, sans parler de ceux, de plus en plus nombreux, qui chiffrent sciemment leurs communications, par obligation professionnelle ou par convenance personnelle, pour se protéger de l'espionnage industriel ou encore de la cybersurveillance que des entreprises comme TMG effectuent au profit de l'Hadopi.

«Nous stockons tous les mots de passe»

«Heureusement pour nous, souligne Bernard Barbier, si le chiffre a atteint un très bon niveau et que la crypto est de plus en plus normalisée, elle ne l'est pas forcément correctement, c'est le bazar total» pour ce qui est de son implémentation. Or, la DGSE est à la tête de la plus forte équipe de crypto mathématiciens de France, qui passe allègrement de la cryptanalyse à l'intrusion informatique, et qui développe une activité très forte de rétro-ingénierie et de *hacking* lui permettant de pénétrer dans les ordinateurs dotés de systèmes d'exploitation et logiciels non mis à jour, pas sécurisés ou qui comportent des failles de sécurité non corrigées :

«Si le méchant utilise un tunnel VPN, réseau privé virtuel permettant de sécuriser les communications, chiffré en 256 bits, on n'arrivera pas à le casser; mais s'il utilise Windows avec plein de failles, on s'y introduit, et on change son VPN en 40 bits, bien plus facile à casser.»

«La mémoire humaine n'étant pas infinie, les utilisateurs utilisent souvent les mêmes mots de passe», ce qui permet d'identifier les apprentis terroristes qui utilisent les mêmes types ou bases de mots de passe lorsqu'ils interviennent sous leurs pseudonymes de guerre, la nuit sur les forums de discussion, que lorsqu'ils s'expriment, le jour, sous leurs vrais noms, sur les réseaux sociaux. «Ils mènent une double vie, mais ont les mêmes mots de passe. Et nous stockons évidemment tous les mots de passe, nous avons des dictionnaires de millions de mots de passe.»

En terme de puissance de calcul, la DGSE est numéro 2, derrière le GCHQ, son homologue britannique: «on sait gérer des dizaines de pétaoctets dans des bases de données (1 pétaoctet, ou Po = 1 000 téraoctets, soit 1 million de gigaoctets, l'équivalent de 2 millions de disque dur à 500 Go), notre limitation, c'est la consommation énergétique», explique Bernard Barbier, qui précise que la chaleur dégagée par leurs super-calculateurs permet aussi de chauffer la DGSE.

En terme d'effectifs, la France est bien moins dotée que les autres services de renseignement dotés de *grandes oreilles*:

- 40'000 personnes à la National Security Agency, auxquelles il faut rajouter les 22000 employés du National Reconnaissance Office chargé du renseignement par l'image.
- 5'000 personnes au GCHQ britannique, une *usine à cryptologie.*
- 5'000 personnes au sein du l'Israel Sigint National Unit, ou Unité 8200, dont un grand nombre d'étudiants qui y effectuent leur service militaire.
- 2'500 au Centre de la sécurité des télécommunications canadien.
- 1'100 personnes à la DGSE (27% de ses effectifs), mais 1800 si on y rajoute les effectifs de la Direction du renseignement militaire.
- En Allemagne, la partie SINGINT emploie 1'000 personnes, en réduction d'effectif, alors que la DGSE est en forte croissance.

Ce à quoi il convient également de rajouter entre 30, 40 ou 50'000 personnes en Russie, et de 100 à 300'000 personnes en Chine... On ne sait pas.

L'EP-3 *Aries* est la version SIGINT de l'Orion (P-3C) de surveillance maritime.

Les forces américaines engagent désormais des appareils de surveillance électronique plus petits, à l'instar du RC-12.