Le cyber-terrorisme

Patrick CHAMBET
patrick@chambet.com
http://www.chambet.com

Depuis le 11 septembre 2001, les pays largement informatisés ont commencé à prendre sérieusement en compte les risques de cyber-terrorisme contre leurs entreprises et leur société en général. Mais il ne faut pas oublier que le cyber-terrorisme, même s'il semble actuellement entrer dans une nouvelle phase d'expansion, n'est pas un phénomène nouveau. Avec une culture de la connectivité ancrée de plus en plus profondément dans les sociétés dites "modernes", il est promis à un bel avenir. Aujourd'hui, on ne saurait plus vivre sans certains services dont l'épine dorsale est constituée par des réseaux informatiques qui pourraient être réduits à néant par quelques attaques bien réelles, judicieusement menées dans le monde virtuel.
Nous allons définir dans cet article les notions de cyber-terrorisme et de cyber-terroristes, puis envisager différents scénarios possibles, examiner les armes dont disposent les cyber-terroristes, et enfin aborder les mesures à prendre pour construire une défense efficace, car la menace de cyber-terrorisme doit maintenant être intégrée dans toute étude de sécurité.

Qu'est-ce que le cyber-terrorisme ?

Le cyber-terrorisme est la convergence entre le terrorisme traditionnel et les réseaux, à commencer par Internet. On peut donc définir le cyber-terrorisme comme l'action délibérée de destruction, dégradation ou modification de données, de flux d'informations ou de systèmes informatiques vitaux d'Etats ou d'entreprises cruciales au bon fonctionnement d'un pays, dans un but de dommages et/ou de retentissement maximum, pour des raisons politiques, religieuses ou idéologiques. Ces dommages peuvent être économiques, sociaux, environnementaux, et même vitaux pour les individus dans certains cas.
Il faut absolument distinguer le cyber-terrorisme du simple cyber-crime, qui consiste à détourner l'usage d'un système dans un but simplement crapuleux. De même, le cyber-terrorisme ne doit pas être amalgamé avec le "hacktivism", qui est certes motivé lui aussi par des éléments idéologiques, mais qui cherche surtout à réveiller la société et à l'éduquer sur certains sujets, pas forcément à la détruire. Enfin, le cyber-terrorisme se distingue du cyber-combat par le caractère généralement civil de ses cibles.

Pourquoi le cyber-terrorisme est-il destiné à avoir autant de succès ? Pour plusieurs raisons. Tout d'abord, le coût d'accès est très faible : un ordinateur portable est beaucoup moins cher qu'un explosif brisant ou qu'une arme de guerre. Ensuite, nos sociétés devenant de plus en plus dépendantes des réseaux d'information, la disparition de ceux-ci peut provoquer des effets économiques, logistiques et émotionnels considérables (voir plus loin). De plus, le public et les journalistes sont fascinés par tous les types d'attaques informatiques, ce qui conduit à une large couverture dans les médias. Enfin, la paralysie des pays dits "développés" lorsqu'ils sont privés de réseaux peut faire la part belle aux pays moins équipés et moins vulnérables de ce côté.

Les scénarios de paralysie des transports...

Qui sont les cyber-terroristes ?

On distingue en général 3 types de cyber-terroristes.
Les cyber-terroristes sont en général des sous-groupes de groupes terroristes traditionnels. Ces sous-groupes peuvent être non structurés et constitués d'individus peu nombreux, travaillant sans organisation particulière, avec peu de moyens, de préparation, de compétences et de stratégie, ou bien au contraire être parfaitement organisés, avec des moyens conséquents et une définition précise de leurs cibles et de leur tactique.

Mais on trouve aussi parmi les cyber-terroristes des sympatisans de groupes terroristes, ainsi que des hackers "patriotes", qui vont procéder à des actions de rétorsion juste après des attaques "physiques" (réelles) ou logiques (sur les réseaux) de ceux qu'ils considèrent comme leurs ennemis [1]. En effet, le terrorisme et l'anti-terrorisme s'emparent d'Internet. Ainsi, tout un chacun peut maintenant faire de l'anti-terrorisme de sa propre initiative, sur une base individuelle, pour le plaisir de se faire peur : par exemple, le groupe de cyber-antiterroristes créé et mené par le hacker allemand à la réputation controversée Kim Schmitz, alias Kimble [2]. Celui-ci a créé le ronflant "Yihat" (en référence au Jihad), acronyme de Young Intelligent Hackers Against Terror, qui se propose de pourchasser les terroristes sur Internet. Ses membres prétendent s'être déjà introduits sur les sites de l'Al Shamal Islamic Bank au Soudan et de l'Arab National Bank à Ryad et y avoir trouvé des données financières concernant Al Qaida et Ben Laden.

On peut aussi citer les attaques de hackers chinois contre des sites américains après le bombardement de l'ambassade chinoise à Belgrade en 1999, les attaques d'Américains contre des sites chinois lors de l'épisode de l'avion espion américain bloqué sur le sol chinois, et les attaques d'autres groupes de hackers américains (les "Dispatchers" notamment) contre les sites taliban [3] en 2001 (voir plus loin). On se rapproche dans ce dernier cas du cyber-combat [4], qui est l'équivalent sur les réseaux de l'affrontement de soldats sur un champs de bataille : les parties sont clairement identifiées et les règles d'engagement obéissent même à un code implicite se rapprochant de la convention de Genève. En effet, les hackers américains ont visiblement fait attention d'attaquer uniquement les sites gouvernementaux taliban, en laissant de côté les sites "civils". Mieux encore, lorsque ces hackers ont "abattu" une cible civile par erreur, ils se sont excusés publiquement, constituant ainsi ce qu'on peut qualifier de premier **cyber-dommage collatéral** déclaré.

Enfin, un dernier type de cyber-terroristes est constitué par des états. Comme il existe des "états terroristes", on commence à observer des "états cyber-terroristes". Certains n'en sont encore qu'à la phase de préparation, notamment à l'acquisition par différents moyens d'équipements informatiques performants. Ainsi, un lot de puissantes machines vendues par les Etats-Unis à la Jordanie et destinées à l'origine à équiper les Renseignements Généraux de ce pays, a été détourné au profit de la Libye [5].

... voire de crash d'avions...

Cibles et impacts

Nous avons vu que les cyber-attentats avaient pour but de causer un maximum de dommages et/ou un maximum de retentissement médiatique, culturel ou social. La simple défiguration ("defacement") de sites Web peu importants constitue donc à peine le premier niveau des cyber-attentats. Ceux-ci consisteront plutôt à faire tomber des sites critiques ou de grande visibilité, ou à rendre inopérantes les infrastructures critiques d'un pays ou d'une organisation. On peut aussi considérer la corruption de données vitales comme un cyber-attentat, puisque la confusion et la chute de confiance créées seront de nature à porter préjudice à la société. Les cibles des cyber-attentats seront donc constituées prioritairement par :

- Les installations de gestion des télécommunications (centraux téléphoniques, points d'accès GSM, réseaux filaires et non filaires, relais hertziens et satellites)
- Les sites de génération et de distribution d'énergie (centrales nucléaires, thermiques, sites de régulation EDF)
- Les installations de régulation des transports (aéroports, ports, contrôle aérien et maritime, gares ferroviaires et routières, autoroutes, systèmes de régulation des feux rouges des grandes agglomérations)
- Les installations de distribution de produits pétroliers (raffineries, dépôts, réseaux de stations services)
- Les centres de gestion du courrier postal

- Les sites de distribution d'eau (usines de traitement, centres d'analyse, stations d'épurartion)
- Les institutions financières et bancaires (bourses nationales, réseau SWIFT, home banking, réseaux de distributeurs de billets)
- Les services d'urgence, de santé et de sécurité publique (police, pompiers, SAMU, hôpitaux)
- Les services gouvernementaux (sécurité sociale, assurance maladie, sites institutionnels)
- Les médias (chaînes de télévision, groupes de presse, fournisseurs de contenus divers)
- Les éléments symboliques d'une société et d'un mode de vie (grande distribution, industries représentatives, ...).

Une attaque sur plusieurs de ces cibles simultanément pourrait avoir un effet dévastateur pour un pays non préparé.

Le moment choisi pour les attaques est également important. Les cyber-terroristes choisiront par exemple de frapper en même temps que des événements politiques ou militaires, ou bien quand l'attention est dirigée dans une autre direction. Ils profiteront également du moment où les procédures se relâchent et où le personnel de surveillance tombe dans la routine. Mais, comme nous l'avons vu, c'est surtout en réaction à des attaques terroristes ou contre-terroristes que les pirates choisissent de frapper.

Les impacts liés à l'attaque des cibles précédentes peuvent être très variés : économiques (des actions ou une bourse peuvent s'effondrer, des entreprises faire faillite), sociaux (chômage, perte de certaines prestations, perte de son "identité sociale"), environnementaux, vitaux. Dans tous les cas, la confusion et la chute de confiance suivant les attaques seront de nature à porter préjudice à la société en général. Les gênes importantes dans les opérations de la vie courante, qui peuvent aller jusqu'au blocage total de certaines fonctions du pays (distribution de billets, d'essence, de produits frais), constituent des dommages majeurs. Certains dommages peuvent même constituer une menace sur la vie de certains individus : ainsi, la mise hors service des systèmes de contrôle de refroidissement des réacteurs d'une centrale nucléaire peut conduire rapidement à un accident radiologique majeur (surtout si la chute automatique des barres de secours a été désactivé), nécessitant l'évacuation d'une zone considérable, avec risque vital à plus ou moins long terme pour la population la plus touchée. De même, un aéroport privé de ses systèmes de contrôle aérien aura beaucoup de mal à éviter des collisions, voire des crashes d'appareils. Enfin, un système de traitement de l'eau victime d'une attaque pourra rendre dangereuse une eau qui n'aura pas été suffisamment chlorée, provoquant potentiellement des épidémies. Le cyber-terrorisme a parfois été qualifié de terrorisme sans mort. Cela pourrait changer à l'avenir.

... sont à envisager sérieusement.

Historique

L'historique du cyber-terrorisme montre que les attaques évoquées précédemment ne sont pas seulement théoriques. Sans être exhaustif, voici quelques événements marquants dans l'histoire du cyber-terrorisme :

- En 1996, un sympathisant du mouvement américain White Supremacist a attaqué et temporairement mis hors service un ISP qui tentait de l'empêcher d'envoyer en masse des messages racistes. L'attaquant avait alors envoyé le message prémonitoire suivant : "Vous n'avez pas encore vu de vrai terrorisme électronique. C'est une promesse" [6].
- En 1997 et les années suivantes, des sympatisants du mouvement Zapatiste mexicain ont effectué des intrusions à plusieurs reprises dans les systèmes logistiques mexicains et ont contribué à influencer l'opinion publique en faveur des Zapatistes, dont la situation, face à l'armée mexicaine, était critique. Des agents d'influence ont propagé des rumeurs sur l'instabilité du Peso mexicain, ce qui a conduit à un effondrement de celui-ci, obligeant le gouvernement à négocier avec les rebelles.
- En 1998, des militants espagnols ont attaqué l'IGC américain (Institute for Global Communications) en effectuant un mail bombing en direction des responsables de l'ISP et des commandes effectuées avec de faux numéros de carte bancaire. Ils menaçaient en outre d'attaquer les autres clients de l'ISP. Ces militants reprochaient à l'IGC d'héberger le site Web du journal Euskal Herria, une publication basée à New York et soutenant le mouvement indépendantiste Basque, et en particulier de soutenir le terrorisme car une partie du site contenait des informations concernant l'ETA. L'IGC a fini par retirer le site incriminé.
- En 1998, la guerrila Tamoule dans le nord du Ski Lanka a engorgé les serveurs des ambassades ski-lankaises avec environ 800 e-mails par jour pendant deux semaines. Les e-mails contenaient le message suivant: "Nous sommes les Tigres Noirs d'Internet et nous allons interrompre vos communications". Les services de renseignement ont qualifié ces attaques comme étant les premières attaques connues de terroristes contre les systèmes informatiques d'un état.

- D'autres exemples non datés sont plus difficilement vérifiables: en Floride, des attaquants auraient détourné les appels au 911 (la police, aux Etats-Unis) vers un magasin de pizzas à emporter. Plus grave, au Massachusetts, un pirate a provoqué la coupure des communications d'une tour de contrôle de la FAA pendant 6 heures. En Russie, des pirates auraient utilisé un collaborateur interne de Gazprom (organisme qui détient le monopole du pétrole en Russie) pour implanter un cheval de Troie leur permettant d'obtenir le contrôle du système de distribution qui gère les flux de pétrole dans les pipe-lines.
- En 1999, pendant le conflit du Kosovo, les ordinateurs de l'OTAN ont été les cibles de mail bombing et de tentatives de dénis de service de la part d'opposants aux bombardements de l'OTAN, dont certains situés dans les états en conflit. Les serveurs de l'OTAN ont été plusieurs fois mis hors service pendant plusieurs jours.
- En 1999, après le bombardement "non tactique" de l'ambassade chinoise à Belgrade, des attaquants chinois ont déposé des messages du type "nous ne cesserons d'attaquer jusqu'à ce que la guerre s'arrête" sur des sites gouvernementaux américains.
- En février 2001, un serveur (heureusement de développement) du fournisseur d'électricité California ISO [7] a été laissé connecté à Internet pendant 11 jours et, bien sûr, hacké.
- En avril 2001, après la collision au dessus de la Chine entre un avion espion américain et un chasseur chinois, et l'incarcération de l'équipage américain en Chine, des groupes de hackers des deux camps (comme les groupes "Honker Union of China" et "Chinese Red Guest Network Security Technology Alliance", en Chine) se sont menés une guerre violente. Plus de 1200 sites américains ont été défigurés ou cibles d'attaques de type déni de service distribué (DDoS), dont les sites de la Maison Blanche, de l'US Air Force, du Département de l'Energie, mais aussi d'entreprises diverses.
- En août 2001, le ver Code Red, qui s'est propagé à très grande vitesse sur Internet, faisait apparaître le message "Hacked by Chinese". Même si aucune preuve n'atteste avec certitude que ce ver provient de Chine, on ne peut s'empêcher de mettre ce message en relation avec les attaques de 1999 (cf ci-dessus). La charge utile de ce ver consistait à établir un grand nombre de connexions vers le site Web de la Maison Blanche afin de provoquer un déni de service distribué. Depuis, d'autres vers (Nimda, Slammer par exemple) ont défrayé la chronique (voir paragraphe suivant).
- Si l'on considère que la défiguration de sites Web constitue le tout premier degré de cyber-attentat, on peut étudier les conflits Inde/Pakistan et Israël/Palestine depuis 1999 jusqu'à aujourd'hui à l'aune des défigurations de sites appartenant aux différentes parties. On observe un strict parallèle entre le nombre de défigurations de sites et les événements politiques et militaires dans les régions citées. Cette comparaison révèle une connexion intime entre les conflits qui ont lieu dans le monde physique et dans le monde virtuel.
- En 2001 et 2002, plusieurs documents retrouvés en Afghanistan et lors des enquêtes sur les réseaux d'Al Qaida ont montré que le cyber-terrorisme était activement étudié par Oussama Ben Laden, passionné par ce type de guerre moderne. Il a consacré des sommes importantes au recrutement dans le monde arabe des meilleurs informaticiens et spécialistes d'Internet. Un plan en ce sens lui avait été remis en juin 2001 par un intégriste séoudien de Londres. D'ailleurs, depuis la capitale britannique, les réseaux Internet intégristes sont de plus en plus actifs [8].

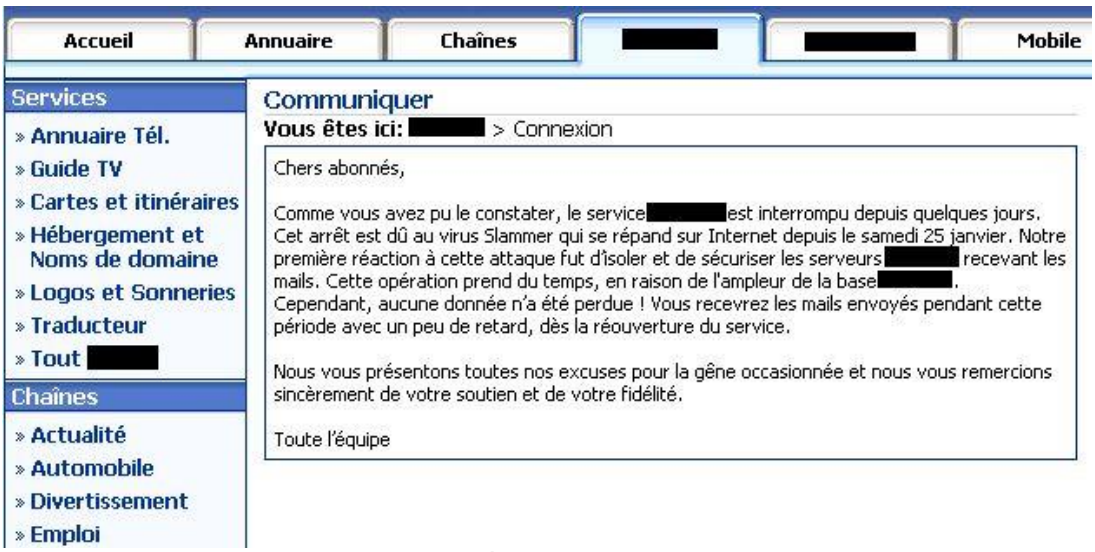
Paralysie des systèmes de communication

Les armes des cyber-terroristes

Les cyber-terroristes ont à leur disposition, comme nous l'avons vu dans les paragraphes précédents, plusieurs types d'armes logiques pour accomplir leurs attaques. Ces armes sont de complexité et de portée différentes, et leurs impacts peuvent être plus ou moins forts. Parmi les armes les plus courantes, on trouve:

- Les défigurations de sites Web et les "attaques sémantiques", qui sont utilisées aussi bien par les "hacktivists" que par les cyber-terroristes. Les attaques sémantiques consistent à changer légèrement le contenu des pages Web afin d'en changer le sens, pour faire passer une idée différente de celle d'origine. Cette modification est difficile à détecter pour le webmaster, contrairement à la défiguration simple qui change complètement l'apparence du site Web.
- Les dénis de service simples (DoS), utilisant soit des vulnérabilités précises du système d'exploitation, soit utilisant des techniques plus génériques comme le SYN flood.
- Les dénis de service distribués (DDoS), utilisant un grand nombre de serveurs compromis sur lesquels tournent des programmes "zombies" attendant les instructions de ceux qui les ont implantés et qui les contrôlent à distance. De véritables "DDoSNets", constitués par des zombies capables de dialoguer entre eux (en peer to peer) et avec leur point de contrôle, se constituent actuellement, qui permettront de lancer des attaques coordonnées aussi rapides que meurtrières sur des cibles bien précises. A cause de ces DDoSNets, les serveurs non sécurisés de n'importe quelle entreprise peuvent se transformer en armes aux mains de cyber-terroristes. De même, les ordinateurs personnels connectés en permanence à Internet par ADSL ou par le câble constituent des cibles privilégiées pour ces DDoSNets, et peuvent, là encore, se transformer en armes.
- Les attaques sur les serveurs DNS et les équipements de routage. Les vulnérabilités des protocoles de routage comme BGP, sensible au poisoning, associées à des attaques sur les root servers DNS, peuvent conduire à une paralysie de certaines parties d'Internet : c'est le phénomène de trou noir, où les informations à destination de certains sites disparaissent complètement. De plus, la majorité des routeurs utilisant l'OS de Cisco (IOS), de nouvelles vulnérabilités mises à jour dans IOS conduiraient à des attaques massives.

- Les vers : Code Red, Nimda, Lion, Adore, Slammer ont montré leurs capacités. Certains prétendent même que le ver Slammer a infecté Internet en 10 minutes seulement [9]. Heureusement, celui-ci ne comportait pas de charge utile hostile et ne résidait qu'en mémoire. On peut imaginer le résultat d'un ver de ce type qui serait capable de mettre hors service instantanément les serveurs infectés, ou de modifier des informations sur ceux-ci...
- Les intrusions classiques, permettant d'implanter des chevaux de Troie, de récupérer des données sensibles ou de mettre hors service des serveurs internes non accessibles autrement.
- La modification furtive de données, suite à une intrusion ou à l'action d'un ver, qui serait capable de décrédibiliser une entreprise ou une organisation, ou même de faire perdre toute confiance en une institution fondée sur cette confiance, comme par exemple la bourse.
- L'implantation de bombes logiques, qui sont capables de se déclencher selon certains paramètres ou certains événements, et peuvent, là encore, faire tomber toute une série de serveurs en même temps, ou modifier des données critiques au moment opportun et de manière automatique.



Le ver Slammer a conduit à l'interruption de nombreux services

Les communications, le recrutement et la formation

Les groupes islamistes se servent d'Internet de manière intensive pour leur recrutement, puis pour la formation et l'endoctrinement de leurs recrues. Les perquisitions menées depuis le 11 septembre 2001 dans les milieux Européens supposés être liés à Al Qaida ont montré qu'ils ont utilisé des sites Web de recrutement de mercenaires [10], comme le site Qoqaz, par exemple [11]. Les mêmes cassettes vidéo ont été trouvées dans une quinzaine d'appartements perquisitionnés. Ces cassettes de formation et d'endoctrinement sont vendues sur Internet, sur des sites comme Maktabah [12]. De même, des newsgroups et des listes de diffusion spécialisés dans la diffusion de sélections documentaires centrées sur l'Islam intégriste présentent les activités des groupes activistes et terroristes au nom de la liberté d'expression [13].

Quant aux communications opérationnelles, les cyber-terroristes savent aller chercher leurs instructions sur l'un des nombreux sites Web entretenus par leur organisation (Al Qaida a installé des centres de communication Internet à Lahore, Karashi, dans les villages pakistanais du Baloutchistan, d'autres sites sont installés au Cashemire), ou encore sur des channels IRC secrets ou totalement banalisés et créés temporairement, pour l'occasion. Certains recommandent même d'utiliser des messageries instantanées de type ICQ.
La multiplication des cybercafés dans le monde entier, y compris et surtout dans les pays en voie de développement, rend la filature des internautes très aléatoire. Pour un dollar chacun, depuis les cybercafés ou les centres d'affaires des hôtels du monde entier, les cyber-terroristes d'une même "cellule-action" peuvent communiquer pendant un quart d'heure en direct, sous un pseudonyme, et s'échanger des informations sensibles relatives à un cyber-attentat avant de se volatiliser dans la nature. S'ils le jugent utile, ils peuvent confirmer leurs instructions par des messages chiffrés envoyés depuis des messageries anonymes. Mais à quoi bon alerter, par un contenu chiffré, la vigilance des services censés surveiller le contenu du trafic Internet, alors qu'il est tout aussi simple de cacher des messages en clair dans une image anodine ? Vu le nombre d'images qui transitent quotidiennement sur Internet, il n'y a aucune chance que le moindre message caché soit détecté. Point n'est besoin d'utiliser de complexes programmes de stéganographie, utilisant des techniques de masquage élaborées, comme certaines rumeurs en ont fait état. Le texte en clair ou tout juste brouillé est tout simplement ajouté au contenu du fichier image.

Principes de défense

Les conflits actuels étant de plus en plus accompagnés par des attaques informatiques, la menace de cyber-terrorisme doit maintenant être intégrée à toute politique de sécurité. Les principes de défense à appliquer sont ceux de la sécurité des systèmes d'information en général : vous avez entre les mains une excellente source de référence pour cela. Il faut donc travailler sur les concepts de défense en profondeur, coupler la sécurité organisationnelle et la sécurité logique, sans oublier la sécurité physique.
En ce qui concerne la sécurité technique, la lecture de MISC vous apportera les bases nécessaire. Pour mémoire, on peut citer :

- Maintenir un état de vigilance élevé
- Effectuer ou faire effectuer une veille technique concernant les dernières vulnérabilités publiées
- Mettre à jour très régulièrement les systèmes d'exploitation et les applications
- Limiter le nombre de services disponibles sur les serveurs et désactiver tous les autres
- Sécuriser les configurations, et en particulier changer tous les mots de passe par défaut, appliquer des mots de passe solides, et utiliser le principe du moindre privilège pour faire tourner les services
- Mettre en place un filtrage d'accès en entrée mais aussi **en sortie** afin que votre plate-forme ne puisse pas être utilisée comme source d'attaques vers d'autres cibles

- Installer des anti-virus côté serveurs et côté clients et les mettre à jour très souvent
- Activer les systèmes de journalisation disponibles sur les systèmes et les applications; centraliser, analyser et sauvegarder les logs régulièrement
- Utiliser des IDS correctement configurés et analysés régulièrement
- Effectuer des sauvegardes régulières, les stocker dans un endroit sûr et tester les procédures de restauration de manière régulière
- Effectuer des sauvegardes
- Effectuer des sauvegardes.

Il ne faut pas non plus oublier les risques internes (voir le cas de Gazprom cité précédemment), d'autant plus que les cibles sont de plus en plus constituées par les postes de travail internes, moins sécurisés et opérés par du personnel non formé aux questions de sécurité. La sensibilisation du personnel est donc primordiale, tout comme la sécurisation des postes de travail, et en particulier des navigateurs Web et des clients de messagerie (voir MISC No 1).

L'avenir

Les risques à venir ont de grandes chances de provenir de **DDoSNets de plus en plus élaborés** et de **vers de plus en plus intelligents**, qui vont certainement voir le jour. Des chercheurs ont prédit l'émergence de nouvelles sortes de vers (Warhol worms, flash worms), qui pourraient se diffuser sur Internet en quelques minutes ou même quelques secondes, laissant peu de temps aux administrateurs pour réagir. Des vers hybrides combinant un ensemble de vulnérabilités anciennes, afin de maximiser leurs chances d'infection, ou bien des vers exploitant des vunérabilités non encore publiées, et donc non patchables immédiatement, vont certainement voir le jour. De tels vers ne laisseront pas d'autre alternative que de stopper les services en attendant la diffusion du correctif de sécurité par les éditeurs.
Pour l'instant, les vers que nous avons vus passer étaient d'une technologie assez fruste. Des vers plus sophistiqués et intelligents, pouvant se mettre à jour de manière autonome en allant télécharger des plug-ins plus récents sur des sites précis, pouvant aller chercher de nouvelles cibles et des instructions sur des channels IRC, pourront effectuer des besognes beaucoup plus dangereuses tout en étant beaucoup plus discrets.

Conclusion

Les frappes physiques sont de plus en plus menées en parallèle avec des frappes logiques. Le cyber-terrorisme fait maintenant intgralement partie des tactiques des groupes terroristes, et les attaques informatiques augmentent en volume, en sophistication et en coordination.
Face à cette menace de plus en plus pressante, l'Europe a commencé à réagir. En lançant le projet de Cyber Security Task Force, la Commission Européenne entre dans la première phase d'élaboration d'une doctrine par l'expression des besoins, c'est-à-dire l'énumération des vulnérabilités générées par la société de l'information. La Commission Européenne a sollicité la Rand Corporation Europe pour réfléchir sur cette typologie des vulnérabilités. Si nul ne songe à contester l'expertise de ce think tank, un certain nombre de réserves peuvent être formulées sur l'objectivité de l'analyse de ce cabinet américain... [14].

NOTES

[1] "Cyber Attacks During the War on Terrorism: A Predictive Analysis." Dartmouth Institute for Security Technology Studies. http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm
[2] http://www.kimble.org/mostwanted.htm
http://www.kill.net
[3] Le mot Taliban est un pluriel.
[4] Le cyber-combat sera traité par ailleurs.
[5] Le Monde du Renseignement No 425 du 14 mars 2002.

[6] Dorothy Denning, “Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” http://www.nautilus.org/info-policy/workshop/papers/denning.html (12 décembre 2001)
[7] http://www.caiso.com
[8] Roland Jacquard, "Les archives secrètes d'Al Qaida", Ed. Jean Picollec.
[9] http://www.cnn.com/2003/TECH/internet/02/05/virus.spread.reut/index.html
[10] Roland Jacquard, "Les archives secrètes d'Al Qaida", op.cit.
[11] http://www.qoqaz.com
http://www.cybcity.com/azzamjihad/
Fatwas: http://www.faharis.net/fatwa.shtml
[12] http://www.maktabah.net/home.asp
[13] Jean Guisnel, "Guerres dans le cyberespace", Ed. La Découverte
[14] Christian Harbulot, "La guerre cognitive: A la recherche de la suprématie stratégique", 25 septembre 2002.

Patrick CHAMBET - http://www.chambet.com
Consultant Senior - Edelweb - Groupe ON-X
http://www.edelweb.fr - http://www.on-x.com

Crédits photo: P.C. - N.R.