Dans Newsweek : "Le brouillard de la cyberguerre"

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 23 avril 2009

Spyworld Actu

Les stratèges militaires de l'OTAN prennent conscience de la menace que constituent les attaques en ligne.

> Cet article a été publié sur le site internet de Newsweek le 18 avril.

Ghostnet, le réseau fantôme : un mot qu'on dirait tout droit sorti d'un roman de John Le Carré. Cette opération de cyber-espionnage à large envergure impliquait 1 295 ordinateurs répartis dans le monde, dont un tiers dans des ministères des Affaires étrangères, des ambassades, des organisations internationales et des organismes de presse, dont certains abritaient des informations secrètes. Selon un rapport publié en mars par trois think tanks canadiens spécialisés dans les questions de sécurité, il comptait au moins un ordinateur, quoique non classifié, du quartier général de l'Otan à Mons en Belgique. Bien qu'on n'ait pu identifier le coupable, certains experts suspectent la Chine. Que les responsables de l'opération aient exploité certaines des données stockées est difficile à dire. Au sein de la plus importante alliance militaire au monde, la facilité avec laquelle on a pu les obtenir a rencontré une certaine incrédulité.

L'Otan commence tout juste à réaliser que l'Internet est devenu un nouveau champ de bataille qui requiert une stratégie militaire. Alors que la vie économique repose de plus en plus sur l'Internet, la possibilité pour de petits groupes de pirates de lancer des attaques dévastatrices sur l'économie du monde est de plus en plus réelle. Pour contrer ces menaces, un groupe de membres de l'Otan, parmi lesquels les Etats-Unis et l'Allemagne, ont établi l'an dernier une sorte de think tank interne consacré à la cybersécurité, installé dans un ancien bâtiment gouvernemental de Tallinn en Estonie. Les trente membres du Cooperative Cyber Defense Centre of Excellence analysent les virus et autres menaces faisant leur apparition, et transmettent des alertes aux membres de l'OTAN qui parrainent cette initiative. Ils travaillent également à mettre d'accord les alliés sur des enjeux difficiles à saisir, et qui rendent le brouillard de la cyberguerre plus épais encore.

Ces experts, dotés d'une expérience de l'armée, de la technologie, du droit et de la science, doivent résoudre des questions délicates. Comment, par exemple, définir avec précision une cyber attaque sur un membre de l'OTAN, attaque qui signifie l'obligation pour les membres de l'alliance de lui venir en aide ? Et comment l'alliance peut-elle se défendre dans le cyberespace ? Le débat a d'ores et déjà engendré des réponses radicalement différentes : alors que Washington envisage de créer un nouveau "tsar de la cybersécurité" et de débloquer des fonds pour la cyberdéfense, l'Estonie va confier une grande partie de la tâche à la population civile, désirant créer un pays de citoyens en alerte et préparés aux menaces en ligne.

Le choix de l'Estonie pour héberger le nouveau brain-trust dédié à la cyberguerre n'est pas un accident. En 2007, l'Estonie et la Russie se chipotaient publiquement sur le sort réservé à un monument datant de l'ère soviétique quand le pays s'est soudainement trouvé en proie à une vague de cyberattaques. Deux des principales banques du pays se trouvaient parmi les cibles et le fonctionnement de leurs services en ligne fut sérieusement dégradé durant plusieurs heures. L'étendue des dommages économiques est un secret d'Etat, mais il est révélateur que ceci arrive en "e-stonie", une société numérique et fière de l'être, où l'on paye même les parcmètres par texto. Bien que la nature décentralisée des attaques ait rendu difficile la désignation du Kremlin comme leur ordonnateur, des preuves ont mené l'Estonie à un suspect de nationalité russe, que le Kremlin a refusé d'extrader.

Une chose est claire : la Russie a remporté ce qui pourrait être qualifié de première invasion réussie de l'ère de la cyberguerre. Hillar Aarelaid, manager de la cellule informatique de réponse urgente estonienne, qui a coordonné la défense de l'Estonie lors de l'attaque, m'a indiqué que celle-ci reposait sur une arme infernale, appelée DDOS pour

"distributed denial of service". Peu coûteux à organiser et d'un effet dévastateur, le DDOS utilise une petite équipe de pirates contrôlant une cyberarmée de PC infectés et qui vont saturer les sites web d'une banque (ou d'une n'importe quelle autre institution) de requêtes apparemment légitimes. Cependant, à en croire Aarelaid, les attaques contre l'Estonie ne visaient qu'à faire étalage de la diversité et de la puissance de l'arsenal des agresseurs. Si l'on considère que les ordres venaient du Kremlin, le message envoyé aux anciens satellites de l'Union Soviétique est clair : si vous nous défiez, c'est à vos risques et périls. L'Estonie, courageusement, a persévéré, et déplacé le monument soviétique malgré tout.

L'attaque a révélé la vulnérabilité d'un membre de l'Otan à une pression extérieure. Si un groupe basé en Russie peut engendrer autant de dégâts pour une histoire de statue, quelles seraient les conséquences d'une opération menée par le gouvernement lui-même ? Les agresseurs pourraient infecter et obtenir le contrôle de milliers d'ordinateurs à la façon de GhostNet et attaquer des banques partout en Europe, provoquant un véritable chaos dans l'économie numérique plus de banques en ligne, impossible de vérifier les achats par carte de crédit. Ajoutez les réseaux électriques, les barrages et les systèmes de navigation des aéroports, tous connectés à l'Internet, et vous avez le parfait scénario d'une production hollywoodienne.

Face à ces attaques, le plus délicat du point de vue de l'OTAN est de distinguer entre la simple malveillance d'un groupe de pirates informatiques et une affaire militaire. En 2007, le ministre de la défense de l'Estonie a déclaré que "les attaques ne pouvaient être considérées comme une simple affaire de hooliganisme, mais devaient être traitées comme une attaque contre le pays". Aune armée n'a cependant franchi les frontières d'Estonie, et rien de ce qu'on associe à un conflit conventionnel n'a pu être constaté. Comment répondre, et contre qui ? Le premier pas, selon les scientifiques du centre, est de déterminer si une menace doit ou non entraîner une réponse militaire. "En l'absence d'un cadre juridique clair concernant la réponse aux cyberattaques, il est très difficile de décider s'il faut les considérer comme les prémices d'un conflit armé" déclare Rain Ottis, l'un des scientifiques en chef du centre.

Les Etats-Unis penchent manifestement pour une stratégie militaire. En mars, le Sénat des Etats-Unis examinait une législation qui placerait l'ensemble des opérations de cybersécurité de la NSA, de l'Armée de l'Air, du Département de la Sécurité Intérieure et d'une dizaine d'autres agences gouvernementales sous la responsabilité d'un "tsar de la cybersécurité" qui prendrait également la fonction de "conseiller national à la cybersécurité". Cette personne serait investie de pouvoirs sans précédents, y compris du droit de fermer les réseaux fédéraux s'il est établi que ceux-ci sont vulnérables. La loi, si elle était adoptée, pourrait entraîner une militarisation plus grande encore du cyberespace. Aujourd'hui, toutes les grandes entreprises titulaires de contrats publics ou presque de Lockheed Martin à Boeing ont créé des divisions consacrées à la cybersécurité, et se battent pour obtenir un financement fédéral. On prévoit que les dépenses consacrées aux réseaux informatiques sécurisés du gouvernement des Etats-Unis passeront de 7,4 milliards de dollars pour 2008 à 10,7 milliards en 2013. La plupart des membres importants de l'OTAN, dont la France, la Grande-Bretagne et l'Allemagne, semble vouloir suivre l'exemple Américain.

L'Estonie, d'un autre côté, a choisi de ne pas monter en épingle la peur de la cyberguerre. En 2007, le débat sur le sujet n'a fait que détériorer plus encore une relation déjà difficile avec la Russie. Elle a préféré démilitariser le problème en transférant la responsabilité de la cybersécurité du ministère de la Défense au ministère des Affaires économiques et de la Communication, et travaille à identifier les services tels que les banques en ligne les plus essentiels au fonctionnement d'une économie numérique. Les Estoniens ont accru leurs efforts visant à éduquer les habitants à l'identification des risques, et à créer des formations universitaires en cybersécurité. Heli Tiirmaa-Klaar, conseiller en chef à la défense au ministère de la Défense d'Estonie, et principal officiel en charge de la cybersécurité dans le pays, évoque l'idée de promouvoir une "culture de la cybersécurité", en commençant à l'école.

Les Estoniens ont raison. Le coût des cyberattaques serait prohibitif si les pirates devaient construire leurs propres ordinateurs plutôt que de pirater des PC laissés en veille. Une société de citoyens avisés est la meilleure défense qui soit, car ceux-ci sont motivés à conserver une longueur d'avance sur les pirates, à l'inverse de l'industrie informatique, car les attaques créent une demande pour des logiciels mis à jour. C'est ainsi que la dépendance de

l'Amérique sur une industrie centralisée de la défense pourrait se retourner contre elle : elle n'est pas suffisamment nombreuse ou agile pour mener les batailles de l'Internet. La réponse civile de l'Estonie a d'une part plus de chances d'être appréciée dans les cercles diplomatiques et, en fin de compte, plus de chance de l'emporter.

> Lire la version américaine de l'article

Post-scriptum :

http://tempsreel.nouvelobs.com/actu...