



net

enquête

La cyberguerre a commencé

Face à la menace d'attaques informatiques de grande envergure, les Etats multiplient les simulations. Mais les piratages récents révèlent les failles des systèmes de protection.

Début mars, des pirates ont infiltré environ 150 ordinateurs de la direction du Trésor du ministère des Finances. L'Elysée et le Quai d'Orsay ont également été ciblés. Le 23 mars, la Commission européenne a été victime d'une attaque, "sérieuse" d'après l'AFP, qui aurait touché les postes des services de la haute représentante de l'UE pour les Affaires étrangères. Quels documents ont été récupérés ? Qui sont les commanditaires ? Autant de questions sans réponses. Ces affaires récentes confirment qu'aucune forteresse - Etat, organisme officiel ou multinationale (comme les compagnies pétrolières récemment) - n'est à l'abri d'une attaque des as du piratage.

Toutes ces opérations ont un point commun qui rend encore plus inquiétante cette loi des séries : le recours à une technique d'infiltration devenue banale, le cheval de Troie. Une ou plusieurs personnes de l'entité visée reçoivent un mail avec une pièce jointe anodine. En réalité, elle cache un code malveillant développé précisément pour cette cible, ce qui explique la difficulté pour les logiciels de sécurité de repérer et d'éradiquer l'infection.

La cyberguerre apparaît comme une technique pour affaiblir l'ennemi en pillant des données stratégiques ou en bloquant ses activités informatiques et ses systèmes de communication. C'est pour éviter la multiplication de ce genre d'opérations

que les Etats réalisent régulièrement des simulations de cyberattaques. En novembre dernier, l'Agence européenne chargée de la sécurité des réseaux et de l'information a imaginé une panne des moyens de communication et des connexions internet dans une trentaine de pays européens. "Cet exercice, qui vise à évaluer l'état de préparation de l'Europe face aux menaces informatiques, est une première étape importante en vue d'instaurer une coopération dans la lutte contre ces menaces", a expliqué Neelie Kroes, vice-présidente de la Commission européenne chargée de la stratégie numérique.

Les États-Unis jouent eux aussi à se faire peur avec l'opération Cyber Storm. Organisée par la division de sécurité informatique du Département américain de la sécurité intérieure, elle simule une panne informatique généralisée causée par une attaque de virus. Plusieurs autres départements américains, une soixantaine d'entreprises privées (dont Intel, Microsoft et Symantec, l'éditeur de l'antivirus Norton) et une trentaine de pays (dont la France) ont participé à la troisième édition en septembre 2010. Le gouvernement français a aussi conduit son propre exercice, baptisé Piranet 2010.

affaiblir l'ennemi en bloquant ses activités informatiques et ses systèmes de communication

Ces simulations permettent de révéler de sérieuses lacunes. En février, lors d'un exercice réalisé par les Européens, les services secrets ont été incapables de localiser l'origine de l'infection... Ces tests confirment aussi que "les États n'ont pas la possibilité de contrer une menace cybernétique de façon autonome et unilatérale : l'absence de frontières étatiques dans l'espace cybernétique ainsi que les interdépendances des systèmes informatiques mettent en évidence la menace d'une attaque lancée à partir de n'importe quel endroit du monde, sans pour autant pouvoir la retracer ou être en mesure de réagir à temps", explique Bart Smedts, chargé de recherches au Centre d'études de sécurité et de défense de l'Institut royal de défense à Bruxelles, dans un numéro de la revue *Défense nationale*.

Ces constats inquiétants ont-ils permis une amélioration de la surveillance et de la protection ? Pas vraiment, selon Eric Filiol, directeur du laboratoire de cryptologie et de virologie opérationnelles à l'École supérieure d'informatique électronique automatique : "Cela fait trois ans que nous avons identifié, expérimenté et publié (pour alerter) ce type d'attaques en laboratoire (...) dans l'indifférence générale. Il n'est donc pas étonnant que des personnes se fassent piéger ni que des attaques comme celles visant Bercy soient faciles à mener. Rappelons que l'efficacité de ces attaques profite de la faiblesse extrême des cibles plus que de la force des attaquants !" **Philippe Richard**