

## Vers le cyberterrorisme?

La dernière série de cyberagressions révèle la fragilité des réseaux informatiques

*BLASTER. Welchia. Sobig.* La dernière série de cyberagressions révèle la fragilité des réseaux informatiques. Ces cyberattaques engendrent des dégâts économiques qui coûtent de plus en plus cher et surtout elles deviennent de plus en plus virulentes. L'insécurité grandissante découlant de la dépendance à l'Internet et de l'interconnexion des différents réseaux informatiques est de plus en plus sérieuse, voire inquiétante. Les pirates informatiques représentent réellement une menace. Mais jusqu'à quel point? Pourraient-ils menacer la sécurité des États et de leurs populations?

En témoigne le black-out qui a récemment frappé plusieurs villes du Canada et des États-Unis. Si, au départ, l'hypothèse d'une cyberagression a été rejetée, les rapports récents démontrent que le virus Blaster a facilité la propagation de la panne électrique et en a prolongé la durée en perturbant le bon fonctionnement des systèmes informatiques relais. Le virus Blaster n'est pas à l'origine de la panne électrique généralisée, mais il en a accru l'ampleur, soulignant la vulnérabilité de plusieurs infrastructures critiques (centrale électrique, banques, centre de traitement des eaux usées, etc.) dépendantes des réseaux informatiques.

### Déjà en 1998

Il est certain que le contexte était particulier. Pour autant, il ne s'agit pas du premier événement soulignant la fragilité des structures dont le fonctionnement repose sur l'informatique. En 1998, par exemple, des *hackers* s'étaient introduits dans le système de gestion de la ventilation de la Bourse de New York: en coupant certains secteurs de la climatisation et en générant ainsi la surchauffe des serveurs, ils avaient perturbé les opérations de la Bourse, entraînant des conséquences économiques notables.

La même année, le groupe de *hackers* "MOD" (Master of Downloading), composé d'Américains, de Britanniques et de Russes, avaient réussi à s'introduire à l'intérieur du "Defense Information System Network", qui contrôle notamment le réseau satellitaire du "Global Positioning System" (GPS), un système qui sert entre autres à gérer le trafic aérien. Si les pirates informatiques ont finalement décidé de se limiter à une simple démonstration de leurs capacités à pénétrer le système, il reste que les dommages auraient pu être considérables.

En 1999, des membres du "l0pht", un des premiers groupes de *hackers* à réussir des piratages fortement médiatisés (aujourd'hui recyclés dans la sécurité informatique), ont été entendus par le Congrès américain: ils ont alors affirmé être en mesure, en moins de 30 minutes, de priver les États-Unis d'électricité pendant deux jours.

Plus inquiétant encore: le piratage du centre indien de recherches nucléaires de Bhabha, perpétré par le groupe de *hackers* "The Milworm". Les pirates informatiques, dont les membres étaient âgés de 15 à 18 ans, ont réussi à dérober des travaux sur les essais militaires nucléaires indiens de mai 1998 et à rendre inopérant deux des huit serveurs du centre.

### Le cyberterrorisme: un scénario plausible?

Si pour l'instant aucun attentat cyberterroriste n'a eu lieu, les différentes enquêtes sur les groupes terroristes démontrent clairement que ces derniers s'intéressent fortement aux possibilités qu'offre l'Internet. On sait qu'Al-Qaeda effectue de nombreuses campagnes de recrutement chez les informaticiens musulmans d'Indonésie et de Malaisie. Dans le manuel offert à ces recrues, il est spécifié que les infrastructures de communications sont une des cibles à frapper tant par des moyens informatiques que par des attentats classiques.

L'Internet est un endroit de prédilection pour fomenter des attentats. Il offre un anonymat quasi impénétrable, renforcée par des capacités de cryptage accrues, en noyant les communications criminelles dans un flot d'innombrables messages licites. C'est également un point faible des sociétés occidentales, et en particulier des États-Unis. La surveillance accrue des réseaux informatiques montre d'ailleurs qu'il y a de véritables plans de cyberattaques. Ainsi,

dans les six mois qui ont suivi le 11 septembre 2001, c'est plus de 129 000 cyberattaques, en provenance essentiellement du Moyen-Orient et d'Indonésie, qui ont été dirigées contre les États-Unis. Même si ces piratages informatiques n'ont encore jamais eu de conséquences graves, les autorités gouvernementales y voient les prémises d'actions de plus grande ampleur. Ces cyberassauts viseraient à déceler des failles potentiellement utilisables dans de futurs actes de **cyberterrorisme**.

### **Pourquoi en sommes-nous là?**

À l'origine réservé aux initiés, l'Internet a connu un essor étonnant et rapide en devenant accessible à une population de plus en plus vaste. Si l'Internet est utilisé généralement pour des motifs tout à fait licites, il est également employé par des personnes ayant des visées criminelles.

Cette explosion de l'Internet ne s'est pas accompagnée d'une éducation appropriée et nombre d'utilisateurs demeurent négligents ou mal informés des risques informatiques. C'est ce qui a d'ailleurs favorisé la rapide propagation de Blaster: alors que la Rustine neutralisant les effets du vers (worm) était disponible trois jours avant l'attaque, bien peu se sont dotés de cette protection et la contamination a pris une dimension mondiale.

Si les imprudences individuelles peuvent fragiliser l'ensemble du réseau, les entreprises s'inscrivent dans la même logique; elles sont en effet particulièrement vulnérables à la contamination et à la prolifération de cyberattaques. Bien des aspects de l'Internet et des secteurs critiques des sociétés sont gérées par des entreprises privées utilisant un nombre croissant d'ordinateurs. Or, trop souvent, ces dernières ne se conforment pas aux normes de sécurité informatique, ces questions étant rarement prioritaires. Tant que les clients n'exigeront pas des compagnies que leurs systèmes informatiques soient sûrs, ces dernières ne chercheront pas à rendre leur réseau fiable et fragiliseront de ce fait le réseau informatique global.

Pour faire face au problème grandissant des cyberattaques, deux évolutions seront nécessaires: D'un côté, il faudra que les mentalités des utilisateurs de l'Internet changent. Les internautes devront prendre conscience que le Web est un environnement peu sûr qui peut engendrer des menaces bien réelles. De l'autre côté, l'élaboration de stratégies à grande échelle sera nécessaire afin de comprendre et de répondre efficacement aux cyberattaques. Puisque l'Internet est un réseau global, les solutions devront l'être également.

### **Benoît Gagnon**

*L'auteur est chercheur à la Chaire Raoul- Dandurand en études stratégiques et diplomatiques de l'UQÀM (www.dandurand.uqam.ca).*

### **Illustration(s) :**

PC

Un employé surveille une partie du réseau de distribution d'électricité en Ontario.

**(c) 2003 La Presse. Tous droits réservés.**

Numéro de document : news·20030914·LA·0020

---

**PUBLI-C** news·20030914·LA·0020

Ce certificat est émis à **Université-de-Montréal** à des fins de visualisation personnelle et temporaire.

Date d'émission : **2007-11-22**

Le présent document est protégé par les lois et conventions internationales sur le droit d'auteur et son utilisation est régie par ces lois et conventions.