

L'attaque chinoise contre Google montre la vulnérabilité des réseaux

Source : Le figaro économie 22 janvier 2010 (Sélection New York Times) Steve Lohr

Depuis les récentes cyberattaques contre le puissant Google, c'est la sécurité de tous les réseaux informatiques qui est remise en cause. La confrontation entre le géant du Web et la Chine - au sujet de la censure en général et d'attaques visant ses systèmes en particulier - est bien entendu un cas exceptionnel. Elle touche des domaines aussi divers que les droits de l'homme, la politique internationale et l'espionnage high-tech. Mais l'intrusion depuis la Chine dans les ordinateurs de Google et de 30 autres entreprises illustre le degré de sophistication des assaillants et la vulnérabilité, même des meilleurs systèmes **de sécurité**.

"Le cas de Google jette la lumière sur ce qu'il est possible de faire en matière d'espionnage et d'infiltration des réseaux d'entreprise", déclare Edward Stroz, ancien agent du FBI et directeur d'un cabinet d'enquêtes spécialisé en cybercriminalité. ces dernières années.

La sécurité informatique est une lutte acharnée et sans fin entre les assaillants, en noir, et les défenseurs, en blanc. La principale arme des premiers est le logiciel malveillant, connu sous le nom de **malware**, qui n'a cessé d'évoluer ces dernières années. Par le passé, ce terme désignait les virus; vers et autres parasites informatiques qui perturbent et parfois endommagent ordinateurs et réseaux.

Aujourd'hui, les malwares sont plus subtils, plus sélectifs, ils nidifient dans les systèmes des entreprises: Ils peuvent servir à l'espionnage industriel, en transmettant des copies numériques de secrets commerciaux, de carnet de clients, de projets ou de contrats.

Chaque année, les sociétés privées et les Institutions publiques dépensent des milliards pour acquérir des outils de sécurité spécialisés capables de détecter et de lutter contre les malwares. Malgré cela, le camp noir semble toujours prendre le dessus.

Une enquête du Computer Security Institute portant sur 443 entreprises et agences gouvernementales publiée le mois dernier montre que 64 % d'entre elles ont signalé des infections informatiques. Le chiffre n'était que de 50 % l'an dernier. En moyenne, les pertes financières dues à ces attaques s'élèvent à 234 000 dollars (163 000 euros) par organisation. "Les malwares nous posent des problèmes colossaux, et le phénomène s'aggrave", déclare Robert Richardson, directeur de l'institut.

Les experts de la sécurité informatique estiment que la sensibilisation et la formation des employés sont cruciales à la protection des entreprises. Les infections ont souvent pour cause des versions high-tech de vieilles arnaques. L'une d'entre elles consiste, par exemple, à laisser une clé USB portant le logo de la société sur le parking de l'entreprise. Des employés curieux la ramassent, la connectent à leur machine et ouvrent ce qui ressemble à un document inoffensif. Mais faisant cela, ils lancent un programme qui enregistre les mots de passe et les informations confidentielles de l'utilisateur et les transmet aux escrocs. Des logiciels plus sophistiqués peuvent permettre à un intervenant extérieur de prendre entièrement le contrôle d'un PC.

Une autre tactique, mise en œuvre pour attaquer Google, est une variation sur le thème du *phishing*, ces courriels provenant prétendument de la banque du destinataire pour l'inciter à communiquer ses mots de passe. Les escrocs envoient des milliers de messages de ce type dans l'espoir de prendre quelques proies dans leurs filets. Dans le cas du *spearphishing*, le faux e-mail est envoyé à une personne spécifique et semble provenir d'un ami ou collègue, ce qui en renforce la crédibilité. Là encore, un fichier joint, une fois ouvert, lance Le logiciel espion.

D'autres techniques exploitent les faiblesses des sites Internet ou des logiciels de routage des réseaux pour pénétrer dans l'infrastructure informa- tique de l'organisation.

Afin d'empêcher les fuites d'informations confidentielles, les logiciels de sécurité de réseau cherchent à détecter les anomalies dans le trafic de données: fichiers volumineux ou taux de transmission) rapide, notamment en provenance d'autres entreprises.

"Pour combattre la cybercriminalité, il faut combiner technologie et science du comportement, pour comprendre la dimension humaine de la menace", explique M. Stroz. "Il n'existe aucune loi qui envoie un ordinateur en prison."

Les téléphones mobiles devenant plus puissants, ils constituent un nouveau terrain exploitable. Récemment, on a détecté des malwares qui en déclenchent subrepticement le micro, et la caméra. "Ils font d'un Smartphone un instrument de télésurveillance", explique Mark Rasch, consultant en sécurité informatique dans le Maryland.

Face à toutes ces méthodes, il semblerait que la démarche idéale consiste à identifier avec soin les éléments de propriété intellectuelle les plus importants pour une société et à les placer sur un réseau informatique distinct, non-relié à Internet.

"Parfois, la solution la meilleure et la moins chère est de fermer la porte et de ne pas se connecter", confie James Litchko, ancien responsable de la sécurité dans l'administration et directeur du cabinet de conseil Cyber Security Professionals.

Mais à l'ère d'Internet, l'isolationnisme est souvent impossible à mettre en pratique. Le partage de l'information et du savoir avec les partenaires industriels et les clients est considéré comme un gage de flexibilité et d'efficacité accrues. Les équipes sont souvent dispersées, les personnes mobiles veulent pouvoir accéder aux données vitales de l'entreprise en tout lieu. L'essentiel de cette communication se fait sur la Toile, ce qui augmente le risque d'attaques extérieures.

La complexité de l'encodage des logiciels des différents fournisseurs, qui s'entremêlent sur les réseaux d'entreprise et sur Internet, ouvre aussi des brèches susceptibles d'être exploitées par les programmeurs de malwares. Les professionnels de la sécurité ont pour habitude de dire en riant : "Le trou est la somme des parties."

Les logiciels eux-mêmes sont pleins de failles. C'est pourquoi la réponse à long terme semble être de favoriser le développement de l'industrie 'du logiciel, en définissant des critères et des responsabilités en cas de manquement à la sécurité, soit par l'autorégulation, soit par la loi.

"C'est un exemple classique d'échec du marché. La sécurité n'est pas au rendez-vous", affirme James Lewis, expert du Center for Strategy and International Studies. "Notre économie est extrêmement dépendante de cette fantastique technologie qu'est Internet, alors qu'elle n'est pas sécurisée. Il va falloir prendre ce problème à bras-le-corps."