Le pire des scénarios : des codes nuisibles dans l’entreprise

Paris, le 24 septembre 2009 - Comment les virus, les Trojan et les vers parviennent-ils jusqu’aux entreprises ? Dans son Livre blanc, G Data décrit les méthodes d’intrusion employées et donne les pistes pour se protéger.

En théorie, les ordinateurs des sociétés sont plus protégés que ceux des particuliers. Mais ils ne sont pas pour autant à l’abri des risques de contamination. Exposés au public via des sites institutionnels ou commerciaux, les entreprises et leurs salariés sont des cibles de choix pour les cyberattaques. Leurs disques durs regorgent d’informations confidentielles qui sont autant de sources potentielles de profit. Pour infecter des ordinateurs, un cyber délinquant innove continuellement. Il est loin le temps du virus intégré dans la pièce jointe d’un e-mail. Maintenant, les attaques se déroulent via l’exploitation de failles dans les navigateurs Internet ou les lecteurs vidéo. Pour cela des armes « clé en main » sont à disposition de tous.

Techniques d’intrusion de pointe

Connus sous les noms de MPack ou encore IcePack, ces d’outils permettent d’intégrer du code nuisible dans des pages Internet d’apparence banale. Une technique redoutable, dite Drive by Download, qui n’est qu’un exemple parmi d’autres de la simplicité avec laquelle un pirate informatique peut s’introduire sur un ordinateur. De la simple navigation sur Internet à la réception de mail en passant par la connexion d’une clé USB sur l’ordinateur, les moyens d’infection n’ont aucune limite.

Contamination lourde de conséquences

Si chez un particulier une attaque se limite seulement à une machine, elle est démultipliée dans un réseau d’entreprise, car tous les postes du réseau deviennent des cibles. Serveurs de stockage, bases de données ou Intranet sont autant de pistes à explorer pour l’intrus, et autant de sources de profit potentielles.

Connaître les méthodes pour les éviter

Pour stopper la contamination, une solution de sécurité efficace dédiée à l’entreprise est, bien entendu, indispensable. Mais la connaissance des méthodes d’attaque et de propagation est aussi une donnée primordiale.

Ralf Benzmüller, directeur du G Data Security Labs : « Une fois qu'un virus ou un ver est en activité, la société a généralement déjà enregistré des pertes ou des dommages dans son réseau. L'administrateur peut alors seulement limiter les dégâts par une réaction rapide. Pour assurer une défense plus efficace, connaître les méthodes de distribution est un avantage qui fait toute la différence. »

Avec son livre blanc « Comment les codes nuisibles parviennent-ils aux ordinateurs d'entreprise ? », G Data fait un point complet sur les méthodes d'attaques et apporte des méthodes pour s'en prémunir.

G Data, reconnu pour ses solutions dédiées à l'entreprise

Les solutions Entreprises de G Data ont reçues une très bonne appréciation de la part du laboratoire de tests AV Comparative (Mai 2009 – version Client Security Entreprise 10). Ces solutions assurent une protection parfaite pour les réseaux des petites, moyennes ou grandes Entreprises. La gamme se compose des versions suivantes : AntiVirus Business 10, AntiVirus Enterprise 10, ClientSecurity Business 10, ClientSecurity Enterprise 10 et MailSecurity 10.