Quand un DSI laisse des backdoors pour pirater son ancien employeur

En matière de sécurité informatique, la menace n'est pas uniquement à l'extérieur de l'entreprise, mais aussi à l'intérieur. Columbia Sportswear, fabricant de vêtements de sports, vient d'en faire l'amère expérience.

En effet, la Cour de l'Oregon va être amené à se prononcer sur une affaire concernant Michael Leeper, ancien DSI de Columbia Sportswear. Il est accusé de vol de données confidentielles au bénéfice d'un partenaire commercial.

Petit rappel historique, Michael Leeper a démarré sa carrière chez Columbia en 2000, comme responsable de l'équipe en charge des PC. Il obtient des promotions pour atteindre le poste de directeur des infrastructures technologiques où il est en charge de la maintenance du système d'information de Columbia et de signer les contrats avec les fournisseurs technologiques. Il était en contact notamment avec Denali, un fournisseur qu'il a rejoint en 2014.

Rester dans le réseau de manière masquée

Mais, juste avant de partir, le responsable IT se serait créé un compte réseau sous le nom « Jeff Maning », aussi appelé « jmanning ». Ce qui lui aurait permis d'accéder au réseau de Columbia, y compris via le VPN et le VDI de la société. Un accès utilisé plus de 700 fois par Michael Leeper pendant 2 ans, afin de voler des documents sensibles de Columbia (plan d'affaires, budget IT, etc) au profit de Denali selon l'accusation. Il aurait mis en place une seconde backdoor (« svcmon ») liée à un compte utilisé par les administrateurs systèmes pour surveiller l'activité réseau. Avant de partir, Michael Leeper s'y serait octroyé le privilège maximal.

Dans sa plainte, Columbia estime que Michael Leeper a eu accès à des e-mails sur des accords commerciaux dans lesquels Denali avait des intérêts financiers. Le prestataire s'est défendu dans un communiqué en indiquant qu'une telle affaire « *ne reflète nullement la politique de Denali et ses valeurs* ». La société précise coopérer à l'enquête et a donné congé à son CTO, Michael Leeper, afin, officiellement, qu'il puisse organiser sereinement sa défense.

Bien sûr, on pourra s'étonner que Columbia Sportswear n'ait pas mis en place des outils pour analyser son réseau et repérer les comportements inhabituels ou les privilèges sur un compte non référencé. Le piratage a été découvert au bout de 2 ans à l'occasion d'une montée de version de la solution de messagerie. Au cours de l'enquête, la firme a obtenu l'appui du FBI.

A lire aussi :

Perte de la messagerie : une amende salée pour un administrateur IT

La NSA mène la chasse aux administrateurs systèmes

Photo credit: kjetikor via Visualhunt.com / CC BY-NC