

Bercy, victime d'une vaste attaque informatique

15 Mars 2011

Courant janvier 2011, les premières alertes sont lancées, concernant l'infiltration du système informatique du ministère de l'Economie et des Finances, après la détection de mouvements « suspects » dans la messagerie. Cette attaque aurait démarré quelques semaines plus tôt dans le courant du mois de Décembre 2010.

Bercy a été victime d'une vaste attaque informatique visant des dossiers ultra-sensibles. La Direction du Trésor était la principale source de hackers cherchant des documents liés à la présidence du G20.

Près de 150 postes ont été touchés par cette attaque, nécessitant plusieurs semaines aux ingénieurs afin de tous les identifier. Il s'agit de la première attaque de cette ampleur contre l'Etat français. De plus, courant Mars, 10.000 postes ont été débranché (sur près de 170.000 postes) afin d'éviter d'éventuelles pertes de données supplémentaires.

La méthode utilisée est très classique : à partir d'une adresse mail piratée, le hacker prend le contrôle de l'ordinateur de sa cible à l'aide d'un cheval de Troie, logé dans un fichier PDF en pièce jointe de l'email. Dès que le fichier s'ouvre, un mouchard pénètre le poste de travail de la cible. Chacun des correspondants au sein de l'administration peut à son tour être infiltré. Cette faille est encore peu, voire non détectée par les éditeurs de solutions de sécurité.

Afin d'infiltrer le réseau du ministère, les pirates ont également utilisés un procédé bien connu des spécialistes de la sécurité informatique : le « Social Engineering » consistant à obtenir des informations clés de manière déloyale et abusive.

Les hackers ont tout de même réussi à obtenir des informations, la plupart étant « banales » mais quelques informations sensibles ont également été téléchargées puis expédiées vers des sites chinois. Heureusement, peu de données personnelles ont été soutirées.

Aujourd'hui, le ministère, et même l'ensemble des administrations et des entreprises sont amenées à renforcer la sécurité de leurs systèmes d'informations pour faire face à ce type d'attaque.