L'attaque de Bercy : « Un mal pour un bien » selon Check Point

« *On tombe un peu de l'armoire.* » La déclaration que **François Baroin**, ministre du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'Etat, a faite au micro d'Europe 1 ce lundi matin 7 mars laisse pantois. Non seulement le système d'information de Bercy est faillible (certes, lequel ne l'est pas?) mais l'attaque a visiblement surpris par son ampleur et sa précision.

Le ministère de l'Économie, des Finances et de l'Industrie (Minefi) a ainsi confirmé, suite à la révélation de *Paris-Match*, avoir été la cible d'une attaque informatique entre décembre 2010 et le week-end dernier, samedi 6 février. Les pirates auraient dérobé des documents liés à l'organisation du G20, dont la présidence et l'organisation sont assurées cette année par la France, rapporte *ITespresso.fr*. Plus précisément, 150 ordinateurs ont été visités, particulièrement ceux de la direction du Trésor.

Une méthodologie qui réduit les soupçons de complicité interne

Selon toute vraisemblance, les attaquants ont réussi à introduire un cheval de Troie envoyé en pièce jointe d'un e-mail dont le compte d'expédition correspond à celui de quelqu'un de connu à Bercy. « *Une méthodologie par* social engineering *qui réduit les soupçons de complicité interne* », estime **Thierry Karsenti**, directeur technique Europe chez Check Point. Et qui montre combien les attaquants étaient très bien organisés. « *Le cheval de Troie employé est inconnu des bases antivirales. Nous n'avons pas affaire à de la réutilisation d'outils malveillant que l'on peut trouver en ligne mais à quelque chose en sous-marin, à une logique d'espionnage à grande échelle.* » Selon le responsable, la recherche d'informations sur la stratégie économique de la France, notamment, semble être la principale motivation des attaquants. Les dossiers fiscaux des particuliers ne seraient pas concernés, selon Bercy.

***Page suivante:* D'où provient l'attaque ?** Qui sont-ils? Impossible à dire pour l'heure. Mais tous les regards se tournent vers la Chine. « *Les flux remontent vers la Chine*, confirme le responsable technique, *mais cela ne signifie pas que les attaques proviennent bien d'organisation chinoises, il y a peut-être un rebond des flux vers des serveurs installés ailleurs.* » Néanmoins, le Canada a connu la même mésaventure en provenance de la province asiatique, six mois plus tôt, également à l'occasion de la préparation du G20, bien qu'aucune preuve n'ait été établie, publiquement du moins.

Dans ce cadre, la révélation de l'affaire par la presse est dommageable selon Thierry Karsenti. « *Maintenant que l'affaire est publique, les services de Bercy vont avoir du mal à pister les attaquants qui ont probablement effacé toutes leurs traces à l'heure qu'il est.* » Outre la publicité sur l'attaque, Bercy a en effet déconnecté quelques 10.000 postes clients de son réseau (12.000 selon *Paris-Match*) pour les mettre à jour (restauration système à une date antérieure à l'attaque ou application des correctifs. Ce qui révèle « *une logique de panique. 10.000 postes déconnectés sur 170.000 [que compte le ministère] montre qu'il y a un risque de propagation forte et donc, la présence de vulnérabilités applicatives ou système exploitées pour la propagation* ».

Une sécurisation difficile à mettre en oeuvre dans les grandes administrations

Sans parler des risques de propagation vers les systèmes d'information des autres ministères. Selon **Patrick Pailloux**, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), les pirates auraient tenté d'attaquer d'autres ministères mais l'Elysée et Matignon seraient épargnés. Le porte-parole de l'Anssi a néanmoins déclaré que *« C'est la première attaque contre l'Etat français de cette ampleur et à cette échelle »*.

Une telle attaque aurait-elle pu être évitée? Au premier chef en évitant d'ouvrir naïvement les pièces jointes aux e-mails. *« Cela nécessite des pistes d'éducation du personnel, des filtres de messagerie et la surveillance des flux d'activité sur le réseau, etc., un certain nombre d'éléments qui peuvent permettre de deviner les alertes*, propose le responsable technique. *Mais c'est très compliqué à faire vivre dans les grandes entreprises et administrations. »* L'attaque de Bercy constitue dans ce cadre *« un mal pour un bien »* car elle *« peut aider à la prise de conscience collective et débloquer des budgets malgré la tendance à la réduction budgétaire »*. Une prise de conscience néanmoins un peu tardive…