

Piratage : Mandiant et le FBI au chevet de Sony Pictures

La semaine dernière, un ex-employé de Sony Pictures alertait le web d'[une attaque massive contre Sony Pictures](#). L'opération est revendiquée par un groupe inconnu qui signe #GOP (Guardian of Peace). Outre **le blocage des ordinateurs sur l'ensemble du réseau**, les cybercriminels ont volé des données sensibles et ont fixé un ultimatum aux dirigeants. Le délai ayant expiré, ils ont commencé à publier certains fichiers comprenant des documents financiers, des adresses électroniques, du code source, etc.

L'attaque a été si violente que Sony Pictures a été obligé de déconnecter l'ensemble de son réseau. La presse américaine indique que la société n'a rebranché les ordinateurs que très récemment et cherche maintenant à savoir qui a perpétré cette attaque. Pour cela, elle a fait appel à [Mandiant, filiale de Fire Eye](#), spécialisé dans les investigations en cybersécurité. **Mandiant** avait déjà été appelé dans [l'affaire Target](#), victime d'un vol de données bancaires via un malware visant les lignes de caisse. Le spécialiste en investigation numérique sera **épaulé par le FBI** dans cette affaire, car les attaques ont débuté dans les locaux New Yorkais de la société de production cinématographique.

La Corée du Nord au banc des accusés

Pendant le week-end, des rumeurs ont circulé sur le fait que **la Corée du Nord** serait derrière cette exaction. Sony Pictures travaille sur un film, *The interview*, une comédie mettant en scène l'assassinat du dirigeant nord-coréen, Kim-Jong Un. Ce film doit sortir le 25 décembre aux Etats-Unis et au Canada, le 11 février en France. Les autorités nord-coréennes avaient saisi l'ONU pour demander des sanctions contre les réalisateurs du film accusés « *de terrorisme et acte de guerre* ».

Sony Pictures est resté très silencieux suite à l'attaque en évoquant simplement un problème informatique interne. Encore moins de commentaires de la part de Mandiant et du FBI. Il faudra attendre pour connaître l'ampleur du piratage.

A lire aussi :

[Comptes à privilèges : la cible privilégiée des hackers](#)

[Pour FireEye, la Chine finance une razzia sur les données de santé US](#)