Sony Pictures : l'Empire contre-attaque… avec du DDoS

Selon Re/code, après le piratage massif dont il a été victime, Sony Pictures a décidé de contre-attaquer sur le terrain choisi par ses assaillants : le cyber-espace. Le studio aurait tout simplement **lancé des attaques par déni de service (DDoS)** pour empêcher que les informations qui lui ont été dérobées soient accessibles. Re/code explique que les studios de cinéma emploient des centaines d'ordinateurs en Asie pour mener ces attaques et s'appuient sur le Cloud d'Amazon Web Services (AWS), sans toutefois préciser quel rôle respectif jouent ces deux pans de l'architecture mise en place par Sony Pictures.

AWS a rétorqué à nos confrères que l'activité qu'ils pointaient du doigt n'existait pas à l'instant t sur son service Cloud. Sans toutefois nier formellement qu'elle puisse y avoir trouvé refuge à un moment donné.

Rappelons qu'en droit français, et européen, une entreprise n'est évidemment pas autorisée à attaquer elle-même des serveurs, même si ceux-ci semblent appartenir à des pirates cherchant à diffuser des informations qu'ils lui ont dérobées.

Un butin impressionnant

Découvert fin novembre, le vol de données perpétré chez Sony est considéré comme l'un des plus graves de ces dernières années. Un groupe de pirates, qui s'est désigné sous l'appellation Guardians of Peace, explique avoir dérobé **près de 100 To de données** de tous types (informations financières, budgets, salaires, e-mails, films, données personnelles des employés). C'est ce trésor de guerre que les hackers dévoilent par petits bouts sur des sites de partage de fichiers comme PasteBin.

Des informations confidentielles sur les contrats que passent les studios Sony avec des tiers ou ses relations avec des stars du cinéma figurent ainsi dans le lot de données dérobées (le numéro de sécurité sociale de Sylvester Stallone a ainsi été rendu public, tout comme les cachets des rôles principaux du film *The Interview*, qui doit sortir prochainement). Sans oublier des **milliers de mots de passe** (donnant accès à des services internes ou externes) que Sony conservait ingénument dans des fichiers bureautiques intitulés 'password'. Nos confrères du Monde dressaient hier un tableau – catastrophique – de la somme d'informations dérobées aux studios hollywoodiens.

L'attaque dont a été victime Sony repose notamment sur **un malware nommé Destover**. Les assaillants cherchaient non seulement à voler le maximum de données, mais ont également effacé les ordinateurs infectés (une façon d'effacer leurs traces). La diffusion de l'infection au sein de l'entreprise était telle au moment de sa découverte que Sony a passé des consignes à ses employés pour qu'ils **évitent de se connecter au réseau de l'entreprise**, de relever leurs e-mails, d'allumer leur ordinateur et d'activer le Wi-Fi sur leurs terminaux mobiles.

A lire aussi :

Piratage de Sony Pictures : les hackers cherchaient à détruire
Destover : le malware revient… et il est signé Sony !
Piratage : Mandiant et le FBI au chevet de Sony Pictures

Crédit photo : Ken Wolter / Shutterstock.com