# Destover : le malware revient… et il est signé Sony !

Alors que le groupe responsable de l'attaque contre Sony Pictures affirme avoir lâché dans la nature un nouveau lot de données dérobées aux studios, les chercheurs en sécurité alertent sur une **nouvelle version du malware Destover** utilisée pour pirater la filiale du Japonais. La particularité ? Cette mouture est signée par un certificat tout ce qu'il y de plus légitime… dérobé à Sony ! Les précédentes versions de Destover, elles, n'étaient pas signées.

Utiliser des malwares signés est une tactique rodée pour les auteurs de logiciels malveillants ; elle permet de **duper plus facilement les technologies de sécurité** qui ont tendance à se fier à ce type de fichiers. « *Parce que les certificats Sony sont reconnus par les solutions de sécurité, les attaques seront plus efficaces* », résume Kaspersky Lab.

## Destover, Shamoon, DarkSeoul : même combat ?

Cette version signée par Sony semble avoir été compilée en juillet dernier et a été signée le 5 décembre, au lendemain de la publication par Kaspersky Lab d'une analyse des moutures de Destover exploitées jusqu'alors. Rappelons que ce malware, utilisé dans de nombreuses attaques ces dernières années, ne se contente pas de s'immiscer sur des réseaux et de voler des données, il **détruit également des données**.

A ce propos, Kurt Baumgartner, l'auteur du billet de blog de Karspersky Lab analysant Destover, rapproche l'attaque contre Sony Pictures de Shamoon (visant le secteur de l'énergie au Moyen-Orient) et de DarkSeoul (ciblant la Corée du Sud), deux malwares intégrant eux aussi des charges destructrices. « *Dans les trois cas, les groupes revendiquant les actions destructrices de ces malwares sur des réseaux étendus n'avaient aucune histoire antérieure ou identité réelle* », remarque le chercheur. Qui note par ailleurs plusieurs bizarreries concernant les agissements de ces équipes de hackers : la volonté de disparaître une fois le vol commis, une communication peu claire, des forfaits s'appuyant sur **un événement « *politiquement chargé* »** suggéré comme étant la cause de l'attaque (dans le cas de Sony, la sortie du film *The Interview*). Kurt Baumgartner dresse une liste de similitudes entre les trois attaques. Insuffisant pour conclure à un commanditaire ou une équipe opérationnelle unique. Même si le chercheur écrit : « *il est extraordinaire que des actes de cyber-destruction massive aussi inhabituels et ciblés soient commis avec des similitudes clairement identifiables* ». Preuve que, au sein de la communauté de la cybersécurité, la thèse d'un groupe de hackers unique sponsorisé par un état prend du poids.

**A lire aussi :**

Piratage Sony Pictures : entre intimidations et localisation
Piratage de Sony Pictures : les hackers cherchaient à détruire
Piratage : Mandiant et le FBI au chevet de Sony Pictures

**crédit photo : © GlebStock / Shutterstock**