Qui a hacké Sony Pictures ? Une énigme digne d'un bon scénario de film

Sony Pictures ne semble pas encore savoir précisément comment a été menée et qui a orchestré l'attaque dont il a été la victime. Mais le studio hollywoodien tient à coup sûr là le scénario d'un futur blockbuster (en tout cas, un scénario un peu plus solide que celui de The Interview, le film qui lui a officiellement valu l'attaque la plus dévastatrice qu'ait connu une entreprise sur le sol des Etats-Unis à ce jour). Quelques jours après cet assaut – qui a forcé le studio à improviser un fonctionnement avec des téléphones portables, des comptes Gmail et un vieux stock de Blackberry exhumés pour l'occasion, son système d'information ayant été partiellement détruit -,la **responsabilité de la Corée du Nord** était pointée du doigt. Rappelons que le dictateur nord-coréen – Kim Jong Un – est la **cible du scénario du film** ***The Interview***.

Cette thèse d'un Etat s'en prenant à un studio pour un film qui déplait s'appuie, selon le FBI, sur l'identification de l'**infrastructure de commande et de contrôle du malware** de destruction de données utilisé par les pirates ainsi que sur des similitudes entre cette attaque et celle ayant visé des banques et des média sud-coréens en 2013, opération qui avait alors été attribuée au voisin du Nord. Si l'administration américaine maintient aujourd'hui cette version, des voix discordantes se font entendre.

La vengeance d'une ex-salariée licenciée ?

Se basant sur des données qu'elle a récupérées, la firme américaine de sécurité **Norse**, dont la réputation est solide, estime en effet qu'il n'y a **aucune preuve de l'implication des nord-coréens** dans l'attaque revendiquée par le groupe Guardians of Peace. Pour l'entreprise de sécurité, les auteurs de l'attaque seraient américains et canadiens. Un Singapourien serait également dans le coup.

Cette société met aussi en avant l'**implication d'une ex-salariée** – baptisée Lena – dans l'intrusion initiale qui a permis aux hackers de récupérer environ 100 To de données, puis de détruire massivement le système informatique de Sony Pictures. Selon Kurt Stammberger, l'un des dirigeants de Norse, Lena partageait avec les Guardians of Peace, un groupe d'activistes en lutte contre les mesures anti-piratage prises par Hollywood, une haine viscérale de Sony.

Employée pendant 10 ans des studios hollywoodiens avec un poste à responsabilité dans l'IT, Lena aurait été **licenciée en mai dernier**. D'ailleurs, Norse explique que la thèse de l'implication d'un salarié ou ex-salarié est renforcée par l'examen du malware exploité pour l'attaque : ce dernier a été **pré-compilé avec les adresses des serveurs Exchange et Active Directory** ainsi que celles d'autres machines du réseau interne de Sony Pictures où résidaient les données ciblées. « *Ce malware a été compilé avec certaines des clefs du royaume* », illustre Kurt Stammberger. Selon Norse, l'attaque a été orchestrée en plusieurs étapes et a démarré dès le mois de juillet.

Deux ou trois groupes de hackers

« *Lena avait les connaissances techniques pour faciliter ce type d'attaques* », juge Norse. En plus de cette ex-employée, la société a répertorié au moins cinq autres individus qu'elle estime liés à l'attaque contre Sony Pictures. Et d'évoquer des **échanges sur un forum underground en amont de l'opération** contre les studios. Dans une interview télévisée, Stammberger évoque même « *des complicités internes* ». Au pluriel.

En réalité, la thèse de Norse n'est pas totalement contradictoire avec celle du FBI. Chez nos confrères de DarkReading, Richard Bejtlich, un des dirigeants de **FireEye** (société qui enquête sur l'attaque pour le compte de Sony), explique : « *le débat sur l'attribution de l'attaque peut dépendre de la façon dont les observateurs définissent ce qu'est la responsabilité* ». En clair, nul besoin que les hackers soient contrôlés directement par la Corée du Nord pour que l'opération lui soit attribuée sur le plan politique. Et Bejtlich d'ajouter que le FBI n'aurait certainement pas pointé publiquement la responsabilité du pays asiatique – un geste à la portée politique lourde – sans éléments à charge convaincants. Rappelons que, suite aux conclusions du 'Bureau', le président Obama a dénoncé la responsabilité du régime de Kim Jong Un, entraînant un regain de tensions entre les deux pays.

Kurt Stammberger (Norse) reconnaît d'ailleurs qu'il est possible que l'exfiltration d'informations et la destruction de données qui a suivie soient le **résultat de deux ou trois attaques différentes**, menées par deux ou trois groupes de hackers différents partageant une cause commune. D'ailleurs, le FBI ne semble pas fermée à la thèse d'une complicité interne, les agents du 'Bureau' ayant rencontré les analystes de Norse la semaine dernière afin de permettre à ces derniers d'exposer en détail leurs conclusions.

Guardians of Peace voulait avant tout de l'argent

A moins que les éléments à charge jusqu'à présent évoqués par le FBI pour accuser la Corée du Nord ne soient de **fausses pistes** laissées par une autre organisation, pour mener les enquêteurs sur la piste du régime de Kim Jong Un, l'isolement international de ce dernier en faisant un coupable idéal.

Dernier élément troublant qui obscurcit encore le scénario de l'attaque : les premières revendications des hackers – en échange de la non publication des données dérobées – portaient sur de l'argent. Et non sur le film *The Interview*. Sur le compte Tweeter de Guardians of Peace, un groupe inconnu jusqu'au hack de Sony, on peut lire « *nous ne sommes pas coréens* » le 19 décembre – jour de l'intervention de Barack Obama – puis, le 30, « *nous sommes russes* ». Affirmation qui corrobore la thèse de la firme de conseil Taia Global qui, en se basant sur **l'analyse linguistique des communications** des hackers en direction de Sony, conclut que ces derniers sont **probablement originaires de Russie**. Et certainement pas de Corée.

A lire aussi :
Sony Pictures : la Corée du Nord aurait embauché des hackers mercenaires
Sony Pictures : le FBI et Georges Clooney accusent clairement la Corée du Nord
Sony Pictures : l'Empire contre-attaque… avec du DDoS

Crédit photo : Ken Wolter / Shutterstock