

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures



Des centaines de gigaoctets de fichiers ont déjà été diffusés par des pirates. Une situation catastrophique pour le géant du divertissement hollywoodien.

Imaginez que toutes les données – ou presque – qui transitent sur votre ordinateur de travail, stockées sur les disques durs et serveurs de votre entreprise, soient compilées et rendues accessibles à tous. Voilà la situation devant laquelle se retrouvent actuellement les employés et la direction de Sony Pictures Entertainment, après l'attaque informatique de grande ampleur subie le 24 novembre. Depuis, des milliers de gigaoctets de fichiers confidentiels du géant du divertissement hollywoodien, producteur et diffuseur de nombreux films, sont dispersés sur le Web.

Un mécanisme bien rodé

Les pirates, réfugiés derrière l'acronyme #GOP (pour Guardian of Peace), avaient au départ évoqué onze terabytes de documents (11 000 gigaoctets) subtilisés lors de leur attaque. Ils parlent maintenant de « dizaines de térabytes » de données – une centaine, disent les médias américains. Qu'un tel volume de données ait effectivement été volé semble de plus en plus probable. Les documents internes de Sony Pictures publiés (fichiers Excel, Word, Powerpoint, PDF, etc.) se comptent déjà par centaines de milliers et en dizaine de gigaoctets, selon un décompte fiable établi par l'entreprise spécialisée en sécurité informatique Risk Based Security. Le processus de diffusion est toujours le même. Des liens permettant de télécharger des fichiers RAR ou ZIP volumineux, par des sites de téléchargement direct ou grâce à des fichiers torrent, apparaissent sur l'éditeur de texte en ligne Pastebin, qui assure un certain anonymat à leurs auteurs. Les hackers envoient ensuite le lien du document Pastebin par e-mails à leurs contacts, soit n'importe qui ayant signifié son intérêt pour les documents Sony Pictures en écrivant aux adresses anonymes et temporaires que les membre de GOP diffusent régulièrement (journalistes, sympathisants des hackers, entreprises de sécurité informatique, enquêteurs, concurrents...).

```
1 Anyone who loves peace can be our member.
2 Please tell your friend at the email address below if you share our intention.
3 Peace comes when you and I share our intention!
4
5 Jack-William@beyondpeace11.com
6
7 You can download a part of Sony Pictures Internal data the volume of which is two of terabyte on the following address
8 These include many photos of confidential data
9
10 The data to be released must seen will excite you more.
11
12 Password: d5a9p333
13
14 1. Torrent
15 http://rapid.net/39439792
16 http://rapidshare.com/861766
17 http://bittorrent.com/rapidshare
18
19 http://hotfile.com/39439792/29p/sony_01.zip.htm
20 http://www.scribd.com/39439792/29p/sony_01.zip
21
```

Extrait d'un message donnant accès aux fichiers volés à Sony Pictures Entertainment. | Pastebin

Les données sont ensuite accessibles pendant quelques heures, avant la désactivation des liens de téléchargement par les hébergeurs et la suppression du document Pastebin – vraisemblablement sur requête des autorités ou de représentants légaux de Sony. Entre le 24 novembre et le 10 décembre, six « livraisons » de ce type ont eu lieu. Les pirates, maniant le sens du teasing, en promettent à chaque fois davantage : « les données que nous publierons la semaine prochaine vous exciteront encore plus », annonçait par exemple un document Pastebin publié le 5 décembre.

Un chantage pécuniaire ?

Les textes diffusés par les hackers qui accompagnent la publication de ces fichiers n'en disent en revanche que peu sur les motivations réelles justifiant cette fuite massive et organisée. La piste de la Corée du Nord, qui agirait en représailles au film The Interview parodiant le régime de Kim Jong-un, est accréditée par des similarités constatées entre l'attaque du 24 novembre et celle subie par la Corée du Sud en 2013. Mais l'un des cadres du FBI, officiellement chargé de l'enquête, a confié le 9 décembre qu'il n'était pour l'instant pas possible d'en attribuer la responsabilité à Pyongyang. Dans un document publié le même jour, les membres proclamés des GOP demandent bien à Sony d'« arrêter immédiatement de diffuser un film sur le terrorisme qui peut mettre fin à la paix régionale et causer une guerre », sans nommer le film en question, et reprenent une rhétorique déjà servie auparavant à The Verge. Mais ils signalent également avoir « formulé une demande claire à l'équipe dirigeante de Sony », encore une fois sans préciser laquelle :

« Ils ont refusé de l'accepter. On dirait que vous pensez que tout se passera bien, si vous trouvez les attaquants et ne réagissez pas à notre demande. Nous vous avertissons à nouveau. Répondez à ce que nous vous demandons si vous voulez nous échapper. »

De quoi donner du crédit à l'hypothèse d'une tentative d'extorsion de fonds de la part des hackers de « Guardian of Peace ». Ce motif a d'ailleurs été clairement exposé dans un e-mail envoyé aux dirigeants de Sony Pictures quelques jours avant l'attaque : « Nous avons de quoi causer beaucoup de tort à Sony Pictures. (...) Nous voulons une compensation monétaire. Payez, ou Sony Pictures sera frappé dans son ensemble. »

La diffusion au compte-gouttes des documents confidentiels constituerait, dans ce contexte, un moyen de pression supplémentaire pour obtenir cette « compensation », de nature à alimenter un feuilleton médiatique dévastateur pour Sony Pictures. Les médias du monde entier ont ainsi repris :

Les données privées de célébrités

Des adresses postales, des numéros de téléphone, des adresses électroniques, ou encore le numéro de sécurité sociale de Sylvester Stallone, contenus dans les documents liés aux films et séries de Sony Pictures ont été rendus publics. Parmi ces informations, on trouve les pseudonymes utilisés par Tom Hanks, Natalie Portman ou encore Ice Cube pour conserver un peu de tranquillité (lors d'une réservation d'hôtel par exemple). On également été publiés une cote de popularité des acteurs pays par pays, ou encore les sommes d'argent perçues par Seth Rogen et James Franco pour le film The Interview. Le premier aurait reçu 8,4 millions de dollars pour avoir coréalisé et interprété l'un des rôles principaux, le second 6,5 millions : des divulgations auxquelles ils ont réagi avec humour.



L'affiche de « The Interview ». | Sony Pictures

Les données privées des salariés et partenaires de Sony Pictures

Numéros de téléphone, CV, photos d'identité, montants de salaires, demandes d'augmentation, e-mails, planning de vacances, factures médicales... Autant d'éléments propres à la vie interne d'une structure qui emploie près de 7 000 personnes aux Etats-Unis, et qui a collaboré avec de très nombreuses personnes ces dernières années – stagiaires, prestataires ou partenaires directs au sein d'entreprises rachetées par Sony, comme Columbia Pictures. Ces détails apparaissent notamment dans un dossier intitulé « Ressources humaines », et se trouvent aussi dans des documents de travail liés aux tournages de films et de séries Sony. Encore plus grave, de très nombreux mots de passe utilisés par les employés pour se connecter à tous types de services (propres à Sony Pictures, mais aussi ailleurs sur Internet) font partie des publications. Comme le note cruellement Gizmodo, ils étaient stockés sur les disques durs de Sony Pictures dans des fichiers Word et Excel sans protection, et dans un dossier appelé « Mot de passe ».

```
1 @Info server storage migration
2 @2015 Passwords
3 @Important Passwords - TAAI, Outlook, Novel
4 @IP and Password
5 @IT Security Assessment Questions for PDSM
6 @ITP Internal Passwords 08_24_2014
7 @Users Passwords
8 @Logon and Passwords
9 @Logon Passwords_Corpus
10 @Logon and Passwords
11 @Network Application List
12 @Network Server List
13 @Network Server List
14 @Network Server List
15 @Network Server List
16 @Network Server List
17 @Network Server List
18 @Network Server List
19 @Network Server List
20 @Network Server List
21 @Network Server List
22 @Network Server List
23 @Network Server List
24 @Network Server List
25 @Network Server List
26 @Network Server List
27 @Network Server List
28 @Network Server List
29 @Network Server List
30 @Network Server List
31 @Network Server List
32 @Network Server List
33 @Network Server List
34 @Network Server List
35 @Network Server List
36 @Network Server List
37 @Network Server List
38 @Network Server List
39 @Network Server List
40 @Network Server List
41 @Network Server List
42 @Network Server List
43 @Network Server List
44 @Network Server List
45 @Network Server List
46 @Network Server List
47 @Network Server List
48 @Network Server List
49 @Network Server List
50 @Network Server List
51 @Network Server List
52 @Network Server List
53 @Network Server List
54 @Network Server List
55 @Network Server List
56 @Network Server List
57 @Network Server List
58 @Network Server List
59 @Network Server List
60 @Network Server List
61 @Network Server List
62 @Network Server List
63 @Network Server List
64 @Network Server List
65 @Network Server List
66 @Network Server List
67 @Network Server List
68 @Network Server List
69 @Network Server List
70 @Network Server List
71 @Network Server List
72 @Network Server List
73 @Network Server List
74 @Network Server List
75 @Network Server List
76 @Network Server List
77 @Network Server List
78 @Network Server List
79 @Network Server List
80 @Network Server List
81 @Network Server List
82 @Network Server List
83 @Network Server List
84 @Network Server List
85 @Network Server List
86 @Network Server List
87 @Network Server List
88 @Network Server List
89 @Network Server List
90 @Network Server List
91 @Network Server List
92 @Network Server List
93 @Network Server List
94 @Network Server List
95 @Network Server List
96 @Network Server List
97 @Network Server List
98 @Network Server List
99 @Network Server List
100 @Network Server List
```

Les mots de passes de Sony Pictures. | Risk Blaised Security

De quoi pousser d'anciens employés à réfléchir à une plainte collective, arguant du manque flagrant de sécurité du réseau de l'entreprise. « Il y a des raisons de penser qu'il y a eu une grosse négligence de la part de [Sony Pictures]. Nous nous inquiétons tous concernant notre vie privée, et nos familles », a déclaré l'un d'entre eux à Fox News, après avoir vu diffuser son passeport, son visa, son numéro de sécurité sociale et ses contrats passés avec l'entreprise.

Des avocats californiens incitent également les salariés actuels à se lancer dans de telles procédures. Particulièrement exposés, ils se sont vus en plus directement menacés dans un e-mail leur étant adressé. « Tout le monde panique, et personne ne sait quoi faire », a témoigné l'un d'eux sur le site Fusion, décrivant une hostilité grandissante au sein de Sony Pictures à l'encontre du service informatique. Le FBI, chargé de l'enquête, devrait faire le point devant les employés sur le comportement à adopter face à cette situation le 12 décembre.

Les dirigeants de Sony Pictures ne sont pas épargnés. L'un des premiers documents diffusés par le site d'information Fusion dresse le détail des rémunérations des 17 salariés les mieux payés, à commencer par le dirigeant Michael Lynton (3 millions de dollars par an) – une seule femme dans ce palmarès. Parmi les fichiers publiés figurent des sauvegardes de plusieurs mois de conversations par courriels (professionnels et personnels) issues des messageries Outlook de cadres de l'entreprise : Amy Pascal, vice-présidente de Sony Pictures, Steve Mosko, à la tête de Sony Television, ou encore Leah Weill, conseiller juridique en chef.

Des révélations sur les films et les séries Sony

Dans son ensemble, cette masse de données fournille d'informations sur la manière dont Sony Pictures gère son catalogue, ses productions et ses projets. Finances de l'entreprise, projets marketing, bilans comptables liés aux séries diffusées à la télévision américaine, rétrospectives annuelles, bases de contacts, documents préparatoires pour des négociations... Ces milliers de fichiers bruts s'accompagnent de visées stratégiques, comme en témoignent les points de vue exprimés par des employés (s'énervant par exemple contre l'omniprésence d'Adam Sandler à l'écran). Dans ces documents se nichent ainsi, fatalement, des informations propres aux films et aux séries télévisées estampillées Sony. On y apprend par exemple comment les dirigeants de Sony Pictures ont fait modifier la fin du film The Interview (attention spoiler !), et négocié avec Marvel, qui souhaitait que Spiderman apparaisse dans le prochain Captain America. Plus problématique, des scripts inédits d'épisodes de séries, et même de films devant sortir en 2015, ont été repérés. Plusieurs médias, comme le Wall Street Journal, ont également extrait diverses phrases chocs des e-mails échangés ces dernières années par la vice-présidente Amy Pascal avec le tout-Hollywood (réalisateurs, agents, stars, etc.). On y trouve quelques commentaires désobligeants sur des acteurs : Angelina Jolie et son « ego devastateur » en prennent pour leur grade. Ou encore, une chronique détaillée des négociations et conversations, parfois brisée de décoffrage, entourant le biopic sur Steve Jobs sur lequel Sony travaille depuis trois ans (notamment sur les choix de casting du scénariste Aaron Sorkin, qui avait songé à Tom Cruise pour incarner le fondateur d'Apple).

En savoir plus sur http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html#0x8W3PwS6l8JjU0T.99
Par Michaël Szadkowski journaliste à Pixels

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html
par Par Michaël Szadkowski