

Sony fait face au plus grand vol d'identités de l'histoire

Sony découvre peu à peu l'ampleur du pillage de données personnelles dont elle a été victime. Les comptes de 100 millions de joueurs, dont de nombreux Suisses, seraient aux mains de hackers. Et ce n'est peut-être pas terminé.



Image © Keystone / Lors d'une conférence de presse au Japon, Kazuo Hirai, président de Sony Computer Entertainment (au centre), s'est excusé auprès des joueurs du monde entier.

Trois semaines de cauchemar. Depuis que des ingénieurs américains de Sony ont détecté une activité suspecte sur certains serveurs le 19 avril, les mauvaises nouvelles se succèdent.

Dans un premier temps, le géant japonais annonce que son PlayStation Network, le réseau qui permet aux joueurs du monde entier de rivaliser en ligne, ainsi que Qriocity, un service de vidéo à la demande, ont été piratés. Les hackers auraient eu accès aux données

personnelles, dont des numéros de cartes de crédit, de 77 millions de comptes. Une fuite de données spectaculaire, au point que le président de Sony Computer Entertainment, Kazuo Hirai, s'en est excusé publiquement.

Malheureusement pour lui, l'affaire ne s'arrête pas là. Quelques jours plus tard, ses équipes découvrent qu'un autre service de jeu en ligne dédié cette fois aux PC, Sony Online Entertainment, 24,6 millions d'inscrits, a aussi été piraté.

430 000 comptes suisses

«Avec plus de 100 millions de comptes touchés au total, c'est la plus grosse affaire de piratage de l'histoire, tranche Guillaume Lovet, spécialiste français en cybercriminalité et en sécurité informatique chez Fortinet. Il y a bien eu les 110 millions de numéros de cartes de crédit volés au système de paiement Heartland, mais, dans le cas de Sony, ce ne sont pas uniquement des coordonnées bancaires qui ont été volées: il s'agit des identités complètes. C'est donc bien plus grave.» Dans les bases de données du PlayStation Network figuraient les noms, prénoms, adresses, dates de naissance et numéros de téléphone des joueurs. Les informations bancaires étaient encryptées, assure Sony, qui ne précise pas de quelle manière.

Les joueurs suisses n'ont pas été épargnés par le piratage. Rien que pour le PlayStation Network, 430 000 comptes sont concernés. «Environ 60 000 avaient fourni un numéro de carte de crédit», précise Angela Blank, de Sony Suisse. La porte-parole n'était pas en mesure vendredi soir d'indiquer le nombre de comptes helvétiques touchés par le second piratage, celui du Sony Online Entertainment.

Suite ↓

Peu de détails techniques sur l'attaque ont filtré. Pour certains experts, les pirates auraient exploité des failles connues dans les logiciels utilisés par Sony. Pour des raisons qui restent à déterminer, l'entreprise japonaise aurait omis de mettre à jour ses serveurs.

Dans une lettre au Congrès américain qui lui demandait des comptes, Sony a indiqué avoir retrouvé sur l'un des serveurs piratés un fichier baptisé «Anonymous», du nom d'un célèbre groupe de hackers. Le fichier contenait un fragment de leur slogan: «We are legion». Ce collectif très secret, qui fonctionne sans structure hiérarchique, s'est récemment illustré en attaquant les sites de plusieurs établissements financiers en réponse à leur décision de bloquer les versements à WikiLeaks.

Mais attention aux conclusions hâtives: «Tout le monde peut créer un fichier de ce type, ce n'est pas une preuve», met en garde Sergio Domingues, ingénieur sécurité chez SCRT à Prévèrenges (VD). Contrairement à une scène de crime, les indices numériques sont aisément falsifiables.

Dans un communiqué envoyé cette semaine, l'organisation nie d'ailleurs toute implication dans le piratage. Sa ligne de défense? Anonymous ne vole pas. «C'est vrai qu'habituellement leur technique est de mettre hors service des serveurs en les bombardant de requêtes grâce à des milliers d'ordinateurs zombies», explique Brian Mariani, consultant en sécurité chez High Tech Bridge à Genève.

Un argument qui ne convainc pas Guillaume Lovet: «Peut-être que le vol de données n'était pas le but premier de l'attaque. Jusqu'ici, il semble que ces informations n'aient pas été utilisées, ni revendues. Plus le temps passe, plus il sera difficile de les vendre, surtout avec le FBI sur le dos.» Pour cet expert, la principale cible de cette attaque n'est pas le joueur, mais bien Sony.

Sony avait fâché les hackers

Anonymous, justement, a une dent contre Sony. L'entreprise de divertissement s'est mis à dos la communauté de hackers en faisant condamner l'un des leurs: GeoHot. Cet Américain de 21 ans avait déverrouillé la PlayStation 3 puis mis à disposition ses clés de décryptage. Le hacker était allé jusqu'à mettre en ligne une vidéo expliquant pas à pas aux débutants comment réaliser ce tour de force, qui permet notamment de jouer à des jeux piratés ou conçus pour les précédents modèles de console. Le procès de GeoHot, qui n'en est pas à son coup d'essai puisqu'il avait déjà été le premier à déverrouiller l'iPhone en 2007, avait valu à Sony une élégante déclaration de cyberguerre: «Votre action contre GeoHot est impardonnable [...] Vous avez vu un nid de frelons, et vous y avez enfoncé vos pénis. Vous allez devoir en payer les conséquences», écrivaient, début avril, les membres d'Anonymous. Simple coïncidence avec les attaques contre les réseaux de jeu en ligne? Un autre groupe de hackers a-t-il profité de la situation, faisant d'Anonymous le bouc émissaire idéal? Trop tôt pour le dire.

Suite ↓

Réseaux toujours hors service

Pendant ce temps, les joueurs ne pouvaient toujours pas se connecter sur les réseaux de Sony hier en fin de journée. La firme a affirmé vouloir «prendre son temps» avant de rétablir ses services et n'ose plus avancer de date de remise en service. Un manque à gagner auquel pourraient s'ajouter les frais de plusieurs actions en justice intentées par des utilisateurs et surtout un dégât d'image considérable. «Et il n'y a pas de raisons que les hackers se soient arrêtés aux jeux en ligne, craint Guillaume Lovet. Je ne serais pas surpris d'apprendre que des données internes à l'entreprise aient été dérobées.» Pour Sony, le cauchemar n'est certainement pas terminé.

RAPPEL DES FAITS

19 avril

En fin de journée, l'équipe réseau de Sony USA détecte une activité suspecte sur ses serveurs.

20 avril

Les ingénieurs repèrent des transferts de données vers l'extérieur non autorisés. Sony désactive ses services PlayStation Networket Qriocity, prétextant une maintenance. Elle fait appel à des experts externes.

22 avril

Sony prend discrètement contact avec le FBI.

26 avril

L'entreprise informe ses clients qu'elle a subi une attaque et que des données personnelles ont pu être dérobées entre le 17 et le 19 avril. Sony est critiquée pour avoir autant attendu avant de communiquer.

1er mai

Sony s'excuse publiquement et promet que ses services seront de nouveau bientôt en ligne.

3 mai

Nouveau coup de théâtre: Sony avoue qu'un autre service de jeu en ligne, Sony Online Entertainment, a aussi été piraté, les 16 et 17 avril.