

Colonial Pipeline : des données personnelles ont aussi été dérobées

Trois mois après que les approvisionnements en carburant de la côte est des États-Unis aient été [paralysés par une attaque](#) de ransomware, Colonial Pipeline a admis que des données personnelles avaient également été volées.

S'adressant à CNN , un porte-parole de l'entreprise a confirmé que l'attaque de ransomware en mai dernier avait compromis les informations personnelles de près de 6 000 personnes.

Le problème a commencé le vendredi 7 mai de cette année, lorsque Colonial Pipeline a été attaqué par DarkSide, ce qui a entraîné une pénurie généralisée de carburant sur la côte est des États-Unis.

Une nouvelle attaque de Darkside

Colonial Pipeline a payé les hackers de DarkSide pour restaurer ses systèmes informatiques. Son PDG, Joseph Blount a autorisé [un paiement de rançon](#) de 4,4 millions \$ (75 Bitcoin) au motif qu'il ignorait combien de temps il faudrait pour les rétablir.

Les chercheurs en sécurité d' Eiptic, basé à Londres, [ont par la suite identifié](#) le portefeuille numérique Bitcoin utilisé par DarkSide pour extraire des rançons de leurs victimes. Et en juin, le ministère de la justice américain a saisi 63,7 bitcoins dans le cadre d'une récupération de rançon .

Outre les systèmes informatiques paralysés à Colonial Pipeline, les pirates de DarkSide auraient également volé les données personnelles de milliers de personnes.

[Bleeping Computer](#) a d'abord signalé que Colonial Pipeline envoyait des lettres de notification selon lesquelles il avait « récemment appris » que DarkSide était également en mesure de collecter et d'exfiltrer des documents contenant des informations personnelles sur un total de 5 810 personnes lors de leur attaque.

Colonial Pipeline : des données de salariés exfiltrées

Les 5 810 personnes touchées sont principalement des employés actuels ou anciens de l'entreprise et des membres de leur famille, a déclaré à CNN un porte-parole de Colonial Pipeline.

La lettre explique que les pirates auraient eu accès à des dossiers, y compris des noms ; informations de contact; dates de naissance; numéros de sécurité sociale, de permis de conduire et d'identification militaire ; et des informations sur l'assurance maladie – qui peuvent toutes être utilisées pour de futurs exploits.

« Bien que notre système soit maintenant pleinement opérationnel, nous avons travaillé d'arrache-pied avec des experts tiers en cybersécurité pour déterminer quelles informations personnelles, le cas échéant, ont pu être affectées à la suite de l'attaque », a déclaré le porte-parole de la société à CNN.

Lire [l'article original](#) de Tom Jowitt