

Colonial Pipeline ransomware

كانت شركة Colonial Pipeline ضحية لهجوم فدية في مايو 2021. وقد أصابت بعض الأنظمة الرقمية لخط الأنابيب، مما أدى إلى إغلاقها لعدة أيام.



أثر الإغلاق على المستهلكين وشركات الطيران على طول الساحل الشرقي. واعتبر الاختراق تهديدًا للأمن القومي، حيث ينقل خط الأنابيب النفط من المصافي إلى أسواق الصناعة. ودفع هذا الرئيس جو بايدن إلى إعلان حالة الطوارئ.

ما هو اختراق خط الأنابيب الاستعماري؟

يعد اختراق خط أنابيب Colonial Pipeline أكبر هجوم إلكتروني تم الكشف عنه علنًا ضد البنية التحتية الحيوية في الولايات المتحدة.

شمل الهجوم مراحل متعددة ضد أنظمة تكنولوجيا المعلومات الخاصة بشركة Colonial Pipeline. لم تتعرض أنظمة التكنولوجيا التشغيلية لخط الأنابيب التي تنقل النفط فعليًا للخطر بشكل مباشر أثناء الهجوم.

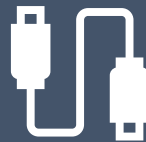
من كان المسؤول عن اختراق خط الأنابيب الاستعماري؟

تم التعرف على قراصنة

Colonial Pipeline

كمجموعة تعرف باسم

DarkSide



الجدول الزمني لهجوم خط الأنابيب الاستعماري
تم الهجوم على خط الأنابيب الاستعماري والتعافي منه بوتيرة سريعة في فترة قصيرة من الزمن.

6 مايو 2021

التطفل الأولي وسرقة البيانات.

7 مايو 2021

يبدأ هجوم برامج الفدية.

أصبح خط الأنابيب الاستعماري على علم بالانتهاك.

واستدعت شركة الأمن Mandiant للتحقيق في الهجوم والرد عليه.

وأبلغت سلطات إنفاذ القانون والسلطات الحكومية الفيدرالية بالهجوم.

تم قطع خط الأنابيب عن العمل لتقليل مخاطر التعرض للشبكة التشغيلية.

تدفع شركة Colonial Pipeline فدية قدرها 75 بيتكوين (4.4 مليون دولار)

9 مايو 2021

إعلان الطوارئ من قبل الرئيس جو بايدن.

12 مايو 2021

تم إعادة تشغيل خط الأنابيب مع استئناف العمليات العادية.

7 يونيو 2021

استعادت وزارة العدل 63.7 بيتكوين -حوالي 2.3 مليون دولار -من المهاجمين.

8 يونيو 2021

جلسة استماع في الكونجرس بشأن الهجوم.

رغد