

ประจำวันจันทร์ที่ 19 กันยายน 2565

บริการรถพยาบาลในนิวยอร์กเปิดเผยถึงข้อมูล รั่วไหลหลังจากการโจมตีด้วยแรนซัมแวร์

Empress EMS (Emergency Medical Services) ผู้ให้บริการฉุกเฉินและบริการรถพยาบาลในนิวยอร์ก ได้เปิดเผยการโจมตีที่ทำให้ข้อมูลลูกค้ารั่วไหล บริษัทได้ประสบกับการโจมตีด้วยแรนซัมแวร์ตั้งแต่วันที่ 14 กรกฎาคม พ.ศ. 2022 จากการสอบสวนพบว่าผู้โจมตีได้เข้าถึงระบบของ Empress EMS เมื่อวันที่ 26 พฤษภาคม พ.ศ. 2022 ต่อมาในวันที่ 13 กรกฎาคม แอ็กเกอร์ได้กรองไฟล์ชุดย่อยก่อนนำไปใช้ในการเข้ารหัส โดยไฟล์เหล่านี้บางไฟล์มีชื่อผู้ป่วย วันที่ให้บริการ ข้อมูลการประกัน และ หมายเลขประกันสังคม

รายละเอียดของการโจมตีเรียกค่าไถ่แบบ double-extortion เป็นมาตรฐานที่อาชญากรไซเบอร์ใช้ขโมยไฟล์ เพื่อเข้ารหัสระบบ แล้วข่มขู่เหยื่อว่าจะเผยแพร่ข้อมูล เว้นแต่จะมีการจ่ายค่าไถ่ ถึงแม้ว่าบริษัทจะไม่กล่าวถึงกลุ่มในการโจมตี แต่ BleepingComputer พบว่ากลุ่ม ransomware ของ Hive ได้เตรียมการเปิดเผยข้อมูลต่อสาธารณะสำหรับการรั่วไหลของข้อมูล Empress EMS เมื่อวันที่ 26 กรกฎาคม

Empress EMS ได้แจ้งกระทรวงสาธารณสุขของสหรัฐฯ ว่าจำนวนรายการที่ได้รับผลกระทบจากเหตุการณ์นี้ประมาณ 318,55 รายการ ซึ่งอย่างไรก็ตามอาจมีผู้ได้รับผลกระทบมากขึ้น และผู้ที่ไม่ได้รับจดหมายแต่สามารถยืนยันได้ว่าใช้บริการของ Empress EMS ผ่านใบแจ้งยอดการรักษาพยาบาล ควรติดต่อบริษัทภายในวันที่ 9 ตุลาคม พ.ศ. 2565 เพื่อรับประโยชน์จากบริการตรวจสอบเครดิต