ประจำวันอังคารที่ 2 สิงหาคม 2565

แก๊งแรนซัมแวร์ BlackCat อ้างความรับผิดชอบการโจมตีท่อส่งก๊าซในยุโรป

แก๊งแรนซัมแวร์ ALPHV หรือที่รู้จักในชื่อ BlackCat อ้างความรับผิดชอบในการโจมตีทางไซเบอร์กับ Creos Luxembourg SA ซึ่งเป็นผู้ให้บริการท่อส่งก๊าซธรรมชาติและเครือข่ายไฟฟ้าในประเทศแถบยุโรปกลาง โดย Encevo เจ้าของ Creos ซึ่งเป็นผู้ส่งพลังงานใน 5 ประเทศในสหภาพยุโรป ได้ประกาศเมื่อวันที่ 25 กรกฎาคม ว่าพวกเขาถูกโจมตีทางอินเทอร์เน็ตเมื่อสุดสัปดาห์ที่ผ่านมาในช่วงระหว่างวันที่ 22 ถึง 23 กรกฎาคม ซึ่งการโจมตีทางไซเบอร์ส่งผลให้พอร์ทัลลูกค้าของ Encevo และ Creos ไม่สามารถใช้งานได้ แต่ก็ไม่มีการหยุดการบริการ และเมื่อวันที่ 28 กรกฎาคม บริษัทได้โพสต์อัปเดตเกี่ยวกับการโจมตีทางไซเบอร์ โดยผลการสอบสวนเบื้องต้นระบุว่าผู้โจมตีได้ขโมยข้อมูลจำนวนหนึ่งจากระบบไป

โดยแก๊งแรนซัมแวร์ ALPHV/BlackCat ได้เพิ่ม Creos ลงในเว็บไซต์ที่ใช้เรียกค่าไถ่เมื่อวันเสาร์ โดยขู่ว่าจะเผยแพร่ไฟล์ที่ขโมยมา 180,000 ไฟล์ ซึ่งมีขนาดรวม 150 GB ซึ่งรวมถึงสัญญา ข้อตกลง หนังสือเดินทาง ตั๋วเงิน และอีเมล แม้ว่าจะยังไม่มีการประกาศเวลาที่แน่นอนสำหรับการดำเนินการนี้ แต่ผู้โจมตีก็จะเปิดเผยภายในวันจันทร์

ALPHV/BlackCat เพิ่งเปิดตัวแพลตฟอร์มแรนซัมแวร์ใหม่ ที่พวกเขาทำให้ข้อมูลที่ถูกขโมยสามารถค้นหาได้โดยผู้เข้าชม โดยมีเป้าหมายเพื่อเพิ่มแรงกดดันต่อเหยื่อของพวกเขาในการทำให้พวกเขาต้องจ่ายค่าไถ่ โดยเป็นที่รู้กันว่า BlackCat เป็นการดำเนินการรีแบรนด์ของ DarkSide ซึ่งปิดตัวลงภายใต้แรงกดดันจากการบังคับใช้กฎหมาย หลังจากการโจมตี ransomware กับ Colonial Pipeline ซึ่งหลังจากปิด DarkSide แล้ว มีการเปลี่ยนชื่อเป็น BlackMatter เพื่อหลบเลี่ยงการบังคับใช้กฎหมาย แต่แรงกดดันยังคงดำเนินต่อไป ทำให้แก๊งค์ต้องปิดตัวลงอีกครั้ง แต่เมื่อเดือนพฤศจิกายน พ.ศ. 2564 ก็ได้มีผู้คุกคามเปิดตัวใหม่เป็น BlackCat/ALPHV ซึ่งมักจะหลีกเลี่ยงเป้าหมายใหญ่ของอเมริกาและพุ่งเป้าหมายไปที่หน่วยงานในยุโรปแทน

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/