วันที่ 25 พฤศจิกายน 2568

CrowdStrike จับผู้มีอิทธิพลภายในที่ส่งข้อมูลให้กับแฮกเกอร์

เกิดความปั่นป่วนครั้งใหญ่ในวงการความปลอดภัยทางไซเบอร์ เมื่อบริษัทไซเบอร์ยักษ์ใหญ่อย่าง CrowdStrike ยืนยันว่ามีพนักงานภายในแชร์ภาพหน้าจอจากระบบของบริษัทให้กับกลุ่มแฮ็กเกอร์ Scattered Lapsus$ Hunters แต่เน้นย้ำว่าระบบหลักของบริษัทและข้อมูลลูกค้ายังคงปลอดภัย

เหตุการณ์ที่เกิดขึ้นและคำชี้แจงของ CrowdStrike

- การยืนยันบริษัท: CrowdStrike ยอมรับว่าได้ตรวจพบและยุติการทำงานของพนักงานต้องสงสัยเมื่อเดือนที่แล้ว หลังจากการสอบสวนภายในพบว่าเขาได้นำภาพหน้าจอจากคอมพิวเตอร์ของตนไปเผยแพร่ภายนอก
- CrowdStrike ยืนยัน: "ระบบของเราไม่เคยถูกแฮ็ก และลูกค้าของเรายังคงปลอดภัยตลอดเวลา เราได้ส่งเรื่องนี้ให้หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องดำเนินการแล้ว"
- การเผยแพร่: ภาพหน้าจอระบบภายในของ CrowdStrike ถูกโพสต์ลงบน Telegram โดยสมาชิกของกลุ่มแฮ็กเกอร์ ShinyHunters, Scattered Spider, และ Lapsus$

คำอ้างของกลุ่มแฮ็กเกอร์ (Scattered Lapsus$ Hunters)

กลุ่ม ShinyHunters ได้บอกกับ BleepingComputer ว่าพวกเขาตกลงจะจ่ายเงินให้พนักงานคนดังกล่าว 25,000 ดอลลาร์ เพื่อให้เข้าถึงเครือข่ายของ CrowdStrike

- ข้อมูลที่อ้างว่าได้: กลุ่มแฮ็กเกอร์อ้างว่าได้รับคุกกี้ SSO ที่ใช้ยืนยันตัวตนจากพนักงานรายนี้ แต่ในตอนนั้นพนักงานต้องสงสัยได้ถูก CrowdStrike ตรวจพบและปิดการเข้าถึงเครือข่ายไปแล้ว
- เป้าหมายอื่น: พวกเขายังอ้างว่าพยายามซื้อรายงานของ CrowdStrike ที่เกี่ยวกับกลุ่ม ShinyHunters และ Scattered Spider แต่ไม่ได้รับข้อมูลดังกล่าว

โครงข่ายอาชญากรรมไซเบอร์ที่อันตราย (The Scattered Lapsus$ Hunters)

กลุ่มที่ตอนนี้เรียกตัวเองว่า “Scattered Lapsus$ Hunters” เป็นเครือข่ายอาชญากรรมไซเบอร์ที่อันตรายอย่างยิ่งและมีประวัติการโจมตีที่กว้างขวาง

- การโจมตี Salesforce ระลอกใหญ่: กลุ่มนี้ได้โจมตีลูกค้าของ Salesforce ผ่านการโทรหลอก (voice phishing) มาตั้งแต่ต้นปี โดยมีบริษัทใหญ่ ๆ ที่ตกเป็นเป้าหมาย เช่น Google, Cisco, Allianz Life, Farmers Insurance, Qantas, Adidas, Workday รวมถึงบริษัทในเครือ LVMH (Dior, Louis Vuitton, Tiffany & Co.)
- การพยายามแบล็กเมล: พวกเขาพยายามแบล็กเมลแบรนด์และองค์กรชื่อดังต่าง ๆ จำนวนมาก รวมถึง Toyota, Instacart, Cartier, Adidas, Sake Fifth Avenue, Air France & KLM, FedEx, Disney/Hulu, Home Depot, Marriott, Gap, McDonald's, Walgreens, Transunion, HBO MAX, UPS, Chanel และ IKEA
- ความเสียหายมหาศาล: พวกเขายังอ้างว่าอยู่เบื้องหลังการแฮ็ก Jaguar Land Rover (JLR) ซึ่งสร้างความเสียหายกว่า 196 ล้านปอนด์ (220 ล้านดอลลาร์) ในไตรมาสที่ผ่านมา
- การเปลี่ยนกลยุทธ์ Ransomware: กลุ่ม ShinyHunters และ Scattered Spider ได้เปลี่ยนไปใช้แพลตฟอร์ม Ransomware-as-a-Service ใหม่ชื่อ ShinySp1d3r หลังจากเคยใช้ตัวเข้ารหัสของแก๊งอื่น ๆ มาก่อน (เช่น ALPHV/BlackCat, RansomHub, Qilin และ DragonForce)

การโจมตี Salesforce ล่าสุด (280 บริษัท)

เมื่อเร็ว ๆ นี้ ShinyHunters ยังอ้างถึงการขโมยข้อมูลระลอกใหม่ที่ส่งผลกระทบต่อลูกค้า Salesforce ของบริษัทกว่า 280 แห่ง โดยอ้างว่าได้ข้อมูลหลังการแฮ็ก Gainsight โดยใช้ข้อมูลลับที่ถูกขโมยมาในเหตุการณ์ Salesloft drift breach

- รายชื่อที่ถูกอ้างถึง: LinkedIn, GitLab, Atlassian, Thomson Reuters, Verizon, F5, SonicWall, DocuSign และ Malwarebytes
- การปฏิเสธของ DocuSign: DocuSign ได้ติดต่อกลับมาเพื่อปฏิเสธคำอ้างนี้ โดยระบุว่า "หลังจากวิเคราะห์บันทึกและตรวจสอบภายในอย่างละเอียด เราไม่พบสัญญาณใด ๆ ที่บ่งบอกว่ามีข้อมูลของ DocuSign รั่วไหล"

ข้อมูลอ้างอิง

Nov 21, 2025, By Sergiu Gatlan

- https://www.bleepingcomputer.com/news/security/crowdstrike-catches-insider-feeding-information-to-hackers/