ประจำวันศุกร์ที่ 23 กันยายน 2565

LinkedIn Smart Links ถูกใช้ประโยชน์ในการโจมตีแบบ email phishing

ผู้โจมตีได้ใช้ลักษณะของ Smart Link ของ LinkedIn เพื่อเลี่ยงผ่านการรักษาความปลอดภัยอีเมล และเปลี่ยนเส้นทางผู้ใช้งานที่เป็นเป้าหมายไปยังหน้า phishing ที่ใช้ในการขโมยข้อมูลการชำระเงิน ซึ่ง Smart Link มีลักษณะสงวนไว้สำหรับผู้ใช้ LinkedIn Sales Navigator และ Enterprise เท่านั้นที่ทำให้สามารถส่งเอกสารได้ถึง 15 ชุดโดยใช้ลิงก์เดียวได้ ดังนั้น Smart Link ไม่ใช่ใช้แค่เพื่อเลี่ยงการป้องกันการรักษาความปลอดภัยอีเมลเท่านั้น แต่ยังสามารถรับข้อมูลเชิงลึกที่เกี่ยวข้องกับแคมเปญได้ด้วย

email phishing ถูกส่งไปที่เป้าหมายใน Slovenská pošta โดยเป็นผู้ให้บริการไปรษณีย์ของรัฐในสโลวาเกีย เพื่อแจ้งให้ผู้รับทราบถึงความจำเป็นในการรับผิดชอบค่าใช้จ่ายสำหรับพัสดุที่รอการจัดส่ง ซึ่งใช้วิธีในส่วนหัวของอีเมลทำให้ที่อยู่ปรากฏถูกต้องสำหรับผู้รับ แต่ถ้าตรวจสอบอย่างละเอียด จะเห็นได้ชัดว่าผู้ส่งคือ sis.sk@augenlabs.com จริงๆแล้ว ไม่มีความเกี่ยวข้องกับการบริการของไปรษณีย์ โดยมีปุ่มที่กดยืนยันฝังไว้ในเพื่อเปลี่ยนเส้นทางเหยื่อไปยังหน้า phishing ซึ่งในขณะที่แคมเปญนี้มุ่งเป้าไปที่ประเทศสโลวาเกีย

โดย BleepingComputer ได้ติดต่อ LinkedIn เพื่อสอบถามว่าพวกเขามีแผนที่จะใช้มาตรการป้องกันเพื่อป้องกันการละเมิดนี้หรือไม่ แต่เรายังไม่ได้รับการตอบกลับ

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/linkedin-smart-links-abused-in-evasive-email-phishing-attacks/