

ประจำวันพุธที่ 21 กันยายน 2565

การโจมตีแบบ Phishing ล่อลวงข้อมูลประจำตัว ของบัญชี Microsoft 365 ที่แอบอ้างเป็น หน่วยงานรัฐบาลสหรัฐฯ

แคมเปญ Phishing มุ่งเป้าไปที่ผู้รับเหมาในประเทศสหรัฐฯ ภายในอีเมล Phishing เป็นข้อเสนอราคาสำหรับโครงการของรัฐบาล โดยจะแสดงหน้าเป็นพอร์ทัลหน่วยงานของรัฐบาลกลางที่ถูกกฎหมาย โดยที่ INKY ได้เคยมีการรายงานเมื่อเดือนมกราคม 2022 ว่าผู้โจมตีได้ใช้ไฟล์ PDF ที่แนบมาพร้อมคำแนะนำเกี่ยวกับขั้นตอนการเสนอราคาสำหรับโครงการของกระทรวงแรงงานสหรัฐฯ

โดย Cofense รายงานว่าได้มีการจัดทำโลโก้ที่ใหญ่ขึ้น และรวมลิงก์ไปยัง PDF แทนที่จะแนบไฟล์ ซึ่งในไฟล์ PDF จะมีคำแนะนำโดยละเอียดเกี่ยวกับวิธีการประมูลพร้อมข้อมูลทางเทคนิค โดยมีโลโก้ที่โดดเด่นยิ่งขึ้นและลิงก์ไปยังหน้า Phishing โดยเว็บไซต์ Phishing ยังมีการปรับปรุง โดยใช้ HTTPS บนหน้าเว็บทั้งหมดในโดเมนเดียวกัน ซึ่งในหน้า Phishing จะพยายามหลอกให้ผู้ใช้งานป้อนข้อมูลประจำตัวของบัญชี Microsoft Office 365 โดยผู้โจมตีได้เพิ่มขั้นตอน Captcha Challenge เพื่อสร้างความมั่นใจว่าไม่ได้บันทึกอินพุตของบอท

วิธีที่จะป้องกันคือต้องตรวจสอบรายละเอียดทั้งหมด เช่น ที่อยู่สำหรับส่ง URL ที่เชื่อมโยงไปถึง และสุดท้ายไปที่พอร์ทัลการเสนอราคาผ่านเครื่องมือค้นหาแทนที่จะติดตามลิงก์ที่ให้ไว้ หากไม่แน่ใจ ให้ลองค้นหา URL ทางออนไลน์