

ประจำวันพุธที่ 25 พฤษภาคม 2565

พบช่องโหว่ใหม่ที่ยังไม่ได้รับการแก้ไข อาจทำให้ถูกขโมยเงินจาก PayPal ได้

นักวิจัยด้านความปลอดภัย h4x0r_dz อ้างว่าได้ค้นพบช่องโหว่ที่ยังไม่ได้รับการแก้ไขในบริการโอนเงินของ PayPal ซึ่งอาจทำให้ผู้โจมตีหลอกให้ทำธุรกรรม โดยไม่รู้ตัวด้วยการคลิกเพียงครั้งเดียวด้วย Clickjacking หรือที่เรียกว่า UI redressing ซึ่งเป็นเทคนิคที่ผู้ใช้งานไม่รู้ตัวและถูกหลอกให้คลิกหน้าเว็บที่ดูเหมือนไม่มีอันตราย ซึ่งมีเป้าหมายในการให้ดาวนิโหลดมลแวร์ เพื่อเปลี่ยนเส้นทางไปยังเว็บไซต์ที่เป็นอันตราย หรือเปิดเผยข้อมูลที่ละเอียดอ่อน โดยทั่วไปแล้วการแสดงผลหน้าที่ยังมองไม่เห็นหรือองค์ประกอบ HTML ที่ด้านบนของหน้าที่ยังมองไม่เห็น ส่งผลให้ผู้ใช้ถูกหลอกให้คิดว่ากำลังคลิกหน้าที่ยังต้องโดยแท้จริงแล้ว แต่ผู้ใช้กำลังคลิกหน้าที่ยังถูกหลอกมองที่ซ้อนทับอยู่ด้านบน

ซึ่งหมายความว่าผู้โจมตีสามารถฝังจุดปลายทางดังกล่าวไว้ใน iframe ได้ ทำให้ผู้ใช้งานที่เข้าสู่ระบบเว็บเบราว์เซอร์อยู่แล้วสามารถโอนเงินไปยังบัญชี PayPal ที่ควบคุมโดยผู้โจมตีเพียงแค่คลิกปุ่ม ยิ่งไปกว่านั้น การโจมตีอาจมีผลร้ายตามมาในพอร์ตออนไลน์ที่ผสานรวมกับ PayPal สำหรับการชำระเงิน ทำให้ผู้โจมตีสามารถหักจำนวนเงินตามอำเภอใจจากบัญชี PayPal ของผู้ใช้



ที่มาของข่าว: <https://thehackernews.com/2022/05/paypal-pays-hacker-200000-for.html>