ประจำวันพุธที่ 10 สิงหาคม 2565

open redirect ทำให้เกิดช่องโหว่ใน American Express และ Snapchat ที่ใช้ประโยชน์จากการโจมตีแบบ Phishing

ช่องโหว่การเปลี่ยนopen redirect ยังคงมีอยู่เนื่องจากเว็บไซต์ที่ได้รับผลกระทบไม่ได้ตรวจสอบการป้อนข้อมูลของผู้ใช้ ซึ่งช่วยให้ผู้โจมตีสามารถจัดการ URL เพื่อเปลี่ยนเส้นทางการเข้าเว็บไซต์ของผู้ใช้ไปยังเว็บไซต์ที่เป็นอันตราย เนื่องจากลิงก์ที่จัดการมีชื่อโดเมนที่ถูกต้อง ทำให้ผู้ใช้งานอาจถือว่าลิงก์นั้นปลอดภัย ซึ่งโดเมนที่เชื่อถือได้จะใช้เป็นหน้า Landing Page เท่านั้น

ตั้งแต่กลางเดือนพฤษภาคมถึงปลายเดือนกรกฎาคม บริษัทรักษาความปลอดภัยอีเมล Inky ได้สังเกตและพบอีเมลฟิชชิ่งประมาณ 7,000 ฉบับที่มาจากบัญชีที่ถูกไฮแจ็กต่างๆ ซึ่งมีการพยายามจะใช้ประโยชน์จากการ open redirect ใน snapchat[.]com และในช่วงสิ้นเดือนกรกฎาคม มีอีเมลฟิชชิ่งประมาณ 2,000 ฉบับพยายามใช้ประโยชน์จากช่องโหว่การ open redirect ของ americanexpress[.]com

อีเมล Phishing ในแคมเปญ Snapchat ปลอมแปลง DocuSign, FedEx และ Microsoft แต่ทั้งหมดได้รับการออกแบบมาเพื่อเปลี่ยนเส้นทางการเข้าเว็บไซต์ของผู้ที่ตกเป็นเป้าหมายไปยังเว็บไซต์ที่ตั้งใจจะเก็บข้อมูลประจำตัวของผู้ใช้ Microsoft 365 ได้มีการรายงานถึงช่องโหว่การ open redirect ไปยัง Snapchat เมื่อวันที่ 4 สิงหาคม 2021 แต่ยังไม่ได้รับการแก้ไข

บริษัทรักษาความปลอดภัยอีเมล Inky กล่าวว่าเจ้าของโดเมนสามารถป้องกันการละเมิดนี้โดยหลีกเลี่ยงการใช้ redirect เว็บไซต์ หากมีความจำเป็นสำหรับเหตุผลทางการค้า การใช้รายการที่อนุญาตของลิงก์ที่ปลอดภัยที่ได้รับอนุมัติจะป้องกันผู้ไม่หวังดีจากการป้อนลิงก์ที่เป็นอันตราย

ที่มาของข่าว : https://www.securityweek.com/open-redirect-flaws-american-express-and-snapchat-exploited-phishing-attacks