ประจำวันอังคารที่ 20 กันยายน 2565

Microsoft เตือนถึงแคมเปญล่อโกงที่มุ่งเป้าหมายไปที่เกมเมอร์

Microsoft ออกมากล่าวว่าได้กำลังติดตามแคมเปญการฉ้อโกงขนาดใหญ่ด้วยการคลิกที่มุ่งเป้าไปที่นักเล่นเกม โดยใช้ส่วนขยายเบราว์เซอร์ที่แอบซ่อนไว้บนระบบที่ถูกโจมตี ซึ่งผู้โจมตีจะสร้างรายได้จากการคลิกที่สร้างโดยโหนดเว็บเบราว์เซอร์หรือส่วนขยายเบราว์เซอร์ที่เป็นอันตรายที่ติดตั้งบนอุปกรณ์อย่างลับๆ

แผนกความปลอดภัยทางไซเบอร์ของบริษัทกำลังติดตามกลุ่มภัยคุกคามที่กำลังพัฒนาภายใต้ชื่อ DEV-0796 โดยเชื่อมต่อด้วยไฟล์ ISO ที่ดาวน์โหลดลงในเครื่องของเหยื่อเมื่อคลิกโฆษณาหรือความคิดเห็นที่เป็นอันตรายบน YouTube และไฟล์ ISO ได้รับการออกแบบมาเพื่อติดตั้งเบราว์เซอร์ node-webkit (aka NW.js) หรือส่วนขยายเบราว์เซอร์ที่หลอกลวง ที่ใช้ในการโจมตีคือไฟล์ DMG ซึ่งเป็นไฟล์ Apple Disk Image ที่ใช้เป็นหลักในการเผยแพร่ซอฟต์แวร์บน macOS ซึ่งบ่งชี้ว่าผู้โจมตีกำลังกำหนดเป้าหมายระบบปฏิบัติการหลายระบบ

Kaspersky ได้เปิดเผยรายละเอียดของแคมเปญที่ล่อให้นักเล่นเกมที่หากลโกงบน YouTube ให้ดาวน์โหลดมัลแวร์ที่เผยแพร่ด้วยตนเองซึ่งสามารถติดตั้งเครื่องขุด crypto และผู้โจมตีสามารถขโมยข้อมูลอื่น ๆ ได้ ซึ่งมัลแวร์และซอฟต์แวร์ที่ไม่พึงประสงค์ที่เปิดให้ดาวน์โหลดโปรแกรมโกงจะเป็นภัยคุกคามต่อเกมเมอร์ โดยเฉพาะอย่างยิ่งสำหรับผู้ที่ชื่นชอบซีรีย์เกมยอดนิยม

ที่มาของข่าว : https://thehackernews.com/2022/09/microsoft-warns-of-large-scale-click.html