ประจำวันอังคารที่ 7 มิถุนายน 2565

แฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐ กำลังใช้ประโยชน์จากช่องโหว่ Follina ของ Microsoft เพื่อโจมตีองค์กรในยุโรปและสหรัฐอเมริกา

บริษัท Proofpoint ซึ่งเป็นบริษัทรักษาความปลอดภัยระดับองค์กร กล่าวว่าได้มีการสกัดกั้นความพยายามในการใช้ประโยชน์จากช่องโหว่ในการเรียกใช้โค้ดจากระยะไกล CVE-2022-30190 (คะแนน CVSS : 7.8) โดยคาดว่าเป็นแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐ ที่กำลังใช้ประโยชน์จากช่องโหว่ Follina ของ Microsoft เพื่อทำการโจมตีองค์กรในยุโรปและสหรัฐอเมริกา โดยเป็นข้อความฟิชชิ่งที่มีเอกสารหลอกลวงไม่น้อยกว่า 1,000 ข้อความที่ถูกส่งไปยังเป้าหมาย โดยมีเพย์โหลด ซึ่งแสดงในรูปแบบของสคริปต์ PowerShell ที่มีการเข้ารหัส Base64 และทำหน้าที่เป็นตัวดาวน์โหลดเพื่อดึงสคริปต์ PowerShell ตัวที่ 2 จากเซิร์ฟเวอร์ระยะไกลที่ชื่อ seller-notification[.]live. โดยสคริปต์นี้จะตรวจสอบ virtualization และจะขโมยข้อมูลจากเบราว์เซอร์ในเครื่อง โดยช่องโหว่ Follina นี้จะใช้ประโยชน์จากโครงร่าง URI ของโปรโตคอล "ms-msdt:" เพื่อควบคุมอุปกรณ์เป้าหมายจากระยะไกลซึ่งยังไม่ได้รับการแก้ไข ด้าน Microsoft ได้แนะนำให้ลูกค้าทำการปิดใช้งานโปรโตคอลเพื่อป้องกันการโจมตี

ที่มาของข่าว : https://thehackernews.com/2022/06/state-backed-hackers-exploit-microsoft.html