ประจำวันจันทร์ที่ 25 ตุลาคม 2564

Malware ขโมยคุกกี้ที่ใช้ในบัญชี YouTube

Google ได้ขัดขวางการโจมตี phishing ที่ผู้โจมตีได้พยายามใช้ malware ขโมยคุกกี้ของบัญชี YouTube และนำไปใช้ในทางที่ผิดเพื่อหลอกลวงทาง cryptocurrency โดยผู้โจมตีนี้จะส่งข้อความ phishing ไปยังอีเมลที่เจ้าของช่อง YouTube เผยแพร่สู่สาธารณะ หลังจากได้รับความไว้วางใจจากเป้าหมายแล้ว แฮกเกอร์จะส่ง URL ไม่ว่าจะทางอีเมลหรือ PDF บน Google Drive โดยใช้ซอฟต์แวร์ที่ถูกต้องตามกฎหมาย แต่สุดท้ายจะนำเหยื่อไปยังหน้า Landing Page ของ malware แทน

เมื่อดำเนินการดังกล่าวแล้ว malware จะขโมยคุกกี้จากเบราว์เซอร์ของผู้ใช้ จากนั้นผู้โจมตีจะใช้คุกกี้เพื่อบังคับเซสชันของเหยื่อและเข้าควบคุมบัญชี แล้วนำไปขายในเว็บมืด (ราคาระหว่าง 3$ ถึง 4,000$ ขึ้นอยู่กับจำนวนสมาชิก) หรือนำมาใช้ใหม่อีกครั้งในการเอาไปหลอกลวงสกุลเงินดิจิทัล โดย malware ที่ใช้ในการโจมตีเหล่านี้ ได้แก่ Azorult, Grand Stealer, Kantal, Masad, Nexus stealer, Predator The Thief, RedLine, Raccoon, Vikro Stealer และ Vidar ควบคู่ไปกับเครื่องมือ open sources เช่น Sorano และ AdamantiumThief โดย Malware นั้นสามารถขโมยทั้งรหัสผ่านและคุกกี้ได้

Google กล่าวว่าได้จัดการกับการโจมตีที่เป็นอันตรายนี้รวมถึงได้บล็อกข้อความ 1.6 ล้านข้อความ ที่ผู้โจมตีส่งถึงเหยื่อ โดย Google แสดงคำเตือน Safe Browsing ประมาณ 62,000 รายการสำหรับหน้า phishing ที่ระบุ บล็อก 2,400 ไฟล์ และกู้คืนบัญชีที่ได้รับผลกระทบประมาณ 4,000 บัญชี และ Google ได้กล่าวอีกว่าในการตรวจจับที่เพิ่มขึ้นสังเกตเห็นผู้โจมตีเปลี่ยนจาก Gmail ไปยังผู้ให้บริการอีเมลรายอื่นอีก (ส่วนใหญ่เป็น email.cz, seznam.cz, post.cz และ aol.com) นอกจากนี้ ได้มีการดำเนินการและแจ้งไปยัง FBI เพื่อทำการตรวจสอบเพิ่มเติม

ที่มาของข่าว : https://www.securityweek.com/cookie-theft-malware-used-hijack-youtube-accounts?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+securityweek+%28SecurityWeek+RSS+Feed%29