ประจำวันพฤหัสบดีที่ 18 สิงหาคม 2565

แฮกเกอร์ของรัฐบาลรัสเซียโจมตีหน่วยงานในยูเครนด้วยมัลแวร์ Infostealer

ผู้โจมตีที่ได้รับการสนับสนุนจากรัฐบาลของรัสเซียได้โจมตีหน่วยงานในยูเครนอย่างต่อเนื่องด้วยมัลแวร์ขโมยข้อมูล โดย Symantec แผนกหนึ่งของ Broadcom Software กล่าวว่าแคมเปญที่เป็นอันตรายนั้นมาจากผู้โจมตี Shuckworm หรือที่รู้จักในชื่อ Actinium ,Armageddon , Gamaredon, Primitive Bear และ Trident Ursa จากการค้นพบนี้ได้รับการยืนยันโดยทีมรับมือเหตุฉุกเฉินทางคอมพิวเตอร์ของประเทศยูเครน (CERT-UA)

การโจมตีล่าสุดได้เริ่มขึ้นในวันที่ 15 กรกฎาคม พ.ศ. 2565 และต่อเนื่องไปจนถึงวันที่ 8 สิงหาคม โดยกลุ่มใช้ประโยชน์จากอีเมลฟิชชิ่งที่ปลอมแปลงเป็นจดหมายข่าวและคำสั่ง โดยท้ายที่สุดจะนำไปสู่การปรับใช้มัลแวร์ขโมย PowerShell ช ที่ชื่อว่า GammaLoad .PS1_v2 . ซึ่งมี backdoors คือ Giddome และ Pterodo ซึ่งทั้งสองนี้เป็นเครื่องมือของ Shuckworm ที่ผู้โจมตีได้พัฒนาขึ้นใหม่อย่างต่อเนื่องเพื่อพยายามไม่ให้ถูกตรวจจับ

Pterodo เป็นมัลแวร์ ดรอปเปอร์ Visual Basic Script (VBS) ที่มีความสามารถในการรันสคริปต์ PowerShell ใช้งานตามกำหนดการ (shtasks.exe) และดาวน์โหลดโค้ดเพิ่มเติมจากเซิร์ฟเวอร์คำสั่งและการควบคุม ส่วน Giddome implant มีความสามารถหลายอย่าง รวมถึงการบันทึกเสียง, จับภาพหน้าจอ, บันทึกการกดแป้นพิมพ์, และดึงข้อมูลและดำเนินการสั่งการโดยพลการบนโฮสต์ที่ติดไวรัส

การค้นพบนี้เป็นไปตามการแจ้งเตือนจาก CERT-UA ซึ่งเตือนถึงการโจมตีแบบฟิชชิ่งที่เป็นระบบใหญ่ และกระจายตัวทางภูมิศาสตร์ ที่เกี่ยวข้องกับการใช้โปรแกรมดาวน์โหลด .NET ที่ชื่อ RelicRace เพื่อดำเนินการเพย์โหลด เช่น Formbook และ Snake Keylogger

ที่มาของข่าว : https://thehackernews.com/2022/08/russian-state-hackers-continue-to.html