เทรนด์ไมโครเตือนองค์กรธุรกิจระวังการโจมตีแบบแฝงสคริปต์ หลังพบช่องโหว่บนเว็บไซต์สำนักนายกฯ สิงคโปร์

บริษัท เทรนด์ไมโคร อินคอร์ปอเรท (TYO: 4704; TSE:4704) ผู้นำระดับโลกด้านซอฟต์แวร์รักษาความปลอดภัย ได้เปิดเผยข้อมูลล่าสุดเกี่ยวกับเว็บไซต์สำนักนายกรัฐมนตรีสิงคโปร์ (Singapore Prime Minister Office: PMO) ที่เกิดความเสียหายเมื่อเร็วๆ นี้ว่าจากการวิเคราะห์ของผู้เชี่ยวชาญด้านภัยคุกคามของบริษัทเทรนด์ไมโคร พบว่าการโจมตีดังกล่าวไม่ใช่การโจมตีในลักษณะเจาะระบบ (แฮก) แต่เป็นการใช้ประโยชน์จากช่องโหว่ที่มีอยู่ภายในเว็บไซต์ดังกล่าวต่างหาก

ทำความเข้าใจกับลักษณะช่องโหว่ที่เกิดขึ้น

การวิเคราะห์ของบริษัท เทรนด์ไมโคร ระบุว่ากรณีของเว็บไซต์ PMO **เป็นเทคนิคการโจมตีแบบแฝงสคริปต์ (Cross Site Scripting: XSS)** ที่อาชญากรไซเบอร์ใช้ประโยชน์จากฟังก์ชั่น ‘ค้นหา’ บนเว็บไซต์และแอบใส่เนื้อหาจากแหล่งภายนอกเข้าไป โดยในกรณีนี้อาชญากรไซเบอร์ได้เปลี่ยนเส้นทาง URL ไปยังรูปที่กำหนดไว้อย่างตั้งใจ

เมื่อดำเนินการตรวจสอบผ่านเครือข่ายป้องกันภัยอัจฉริยะ (เทรนด์ไมโคร สมาร์ท โพรเท็คชั่น เน็ตเวิร์ค) พบว่า URL ที่ถูกนำไปใช้ประโยชน์ได้รับการเผยแพร่บนไซต์เครือข่ายสังคมออนไลน์หลายแห่ง รวมถึงทวิตเตอร์ เฟซบุ๊ก และอื่นๆ ซึ่งนั่นทำให้เว็บไซต์ของ PMO เสียชื่อเสียง โดยเมื่อมีการคลิกลิงก์ที่มีการดัดแปลงซึ่งอ้างอิงไปยัง URL ทางการของเว็บไซต์ PMO (www.pmo.gov.sg) ผู้ใช้งานอินเทอร์เน็ตและผู้บริโภคที่ไม่รู้สึกสงสัยก็จะถูกลวงให้เชื่อว่าเว็บไซต์ PMO ถูกแฮกระบบแล้ว และยิ่งมีการแสดงภาพที่อาชญากรไซเบอร์ได้จัดเตรียมไว้ก็ยิ่งทำให้ผู้ใช้และผู้บริโภคเชื่อว่าเป็นผลงานของกลุ่มแฮกเกอร์ที่ชื่อ Anonymous Collective

จะเห็นได้ว่าในช่วงสองสามสัปดาห์ที่ผ่านมา สินทรัพย์ออนไลน์ของหน่วยงานภาครัฐหลายแห่งในสิงคโปร์ถูกบุกรุกโดยอาชญากรไซเบอร์ที่ส่งผลให้บริการต่างๆ หยุดชะงักและกระทบในด้านอื่นๆ โดยบริษัท เทรนด์ไมโครได้ให้คำแนะนำองค์กรธุรกิจต่างๆ ในการตรวจสอบประสิทธิภาพของโครงสร้างระบบ ไอทีของตนอย่างสม่ำเสมอเพื่อป้องกันไม่ให้เกิดช่องโหว่ขึ้น

คำแนะนำเพื่อป้องกันไม่ให้ให้เกิดช่องโหว่ในอนาคต

บริษัท เทรนด์ไมโคร แนะนำให้องค์กรธุรกิจต่างๆ ทำตามขั้นตอนต่อไปนี้ในการตรวจสอบสถานะสินทรัพย์ออนไลน์ของตนเพื่อป้องกันการเกิดช่องโหว่ด้านความปลอดภัย

1. สแกนหาช่องโหว่ของเว็บแอพพลิเคชัน
2. ตรวจสอบโค้ด HTML เพื่อให้แน่ใจว่าฟังก์ชันการค้นหาเป็นปกติ ซึ่งรวมถึงตั้งค่าข้อจำกัดในการใส่เนื้อหาที่มีอักขระพิเศษ ตลอดจนกลั่นกรองผลลัพธ์โดยใช้การเข้ารหัสลับ HTML ของข้อมูลหรือสตริงที่ผู้ใช้ใส่เข้าไป
3. สำหรับการป้องกันระบบทั้งหมดภายในระยะเวลาสั้นๆ ให้ปิดใช้งานฟังก์ชั่นค้นหาของเว็บไซต์

บริษัท เทรนด์ไมโคร มีชุดทดลองใช้สำหรับให้องค์กรธุรกิจต่างๆ นำไปสแกนเว็บแอพพลิเคชันของตนเพื่อหาช่องโหว่ได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับชุดทดลองใช้ โปรดติดต่อบริษัท เทรนด์ไมโคร (ประเทศไทย) โทรศัพท์ 0-2646-1968

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับกลยุทธ์ด้านการรักษาความปลอดภัยจากการโจมตีเจาะระบบ คลิกดูได้ที่: http://blog.trendmicro.com/trendlabs-security-intelligence/security-strategies-against-hacking-attacks/