แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แคมเปญ VENOM Phishing มุ่งเป้าโจมตีผู้บริหารระดับสูง เพื่อขโมย Microsoft Credentials

วันที่แจ้งเตือน 10 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานจาก Abnormal Security เกี่ยวกับแคมเปญ “VENOM” Phishing (Phishing-as-a-Service (PhaaS)) ซึ่งมุ่งเป้าขโมยข้อมูล credentials ของผู้บริหารระดับสูง และสามารถหลีกเลี่ยงการยืนยันตัวตนแบบ MFA ได้

การโจมตีดังกล่าวเริ่มจากการส่งอีเมลฟิชชิงที่ปลอมเป็นการแจ้งเตือนการแชร์เอกสาร Sharepoint เกี่ยวกับรายงานทางการเงิน เพื่อให้กลุ่มเป้าหมายให้ความสนใจ และใช้เทคนิคหลบเลี่ยงการตรวจจับ เช่น การแทรก HTML และ CSS ปลอม รวมถึงการใช้ QR code ที่สร้างจาก Unicode characters เพื่อหลีกเลี่ยงระบบสแกน เป็นต้น เมื่อเหยื่อสแกน QR code จะถูกนำไปยังหน้าเว็บปลอม เพื่อหลีกเลี่ยงระบบตรวจจับ และนำไปยังหน้า phishing ที่เลียนแบบ Microsoft login โดยใช้เทคนิค Adversary-in-The-Middle (AiTM) เพื่อดักจับ username password และ MFA code แบบเรียลไทม์ พร้อมทั้งบันทึก session token เพื่อใช้เข้าถึงบัญชีของเหยื่อ นอกจากนี้ ยังมีการใช้เทคนิค device code phishing ซึ่งหลอกให้ผู้ใช้งานอนุมัติการเข้าถึงบัญชีผ่าน OAuth device authorization flow ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงบัญชีได้โดยไม่ต้องทราบรหัสผ่าน และสามารถรักษาการเข้าถึงแบบต่อเนื่อง (persistent access) ได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาเสริมมาตรการยืนยันตัวตนที่มีความมั่นคงปลอดภัยสูง รวมทั้งสร้างความตระหนักรู้แก่ผู้ใช้งานเกี่ยวกับภัยคุกคามจาก QR code phishing และการหลอกลวงรูปแบบ social engineering รวมถึงติดตั้งระบบ Email Security และ Endpoint Detection เพื่อช่วยตรวจจับพฤติกรรมผิดปกติ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.techradar.com/pro/security/this-devious-venom-phishing-campaign-targets-business-executives-by-name-so-watch-what-you-click-on
2. https://abnormal.ai/blog/venom-phishing-campaign-mfa-credential-theft