แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แคมเปญการโจมตีบัญชี Microsoft Entra ด้วยเทคนิค Device Code Phishing และ Vishing

วันที่แจ้งเตือน 24 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับแคมเปญการโจมตีมุ่งเป้าบัญชี Microsoft Entra ซึ่งใช้เทคนิคผสมผสานระหว่าง Device Code Phishing และ Vishing โดยภาคการเงินเป็นหนึ่งในกลุ่มเป้าหมาย

รูปแบบการโจมตีดังกล่าวอาศัยการใช้กระบวนการยืนยันตัวตนแบบ Oauth 2.0 Device Authorization Flow โดยผู้ไม่ประสงค์ดีใช้การหลอกล่อให้ผู้ใช้งานกรอกรหัส (user code) บนหน้าเว็บไซต์ยืนยันตัวตนของ Microsoft และทำการเข้าสู่ระบบพร้อมยืนยันตัวตนแบบหลายปัจจัย (MFA) ตามปกติ จากนั้นผู้ไม่ประสงค์ดีจะได้รับ Authentication Token จากระบบ และสามารถเข้าถึงบัญชีของผู้ใช้งานได้โดยไม่ต้องยืนยันตัวตนแบบ MFA ซ้ำ ทั้งนี้ เมื่อผู้ไม่ประสงค์ดีสามารถเข้าสู่ระบบได้ อาจเข้าถึงบริการ SaaS ที่เชื่อมต่อผ่าน Single Sign-On (SSO) ภายในองค์กร และนำไปสู่การขโมยข้อมูลสำคัญและทำให้เกิดความเสียหายกับองค์กรได้

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจพิจารณาดำเนินการมาตรการ ดังนี้

- ทบทวนและตรวจสอบ Log การเข้าสู่ระบบ โดยเฉพาะเหตุการณ์ที่เกี่ยวข้องกับ Device Code Authentication
- เพิกถอนสิทธิ์ (Revoke) ของ OAuth Applications ที่ไม่จำเป็นหรือมีพฤติกรรมผิดปกติ
- ตรวจสอบและเฝ้าระวังการเข้าถึงแอปพลิเคชัน SaaS ที่เชื่อมต่อผ่าน SSO
- ติดตามข่าวสารการแจ้งเตือนภัยคุกคามทางไซเบอร์ จากผู้พัฒนาผลิตภัณฑ์อย่างต่อเนื่อง
- เสริมสร้างมาตรการป้องกัน Social Engineering และอบรมพนักงานให้ตระหนักรู้ภัยคุกคามอย่างสม่ำเสมอ

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/hackers-target-microsoft-entra-accounts-in-device-code-vishing-attacks/
2. https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-device-code

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ