

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

แจ้งเตือน แคมเปญฟิชชิง Astaroth มุ่งเป้าไปที่ Gmail, Microsoft และ 3rd Party Login

วันที่แจ้งเตือน 5 มีนาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบการหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (“ThaiCERT”) ได้ติดตามเกี่ยวกับการโจมตีทางไซเบอร์ โดยพบรายงานข้อมูล แคมเปญฟิชชิง Astaroth ที่มุ่งเป้าโจมตีผู้ใช้งานบริการยืนยันตัวตน เช่น Gmail, Yahoo, AOL, Microsoft 365 และบริการอื่น ๆ โดยผู้ไม่ประสงค์ดีใช้เทคนิค Man-in-the-Middle (MiTM) เพื่อขโมยข้อมูลและรหัส MFA รวมทั้ง หลบเลี่ยงระบบความปลอดภัยในการยืนยันตัวตนแบบหลายปัจจัย (MFA) ของผู้ใช้งานได้ ภัยคุกคามนี้เริ่มต้นจากอีเมลฟิชชิงที่ออกแบบมาเพื่อหลอกให้ผู้ใช้งานคลิกลิงก์ไปยังหน้าล็อกอินที่ปลอมแปลงขึ้นมา เมื่อผู้ใช้งานป้อนข้อมูลล็อกอิน รหัสผ่าน และรหัส MFA ข้อมูลเหล่านี้จะถูกส่งตรงไปยังผู้ไม่ประสงค์ดีทันที ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมบัญชีของผู้ใช้งานได้ ทั้งนี้ เพื่อเป็นการป้องกัน ผู้ใช้งานควรระมัดระวังอีเมลที่น่าสงสัย ตรวจสอบ URL ให้ละเอียดก่อนกรอกข้อมูลใด ๆ หลีกเลี่ยงการคลิกลิงก์โดยตรงจากอีเมล ใช้งาน Passkeys และตรวจสอบประวัติการล็อกอินอย่างสม่ำเสมอ รวมทั้งติดตามข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์เพื่อประกอบการเฝ้าระวัง ตอบสนอง และรับมือต่อภัยคุกคามไซเบอร์ได้ทันต่อเหตุการณ์

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบการธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. <https://www.infosecurity-magazine.com/news/astaroth-phishing-kit-bypasses-2fa/>
2. <https://cybersecuritynews.com/new-astaroth-2fa-phishing-kit-targeting-gmail/>
3. <https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-021>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ