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

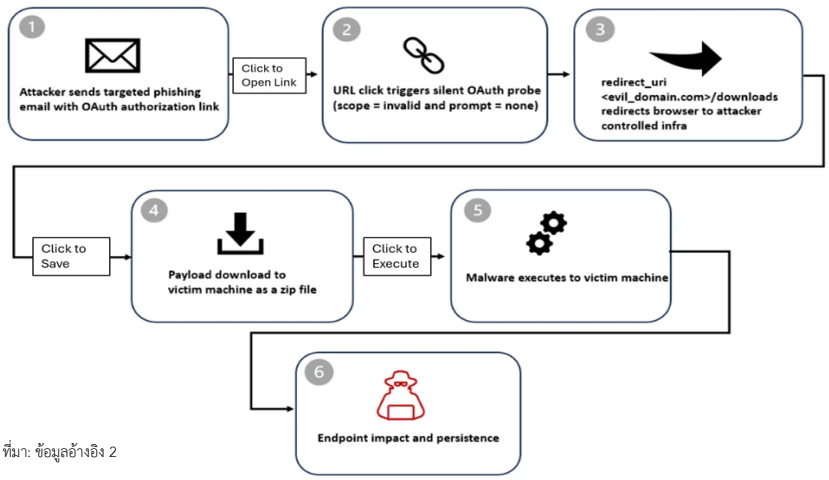
ผู้ไม่หวังดีใช้ประโยชน์จากการเปลี่ยนเส้นทางการยืนยันตัวตนผ่านระบบ OAuth เพื่อนำส่งมัลแวร์

วันที่แจ้งเตือน 6 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีมีการใช้ประโยชน์จากการเปลี่ยนเส้นทางระบบยืนยันตัวตนและตรวจสอบสิทธิ (OAuth) เพื่อนำส่งฟิชชิ่ง และ มัลแวร์ หลอกให้เหยื่อคลิกลิงก์และนำไปยังเว็บไซต์ที่ผู้ไม่หวังดีควบคุม (attacker-controlled phishing pages) ซึ่งหลอกให้เหยื่อดาวน์โหลดไฟล์อันตราย และทำให้เครื่องคอมพิวเตอร์ติดมัลแวร์ได้

ผู้ไม่หวังดีจะสร้างลิงก์ OAuth โดยใช้พารามิเตอร์ที่ผิดพลาด (เช่น invalid scope หรือ prompt=none เป็นต้น) ทำให้ระบบ OAuth ของผู้ให้บริการ เช่น Microsoft Entra ID หรือ GoogleWorkspace เป็นต้น เปลี่ยนเส้นทางตามที่ผู้ไม่หวังดีกำหนด และนำส่งลิงก์ดังกล่าวผ่านอีเมลในรูปแบบของฟิชชิงที่ออกแบบให้ดูเหมือนข้อความจริงจากองค์กร เช่น การแจ้งเตือนลายเซ็นต์อิเล็กทรอนิกส์ คำเชิญประชุม หรือคำขอรีเซ็ตรหัสผ่าน เป็นต้น โดยลิงก์อาจอยู่ในเนื้อหาอีเมลโดยตรงหรือซ่อนไว้ในไฟล์แนบ PDF ทั้งนี้ เมื่อเหยื่อทำการดาวน์โหลดไฟล์ ZIP ที่มีมัลแวร์และเปิดไฟล์แล้ว ระบบจะรันคำสั่ง PowerShell เพื่อดาวน์โหลดและติดตั้งมัลแวร์อันตราย



ที่มา: ข้อมูลอ้างอิง 2

ThaiCERT ได้ออกคำแนะนำเพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว โดย

- ตรวจสอบและควบคุมแอปพลิเคชัน OAuth ที่อนุญาตให้เข้าถึงบัญชี
- ลบแอปที่ไม่จำเป็นหรือมีสิทธิมากเกินความจำเป็น
- ใช้มาตรการป้องกัน เช่น Cloud Email Security, Identity Protection, Conditional Access Policies หรือ Monitoring Cross-Domain Activity ทั้งในอีเมล, ระบบยืนยันตัวตน และ อุปกรณ์ปลายทาง

นอกจากนี้ผู้ประกอบธุรกิจสามารถพิจารณาข้อมูลตัวบ่งชี้การโจมตี (IOCs) เช่น IPs, Redirection URLs, file hashes, Microsoft Client ID เป็นต้น เพื่อนำไปใช้ประกอบการตรวจสอบ เฝ้าระวังภัยคุกคามดังกล่าวภายในระบบของตนเองตามข้อมูลอ้างอิง 2

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

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 6 มี.ค. 2569
2. https://www.microsoft.com/en-us/security/blog/2026/03/02/oauth-redirection-abuse-enables-phishing-malware-delivery