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

กลุ่มผู้ไม่หวังดี Storm-2949 และ Tycoon2FA พยายามเลี่ยงการตรวจจับ และขโมยข้อมูลสำคัญจากองค์กร

วันที่แจ้งเตือน 20 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับกลุ่มผู้ไม่หวังดี ได้แก่

กลุ่มผู้ไม่หวังดี	รายละเอียด	ผลกระทบ
Storm-2949	ใช้ฟีเจอร์ Self-Service Password Reset (SSPR) และฟังก์ชันด้านการจัดการบัญชีของ Microsoft 365 และ Microsoft Azure เพื่อขโมยข้อมูลสำคัญจากองค์กรเป้าหมาย • เป็นการใช้ฟังก์ชันของ Microsoft ในทางที่ผิด เพื่อหลีกเลี่ยงการตรวจจับและเข้าถึงข้อมูลภายในองค์กรอย่างต่อเนื่อง มุ่งเป้าไปที่บัญชีที่มีสิทธิ์สูง ในองค์กรที่ใช้งาน Microsoft Entra ID (Azure AD เดิม), Microsoft 365 และ Azure Environment โดยโจมตีร่วมกับฟีเจอร์ OAuth Application, API Access และการกำหนดสิทธิ์ของ Azure เพื่อดึงข้อมูลจำนวนมากออกจากระบบเป้าหมาย	ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Microsoft 365, Microsoft Entra ID (Azure AD), Azure Subscription, Exchange Online, SharePoint Online, OneDrive, Azure Key Vault และ Azure Resource Management Environment ที่เปิดใช้งาน Self-Service Password Reset หรือมีการกำหนดสิทธิ์ Identity Management ไม่เหมาะสม
Tycoon2FA	ใช้วิธี Device Code Phishing เพื่อยึดบัญชีผู้ใช้งาน Microsoft 365 และหลีกเลี่ยงการป้องกันแบบ Multi-Factor Authentication (MFA) • เป็นการสร้าง Device Authentication Request ไปยังระบบ Microsoft และนำ Device Code ที่ได้รับไปส่งให้เหยื่อผ่านอีเมล ฟิชชิง หน้าเว็บปลอม หรือ QR Code เพื่อหลอกให้เหยื่อทำการยืนยันตัวตนผ่านหน้า Login จริงของ Microsoft เมื่อเหยื่อกรอก Device Code และผ่านกระบวนการ MFA สำเร็จ ระบบ Microsoft จะมองว่าการอนุมัติดังกล่าวเป็นการอนุญาตให้เข้าถึงบัญชี Microsoft 365 อย่างถูกต้อง ส่งผลให้ผู้ไม่หวังดีได้รับ Access Token และ Refresh Token สำหรับใช้งานบัญชีของเหยื่อโดยไม่จำเป็นต้องทราบรหัสผ่านจริง	ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Microsoft 365, Microsoft Entra ID, Outlook Online, Exchange Online, OneDrive, SharePoint Online และ ระบบที่เปิดใช้งาน OAuth Device Code Authentication

ข้อมูลอ้างอิง

<u>กลุ่ม Storm-2949</u>

1. https://www.bleepingcomputer.com/news/security/microsoft-self-service-password-reset-abused-in-azure-data-theft-attacks/
2. https://www.microsoft.com/en-us/security/blog/2026/05/18/storm-2949-turned-compromised-identity-into-cloud-wide-breach/

<u>กลุ่ม Tycoon2FA</u>

1. https://www.bleepingcomputer.com/news/security/tycoon2fa-hijacks-microsoft-365-accounts-via-device-code-phishing/
2. https://www.microsoft.com/en-us/security/blog/2026/03/04/inside-tycoon2fa-how-a-leading-aitm-phishing-kit-operated-at-scale/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ