แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่อเฝ้าระวังการนำ Cloudflare ไปใช้ในทางที่ไม่สุจริต

วันที่แจ้งเตือน 8 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีเว็บไซต์ที่ใช้บริการ Cloudflare ถูกนำไปใช้ในทางที่ไม่สุจริตหรือสร้างหน้าเว็บปลอมเพื่อหลอกขโมยรหัสผ่าน และแพร่กระจายมัลแวร์ โดย ThaiCERT ได้ออกคำแนะนำในการเฝ้าระวัง และแนวทางการดำเนินการดังนี้

รูปแบบการใช้งานที่พบ	เทคนิคการทำงานของมัลแวร์/ภัยคุกคาม	วัตถุประสงค์และผลกระทบ
อีเมลฟิชชิ่ง (Phishing Emails)	• **การอำพรางลิงก์:** ใช้ Redirect URL และบริการ Cloudflare เพื่อให้ระบบสแกนมองว่าเป็นลิงก์ปลอดภัย • **ไฟล์แนบอันตราย:** แนบไฟล์จำพวก .LNK หรือ .ZIP ที่ดูเหมือนเอกสารทั่วไป (เช่น ใบเสนอราคา, ข้อความเสียง)	• หลอกล่อให้เหยื่อคลิกเพื่อเริ่มกระบวนการโจมตี • หลบเลี่ยงตัวกรองสแปมของระบบรักษาความปลอดภัยอีเมล
หน้าเว็บปลอม (Fake Landing Pages)	• **การทำหน้าเว็บปลอมอย่างแนบเนียน:** ใช้พื้นที่ Cloudflare สร้างหน้าล็อกอินปลอม • **ระบบยืนยันตัวตนปลอม:** ใช้ CAPTCHA ปลอมเพื่อหลอกผู้ใช้งานและปิดกั้น Bot ตรวจสอบความปลอดภัย • **การปิดบังเนื้อหา:** ตั้งค่าให้แสดงผลเฉพาะเมื่อมีคน click แต่ซ่อนเนื้อหาจากโปรแกรมตรวจจับอัตโนมัติ	• ขโมยรหัสผ่าน (Credentials) ของผู้ใช้งาน • ป้องกันไม่ให้โปรแกรมสแกนไวรัสตรวจเจอหน้าเว็บอันตรายที่ซ่อนไว้
การสร้างช่องทางพิเศษ (Secure Tunneling)	• **การสร้าง Tunnel:** ใช้บริการเชื่อมต่อเครือข่าย (เช่น Cloudflare Tunnels) มาอำพรางการส่งข้อมูล • **การรับ-ส่งข้อมูลลับ:** ทำให้ทราฟฟิกมัลแวร์ดูเหมือนการใช้งานอินเทอร์เน็ตปกติ	• แอบส่งมัลแวร์เข้ามาฝังตัวในเครื่อง • เข้าควบคุมเครื่องเหยื่อ (Remote Control) โดยที่ระบบป้องกันไม่รู้ตัว
บริการฝากไฟล์ออนไลน์ (Cloud Storage)	• **การใช้โฮสต์ที่น่าเชื่อถือ:** นำไฟล์ไวรัสไปเก็บไว้บนบริการ Cloud Storage • **แหล่งรวบรวมข้อมูล:** ใช้เป็นจุดรับข้อมูลรหัสผ่านที่ผู้ไม่หวังดีขโมยมาได้	• ลดการถูกบล็อกไฟล์ เพราะไฟล์อยู่บนโดเมนที่ระบบความปลอดภัยไว้วางใจ
การเดารหัสผ่าน (Credential Cracking)	• **Brute Force / Password Reuse:** พยายามเข้าสู่ระบบจากรหัสผ่านที่คาดเดาง่ายหรือรหัสที่หลุดมาจากบริการอื่น	• เจาะเข้าสู่ระบบภายในและขยายผลเพื่อยึดครองเครือข่ายทั้งหมด

แนวทางการป้องกัน: <u>สำหรับผู้ดูแลระบบเครือข่ายและระบบคลาวด์</u>

- ตรวจสอบการเข้าถึงเว็บไซต์ที่มีชื่อลงท้ายแปลก เช่น .workers.dev, .trycloudflare.com หรือ .r2.dev หากไม่ได้ใช้บริการเหล่านี้ในการทำงาน ให้บล็อกการเข้าถึงเว็บไซต์อันตรายดังกล่าว
- ควรใช้แนวทางการป้องกันแบบหลายชั้น (Defense-in-Depth) โดยเพิ่มการติดตั้งโปรแกรมตรวจจับและตอบสนองพฤติกรรมผิดปกติบนเครื่องคอมพิวเตอร์พนักงานโดยตรง (EDR) เพื่อปิดช่องโหว่กรณีที่อีเมลอันตรายหลุดรอดเข้ามาได้

<u>สำหรับผู้ใช้งานทั่วไป</u>

- ควรตรวจสอบที่มาของอีเมลอย่างระมัดระวัง หากพบอีเมลที่แจ้งให้กรอกรหัส Device Code ในหน้าต่างอื่น ไม่ควรทำตามเด็ดขาด และเว็บไซต์ที่มีวิธีการรับส่งข้อมูลที่ปลอดภัย (HTTPS) ก็ไม่ใช่เว็บไซต์ที่ปลอดภัยเสมอไป
- ใช้รหัสผ่านที่มีความซับซ้อน, ไม่ใช้รหัสผ่านของบัญชีที่ใช้งานภายในองค์กรซ้ำกับบริการส่วนตัว และพิจารณาเปิดการใช้งานยืนยันตัวตนแบบหลายปัจจัย (MFA)

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

<u>ข้อมูลอ้างอิง</u>

รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 6 พ.ค. 2569