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

ThaiCERT แจ้งเตือนผู้ไม่หวังดีใช้เทคนิค Zombie ZIP เพื่อหลีกเลี่ยง ระบบตรวจจับมัลแวร์ในไฟล์ ZIP

วันที่แจ้งเตือน 16 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์กรณีพบผู้ไม่หวังดีใช้เทคนิค "Zombie ZIP" สำหรับซ่อนมัลแวร์ (Payload) ไว้ในไฟล์บีบอัด (CVE-2026-0866) เพื่อหลบเลี่ยงการตรวจจับจากระบบรักษาความปลอดภัย เช่น โปรแกรม Antivirus และระบบ EDR (Endpoint Detection and Response) เป็นต้น โดยผู้โจมตีจะทำการดัดแปลงข้อมูลส่วน ZIP headers เพื่อหลอกให้ Antivirus เข้าใจว่าข้อมูลในไฟล์ "ไม่ได้ถูกบีบอัด" โดยตั้งค่า Method=0 (STORED) ทำให้ระบบสแกน อ่านข้อมูลไม่พบสัญลักษณ์ (Signature) ของมัลแวร์ ซึ่งนักวิจัยพบว่าเทคนิคนี้สามารถหลบเลี่ยง Antivirus บน VirusTotal ได้ถึง 50 จาก 51 ยี่ห้อ โดยช่องโหว่ดังกล่าวมีความคล้ายคลึงกับช่องโหว่ CVE-2004-0935

ThaiCERT ได้เผยแพร่ตัวอย่างโปรแกรมที่อาจได้รับผลกระทบ และคำแนะนำในการป้องกัน ดังนี้

ตัวอย่างโปรแกรมป้องกันมัลแวร์ที่อาจได้รับผลกระทบจาก Zombie ZIP	• Microsoft (Microsoft Defender) • Avast- Bitdefender • ESET- Kaspersky	• McAfee • Sophos • Trend Micro

แนวทางการป้องกัน

- ตรวจสอบ compression method ใน ZIP header เทียบกับลักษณะข้อมูลจริง
- เพิ่มกลไกตรวจจับความผิดปกติของโครงสร้างไฟล์บีบอัด
- ใช้โหมด Deep Archive Inspection เพื่อตรวจจับมัลแวร์ที่ซ่อนอยู่ภายในไฟล์บีบอัด
- ไม่พึ่งพา metadata ในไฟล์เพียงอย่างเดียว
- เพิ่ม heuristic detection สำหรับ malformed archive
- อัปเดตโปรแกรมป้องกันมัลแวร์และ EDR ให้เป็นเวอร์ชันล่าสุด
- ติดตามคำแนะนำจากผู้ให้บริการโซลูชันด้านความปลอดภัย

คำแนะนำด้านความปลอดภัยเพิ่มเติม

- ควรหลีกเลี่ยงการเปิดไฟล์บีบอัดจากแหล่งที่ไม่น่าเชื่อถือ
- ปิดกั้นหรือ quarantine ไฟล์ archive ที่มีโครงสร้างผิดปกติ
- เฝ้าระวังไฟล์ที่ unzip แล้วเกิดข้อผิดพลาด เช่น unsupported method เป็นต้น
- ตรวจสอบพฤติกรรมของโปรแกรมที่พยายามคลายข้อมูล archive แบบ programmatic
- ใช้ sandbox หรือระบบวิเคราะห์มัลแวร์ก่อนเปิดไฟล์

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

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 13 มี.ค. 2569
2. https://www.bleepingcomputer.com/news/security/new-zombie-zip-technique-lets-malware-slip-past-security-tools/
3. https://kb.cert.org/vuls/id/976247
4. https://kb.cert.org/vuls/id/968818