แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

กลุ่ม Storm-1175 ใช้ payload Medusa Ransomware โจมตีผ่านช่องโหว่หลายรายการ

วันที่แจ้งเตือน 9 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานกรณีกลุ่ม Storm-1175 ซึ่งมีความเชื่อมโยงกับการใช้ Medusa Ransomware ในการโจมตีที่รวดเร็วและมีประสิทธิภาพสูง สามารถเข้าถึงระบบและติดตั้ง ransomware เพื่อขโมยข้อมูลและเรียกค่าไถ่ โดยอุตสาหกรรมการเงินเป็นหนึ่งในเป้าหมาย

จากรายงานของ Microsoft และการวิเคราะห์จากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย พบว่ากลุ่ม Storm-1175 มุ่งเป้าระบบที่เปิดให้เข้าถึงจากภายนอก และยังไม่ได้รับการอัปเดตแพตช์ โดยใช้ช่องโหว่หลายรายการ ทั้งช่องโหว่ Zero-Day และที่เปิดเผยแล้ว (n-day vulnerabilities)

กลุ่มผู้ไม่หวังดีโจมตีด้วยการใช้ช่องโหว่เพื่อเข้าถึงระบบและฝังตัว (persistence) เช่น การสร้างบัญชีผู้ใช้งาน การติดตั้ง web shell หรือเครื่องมือ remote management เป็นต้น เพื่อใช้ในการเคลื่อนย้ายภายในเครือข่าย ขโมยข้อมูล credential และหลบเลี่ยงกลไกด้านความมั่นคงปลอดภัย ก่อนดำเนินการขโมยข้อมูลสำคัญขององค์กรและติดตั้ง Medusa Ransomware ในขั้นตอนสุดท้าย

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการบริหารจัดการช่องโหว่ (Vulnerability Management) อย่างมีประสิทธิภาพ โดยเฉพาะระบบที่เปิดให้เข้าถึงจากภายนอก พร้อมติดตั้งแพตช์ด้านความปลอดภัยตามคำแนะนำของผู้ผลิต และตรวจสอบระบบเพื่อค้นหาสัญญาณของการถูกบุกรุก ควบคู่กับการจำกัดการเข้าถึงระบบจากเครือข่ายภายนอก รวมถึงเฝ้าระวังพฤติกรรมผิดปกติและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง ตลอดจนสำรองข้อมูล (Backup) และทดสอบแผนการกู้คืนระบบอย่างสม่ำเสมอ และปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคามล่าสุด

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/china-linked-storm-1175-exploits-zero.html
2. https://www.microsoft.com/en-us/security/blog/2026/04/06/storm-1175-focuses-gaze-on-vulnerable-web-facing-assets-in-high-tempo-medusa-ransomware-operations