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

VECT 2.0 Ransomware ทำลายไฟล์ข้อมูลขนาดใหญ่ บน Windows, Linux และ VMware ESXi

วันที่แจ้งเตือน 30 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานของนักวิจัยเกี่ยวกับ VECT 2.0 Ransomware (เป็น Ransomware-as-a-Service (RaaS)) มุ่งเป้าทำลายไฟล์ข้อมูลที่มีขนาดไฟล์มากกว่า 128 KB บน ระบบ Windows, Linux และ VMware ESXi

แรนซัมแวร์ดังกล่าวใช้วิธีการเข้ารหัสไฟล์ข้อมูลด้วยอัลกอริทึม ChaCha20-IETF และเปลี่ยนนามสกุลไฟล์เป็น .vect แต่กระบวนการเข้ารหัสมีความบกพร่องในการจัดการค่าสุ่ม (Nonce) เพื่อการเข้ารหัส เป็นผลให้ไฟล์ที่มีขนาดมากกว่า 128 กิโลไบต์ถูกทำลายอย่างถาวรและไม่สามารถกู้คืนได้ แม้จะมีการชำระค่าไถ่ ทั้งนี้ มัลแวร์ดังกล่าวมีพฤติกรรมใกล้เคียงกับ data wiper มากกว่าแรนซัมแวร์ทั่วไป เป็นผลให้เกิดผลกระทบต่อองค์กรที่ตกเป็นเป้าโจมตี

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบเฝ้าระวังและตรวจสอบพฤติกรรมการเข้าถึงระบบที่ผิดปกติ พร้อมทั้งติดตามความผิดปกติในระบบงานต่าง ๆ วิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง รวมถึงจัดให้มีการสำรองข้อมูลอย่างสม่ำเสมอและแยกเก็บออกจากระบบหลัก และเสริมมาตรการเฝ้าระวังและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อให้สามารถตรวจจับและรับมือกับภัยคุกคามได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://cybersecuritynews.com/new-vect-2-0-ransomware-destroys-files/
2. https://research.checkpoint.com/2026/vect-ransomware-by-design-wiper-by-accident/
3. https://www.dsci.in/files/content/advisory/2026/threat-report-feb-2026.pdf