แจ้งเตือน : ช่องโหว่

Alert

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนภัยคุกคาม TargetCompany Ransomware (Linux variant) ที่มุ่งโจมตี VMware ESXi

วันที่แจ้งเตือน 17 มิถุนายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่การแจ้งเตือนเตือนเกี่ยวกับ TargetCompany Ransomware สายพันธุ์ลินุกซ์ (Linux variant) หรือที่รู้จักในชื่อ Mallox, FARGO และ Tohnichi ซึ่งมีเป้าหมายโจมตีองค์กรที่ใช้งานระบบปฏิบัติการลินุกซ์ (Linux) ที่ติดตั้งอยู่บน VMware ESXi

มีลักษณะการโจมตี ดังนี้ (1) ใช้ Shell Script ที่กำหนดเอง เพื่อดาวน์โหลดและเรียกใช้ Payload ตรวจสอบสิทธิผู้ดูแลระบบก่อนเริ่มโจมตี (2) เมื่อเข้าสู่ระบบเป้าหมาย จะเข้ารหัสไฟล์ที่เกี่ยวข้องกับ VM และเปลี่ยนนามสกุลไฟล์เป็น ".locked" (3) สร้างไฟล์ "TargetInfo.txt" และเชื่อมต่อกับ Command and Control Server (C2) พร้อมส่งข้อมูลของเหยื่อ เช่น hostname, IP address เป็นต้น และ (4) แสดงข้อความเรียกค่าไถ่ "HOW TO DECRYPT.txt" เพื่อให้จ่ายเงินแลกกับกุญแจถอดรหัส ทั้งนี้ พิจารณาข้อมูล IOC ได้จากข้อมูลอ้างอิง 2)

ในการนี้ สำนักงาน ก.ล.ต. ขอแนะนำให้หน่วยงานที่ใช้งาน VMware ESXi ควรปฏิบัติตามโดยพิจารณาดำเนินการ ดังนี้

1. อัปเดตแพตช์ด้านความปลอดภัยของระบบอยู่เสมอ
2. เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)
3. สำรองข้อมูล (Data Backup) อย่างสม่ำเสมอ

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจจะเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 10 มิ.ย. 2567
2) https://www.trendmicro.com/en_fi/research/24/f/targetcompany-s-linux-variant-targets-esxi-environments.html
3) https://www.bleepingcomputer.com/news/security/linux-version-of-targetcompany-ransomware-focuses-on-vmware-esxi/