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

แจ้งเตือน การโจมตีของ Dire Wolf Ransomware

วันที่แจ้งเตือน 26 สิงหาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ พบรายงานเกี่ยวกับกลุ่ม Ransomware ชื่อ Dire Wolf ได้ปฏิบัติการโจมตีแบบกำหนดเป้าหมาย (targeted attacks)

Dire Wolf ใช้วิธีโจมตีที่เรียกว่า “Double-Extortion” โดยเข้ารหัสระบบของเหยื่อ พร้อมข่มขู่ว่าจะเปิดเผยข้อมูลที่ถูกขโมยต่อสาธารณะหากไม่จ่ายค่าไถ่ รวมถึงยังใช้เทคนิค Anti-Forensics และ Multi-Stage Attack Chains เพื่อให้แน่ใจว่าการเข้ารหัสสำเร็จ และเพื่อหลีกเลี่ยงการตรวจจับ ทำให้การกู้คืนระบบทำได้ยากขึ้น หน่วยงานจึงควรเฝ้าระวังและบล็อก Indicators of Compromise (IOCs) ที่เกี่ยวข้อง ดังนี้

Type	File name	Hash
Win64 EXE	data345.exe	**MD5:** A71dbf2e20c04da134f8be86ca93a619 **SHA-1:** Ed7c9fbd42605c790660df86b7ec325490f6d827 **SHA-256:** 8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
Win64 EXE	data345.exe (unpacked)	**MD5:** aa62b3905be9b49551a07bc16eaad2ff **SHA-1:** 4a5852e9f9e20b243d8430b229e41b92949e4d69 **SHA-256:** 27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3

เพื่อป้องกันความเสี่ยงและผลกระทบที่อาจเกิดขึ้น หน่วยงานควรติดตามพฤติกรรมที่ผิดปกติในระบบ รวมถึงมีการสำรองข้อมูลหลายชุดที่ทดสอบกู้คืนได้จริง รวมถึงสอบทานมาตรการป้องกัน ซักซ้อมแผนตอบสนองและแผนความต่อเนื่องทางธุรกิจ กรณีถูกแรนซัมแวร์เข้ารหัส ครอบคลุมกระบวนการตัดสินใจ การสื่อสาร และแผนการกู้คืนระบบ ทั้งนี้ หากเกิดเหตุที่กระทบความมั่นคงปลอดภัยของระบบสารสนเทศ ขอให้รายงานผ่านระบบ Incident Report ของสำนักงาน ก.ล.ต. ทันที

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

ข้อมูลอ้างอิง

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-082
2. https://www.csoonline.com/article/4042182/singapore-issues-critical-alert-on-dire-wolf-ransomware-targeting-global-tech-and-manufacturing-firms.html
3. https://www.facebook.com/techmovementofficial

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ