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 Gentlemen Ransomware และ Kyber Ransomware ขยายการโจมตีหลายหน่วยงาน

วันที่แจ้งเตือน 24 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานของนักวิจัยว่า กลุ่ม Gentlemen Ransomware (เป็น Ransomware-as-a-Service (RaaS)) และ Kyber Ransomware มุ่งโจมตีระบบ Windows, Linux และ VMware ESXi

1. **Gentlemen Ransomware** ใช้มัลแวร์ SystemBC ซึ่งเป็นเครือข่ายบอทเน็ตเข้าโจมตี โดยมุ่งเป้าไปยังระบบที่ให้เข้าถึงจากอินเทอร์เน็ตและมีช่องโหว่ เช่น VPN, remote access gateways และระบบ firewall management เพื่อเข้าถึงเครือข่ายขององค์กร ซึ่งใช้เครื่องมือและโครงสร้างพื้นฐานที่รองรับหลายแพลตฟอร์ม เช่น Windows, Linux และ VMware ESXi เพื่อเพิ่มความสามารถในการโจมตีในวงกว้าง

2. **Kyber Ransomware** มุ่งโจมตีระบบ Windows และ VMware ESXi โดย รายงานระบุว่า พบมัลแวร์ 2 เวอร์ชันที่ถูกใช้ในเครือข่ายเดียวกัน (1) เวอร์ชัน VMware ESXi มีความสามารถในการเข้ารหัสไฟล์ใน datastore ขัดขวางการทำงานของ virtual machine และปรับเปลี่ยนหน้าอินเทอร์เฟซ เพื่อแสดงข้อความเรียกค่าไถ่ และ (2) เวอร์ชัน Windows มุ่งเป้าไปที่ Windows file servers มีฟีเจอร์สำหรับโจมตี Hyper-V และขัดขวางการทำงาน Virtual Machines ลบข้อมูลสำรอง รวมถึงทำลายช่องทางการกู้คืนข้อมูล เช่น การลบ shadow copies และ event logs เพื่อขยายความรุนแรงของการโจมตีในระดับโครงสร้างพื้นฐาน ทั้งนี้ พบว่ามีการใช้การเข้ารหัสแบบ Hybrid Approach (Kyber1024 ร่วมกับ X25519) เพื่อป้องกันคีย์ที่อาจถูกโจมตีจากคอมพิวเตอร์ควอนตัม

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบเฝ้าระวังและตรวจสอบพฤติกรรมการใช้งานระบบผ่านเครือข่ายอินเตอร์เน็ตที่ผิดปกติ ควบคุมสิทธิ์การเข้าถึงโดยเฉพาะบัญชีผู้ดูแลระบบ รวมถึงจัดให้มีการสำรองข้อมูลอย่างสม่ำเสมอและแยกเก็บออกจากระบบหลัก ตรวจสอบการเชื่อมต่อเครือข่ายที่ผิดปกติ และเสริมมาตรการเฝ้าระวังและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อให้สามารถตรวจจับและรับมือกับภัยคุกคามได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/the-gentlemen-ransomware-now-uses-systembc-for-bot-powered-attacks/
2. https://www.bleepingcomputer.com/news/security/kyber-ransomware-gang-toys-with-post-quantum-encryption-on-windows/
3. https://www.rapid7.com/blog/post/tr-kyber-ransomware-double-trouble-windows-esxi-attacks-explained/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ