แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนภัยเฝ้าระวังกลุ่ม 0APT Ransomware

วันที่แจ้งเตือน 11 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานภัยคุกคามทางไซเบอร์กรณีกลุ่มผู้ไม่หวังดี 0APT (0APT Syndicate) ซึ่งอ้างตัวว่าเป็นผู้ให้บริการมัลแวร์เรียกค่าไถ่ (Ransomware-as-a-Service: RaaS) มุ่งเป้าโจมตีหน่วยงานที่มีชื่อเสียงโดยมีเป้าหมายเพื่อเจาะระบบ ขโมยข้อมูลสำคัญ และทำการเข้ารหัสไฟล์และนำชื่อองค์กรไปเปิดเผยบน DarkWeb โดยเริ่มพบการโจมตีในช่วงปลายเดือนมกราคมที่ผ่านมา

รูปแบบลักษณะการโจมตี:

- การเข้าถึงเข้าระบบ (Initial Access) สแกนหาช่องโหว่ซอฟต์แวร์ หรือใช้รหัสผ่านที่รั่วไหลจาก Dark Web
- การแทรกซึมภายในเครือข่าย (Lateral Movement) ขยายสิทธิการเข้าถึง (Privilege Escalation) เพื่อยึดครองเครื่องแม่ข่าย และฐานข้อมูล
- การข่มขู่เรียกค่าไถ่ (Double Extortion) ขโมยข้อมูลก่อนทำการล็อกระบบ เพื่อใช้ต่อรองและสร้างความกดดันต่อชื่อเสียง

แนวทางการป้องกันและเฝ้าระวัง:

1. การจัดการระบบและโปรแกรม (Updates & Patching)
   - ดำเนินการอัปเดตระบบปฏิบัติการและแอปพลิเคชันของหน่วยงานอย่างสม่ำเสมอ รวมถึงอุปกรณ์สื่อสารเคลื่อนที่
   - ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส/มัลแวร์ ให้เป็นปัจจุบันและสแกนไวรัสในระบบอย่างสม่ำเสมอ
2. การสำรองข้อมูล (Backup)
   - สำรองข้อมูลอย่างสม่ำเสมอ ทั้งในรูปแบบออนไลน์และออฟไลน์ โดยแยกจากเครือข่ายหลักหรือบนระบบคลาวด์ เพื่อป้องกันการทำลายข้อมูลสำรอง
3. การแบ่งส่วนพื้นที่ติดตั้งอุปกรณ์และเครือข่าย (Asset & Network Compartmentalization)
   - การแบ่งประเภทและส่วนจัดเก็บข้อมูล โดยแยกส่วนจัดเก็บข้อมูลสำคัญ (Sensitive Data) ออกจากข้อมูลทั่วไป
   - การแบ่งส่วนเครือข่าย (Network Segregation) เพื่อจำกัดขอบเขตการเข้าถึงส่วนอื่นภายในเครือข่ายได้
   - การควบคุมการเชื่อมต่อระยะไกล (RDP) จำกัดการเข้าถึงทรัพยากรภายใน และบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA)
4. การตรวจสอบและทดสอบระบบ (Monitoring & Testing)
   - ตรวจสอบและเฝ้าระวังการลักลอบส่งข้อมูลออกภายนอก (Data Exfiltration) เพื่อลดผลกระทบจากการถูกข่มขู่เปิดเผยข้อมูล
   - การดำเนินการทดสอบเจาะระบบ (Penetration Testing) และทดสอบกระบวนการฟื้นฟูข้อมูลเป็นประจำ
5. การลดความเสี่ยงจากเนื้อหาอันตราย (Malicious Content Mitigation)
   - การจำกัดสภาพแวดล้อมการทำงาน โดยปิดการใช้งานสคริปต์ (Script) และมาโคร (Macros) ที่ไม่จำเป็น
   - การกรองข้อมูลและจราจรเครือข่าย ตั้งค่าระบบเพื่อตรวจสอบเนื้อหาและอนุญาตเฉพาะไฟล์ประเภทที่กำหนด รวมถึงการทำ Whitelisting /Blacklisting เพื่อปิดกั้นการเข้าถึงเว็บไซต์ที่มีความเสี่ยง
6. การจัดการสิทธิ (Identity & Privilege Management)
   - ใช้นโยบายรหัสผ่านที่ซับซ้อน (Password Complexity) และการยืนยันตัวตนหลายปัจจัย (MFA) ในระบบสำคัญ
   - การบริหารจัดการสิทธิผู้ใช้งาน (Privileged Accounts) ให้สิทธิเท่าที่จำเป็น (Least Privilege) และแบ่งแยกหน้าที่ (Segregation of Duties)
7. ความปลอดภัยการทำงานนอกสถานที่ (Teleworking Security)
   - การควบคุมการใช้งานอุปกรณ์ส่วนตัว การเข้ารหัสฮาร์ดดิสก์ การควบคุมสื่อบันทึกข้อมูลภายนอก (USB) และจัดให้มีกระบวนการระงับการเข้าถึงอุปกรณ์ระยะไกล กรณีสูญหายหรือถูกโจรกรรม
   - การเข้าใช้งานผ่านระบบสาธารณะ กำหนดนโยบายห้ามหรือจำกัดการเข้าถึงข้อมูลองค์กรผ่าน Wi-Fi สาธารณะที่ไม่มีความปลอดภัย
8. สร้างความตระหนักรู้และมาตรการสนับสนุน
   - การฝึกอบรมบุคลากร สร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ โดยเฉพาะการหลอกลวงทางอีเมล (Phishing)
   - การถ่ายโอนความเสี่ยง เช่น พิจารณาการทำประกันภัยความรับผิดทางไซเบอร์ (Cyber Liability Insurance)

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 11 ก.พ. 2569
2) https://socradar.io/blog/dark-web-profile-0apt-ransomware/