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

นักวิจัยเตือน พบ VoidStealer มัลแวร์ขโมยข้อมูลผ่านเบราว์เซอร์ Chrome และ Callback Phishing ผ่าน Microsoft Azure Monitor Alerts

วันที่แจ้งเตือน 23 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบกรณีนักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์แจ้งเตือนภัยคุกคามซึ่งอาจส่งผลกระทบต่อระบบสารสนเทศและข้อมูลขององค์กร ได้แก่ (1) กรณี VoidStealer มัลแวร์ขโมยข้อมูล ที่มีความสามารถหลีกเลี่ยงการป้องกันของเว็บเบราว์เซอร์ Chrome และ (2) กรณี Callback Phishing ที่อาศัยบริการแจ้งเตือนของระบบคลาวด์

1. **VoidStealer มัลแวร์ขโมยข้อมูล (infostealer) ในเว็บเบราว์เซอร์ Chrome** ใช้การเทคนิค debugger แบบใหม่ที่ bypass การทำงานของ Application-Bound Encryption (ABE) ซึ่งเชื่อมต่อเพื่อเข้าถึงข้อมูลที่ถูกป้องกันในเว็บเบราว์เซอร์ เพื่อดักจับและดึงค่า master key ของ Chrome ออกจากหน่วยความจำ เพื่อนำไปใช้ถอดรหัสข้อมูลสำคัญได้ ซึ่งเทคนิคดังกล่าวมีความซับซ้อนและสามารถหลีกเลี่ยงการตรวจจับจากระบบรักษาความมั่นคงปลอดภัยแบบเดิมได้

2. **การโจมตีแบบ Callback Phishing ผ่าน Microsoft Azure Monitor Alerts** โดยผู้ไม่หวังดีใช้การโจมตีแบบ callback phishing ผ่านบริการแจ้งเตือนของ Microsoft Azure Monitor โดยตั้งค่าข้อความแจ้งเตือนและแนบหมายเลขโทรศัพท์ปลอม เพื่อหลอกลวงให้เหยื่อติดต่อกลับ เมื่อเหยื่อติดต่อไปยังหมายเลขดังกล่าว ผู้ไม่หวังดีจะปลอมตัวเป็นเจ้าหน้าที่ทางเทคนิคของ Microsoft และหลอกให้เหยื่อเปิดเผยข้อมูลสำคัญหรือข้อมูลยืนยันตัวตน เพื่อนำไปใช้เข้าถึงระบบขององค์กร ทั้งนี้ การโจมตีนี้อาศัยความน่าเชื่อถือของระบบที่ถูกต้องและใช้ช่องทางโทรศัพท์เพื่อหลีกเลี่ยงมาตรการป้องกัน phishing แบบเดิม

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการอัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด รวมถึงเฝ้าระวังพฤติกรรมผิดปกติของระบบและการเข้าถึงข้อมูลสำคัญ ตรวจสอบความถูกต้องของการแจ้งเตือนจากระบบต่าง ๆ อย่างรัดกุม และหลีกเลี่ยงการติดต่อกลับผ่านช่องทางที่ไม่ได้รับการยืนยัน พร้อมทั้งส่งเสริมการสร้างความตระหนักรู้แก่ผู้ใช้งานเกี่ยวกับภัยคุกคามแบบ social engineering ตลอดจนเพิ่มการเฝ้าระวังและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) เพื่อให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/voidstealer-malware-steals-chrome-master-key-via-debugger-trick
2. https://www.bleepingcomputer.com/news/security/microsoft-azure-monitor-alerts-abused-in-callback-phishing-campaigns
3. https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/overview

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ