แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ThaiCERT แจ้งเตือน แคมเปญการโจมตีจากกลุ่มผู้ไม่หวังดี Silver Fox โดยใช้เทคนิค Social Engineering และการซ่อนคำสั่งในไฟล์เอกสารด้านการเงิน

วันที่แจ้งเตือน 30 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์กรณีพบกลุ่มผู้ไม่หวังดี Silver Fox ใช้เทคนิค Social Engineering (Phishing email) โดยใช้บริบทที่เกี่ยวข้องกับหน่วยงานด้านการเงิน เช่น การส่ง เอกสารภาษี เอกสารการเงิน และบัญชีองค์กร เป็นต้น เพื่อหลอกให้ผู้ใช้งานเปิดไฟล์หรือดาวน์โหลดโปรแกรมอันตราย ทั้งนี้ พบว่ามีการกระจายแคมเปญในหลายประเทศในภูมิภาคเอเชีย รวมถึงประเทศไทย

รายละเอียดช่องโหว่: กลุ่ม Silver Fox เป็นกลุ่มภัยคุกคามทางไซเบอร์ที่มีการพัฒนาและปรับเปลี่ยนแนวทางการโจมตีอย่างต่อเนื่อง โดยมีการใช้เทคนิค Phishing ผ่านอีเมลปลอมและเอกสารที่มีลักษณะน่าเชื่อถือ โดยพบว่ากลุ่มดังกล่าวมีการปรับเปลี่ยนรูปแบบการโจมตีและเครื่องมืออย่างต่อเนื่องเพื่อเพิ่มประสิทธิภาพและหลีกเลี่ยงการตรวจจับ โดยในปัจจุบันมีการใช้หลากหลายวิธีการและเครื่องมือในการดำเนินการโจมตี ได้แก่	**1. Remote Access Trojan (RAT)** ได้แก่ ValleyRAT หรือ Winos เป็นมัลแวร์ ที่ผู้ไม่หวังดีใช้ควบคุมระบบของเหยื่อจากระยะไกล โดยมีความสามารถรองรับการดำเนินการได้หลากหลาย เช่น การบันทึกการกดแป้นพิมพ์ การเข้าถึงและถ่ายโอนข้อมูล การสั่งรันคำสั่งเพิ่มเติม รวมถึงการพยายามหลีกเลี่ยงกลไกการตรวจจับของระบบรักษาความปลอดภัย เพื่อรักษาการเข้าถึงระบบของเครื่องเหยื่อ **2. Remote Monitoring and Management (RMM)** เป็นซอฟต์แวร์ที่องค์กรใช้สำหรับบริหารจัดการอุปกรณ์ปลายทาง เช่น การติดตั้งซอฟต์แวร์ การอัปเดตระบบ และการเข้าควบคุมเครื่องเหยื่อ เนื่องจากเป็นซอฟต์แวร์ที่ถูกต้องตามกฎหมายและมีการใช้งานจริงในองค์กร อาจทำให้การตรวจจับจากระบบความมั่นคงปลอดภัยทำได้ยากขึ้นเมื่อเทียบกับมัลแวร์ทั่วไป **3. มัลแวร์ประเภท Stealer** (พัฒนาโดยภาษา Python) ใช้สำหรับขโมยข้อมูลสำคัญ เช่น Credentials และข้อมูลจากเบราว์เซอร์ เป็นต้น

ผลกระทบที่อาจเกิดขึ้น:

- ข้อมูลบัญชีผู้ใช้งาน (Credentials) ถูกขโมย
- ข้อมูลจากเบราว์เซอร์และเอกสารสำคัญถูกเข้าถึง
- เครื่องถูกใช้เป็นจุดเริ่มต้นในการโจมตีระบบขององค์กร (Initial Access) และอาจถูกต่อยอดไปยังการโจมตีอื่น เช่น การเข้าถึงอีเมลองค์กร การหลอกลวงทางการเงิน หรือการเคลื่อนย้ายภายในเครือข่าย (Lateral Movement)

แนวทางป้องกัน: • กรองและตรวจสอบอีเมลที่เกี่ยวข้องกับภาษีหรือเอกสารการเงินอย่างเข้มงวด • จำกัดการดาวน์โหลดไฟล์ ZIP/RAR และไฟล์ปฏิบัติการจากแหล่งที่ไม่น่าเชื่อถือ • ตรวจสอบการรันไฟล์จากโฟลเดอร์ เช่น %TEMP% และ Downloads • เฝ้าระวังการใช้งานเครื่องมือ RMM ที่ไม่ได้รับอนุญาต	• ตรวจสอบการเชื่อมต่อไปยังโดเมนหรือ IP ที่ผิดปกติ • ใช้ EDR/Antivirus ที่สามารถตรวจจับพฤติกรรมผิดปกติได้ • จำกัดการเข้าถึงอุปกรณ์จากเครือข่ายภายนอก และอนุญาตเฉพาะแหล่งที่จำเป็นเท่านั้น • เฝ้าระวังตรวจสอบข้อมูลจาก IoCs เพิ่มเติมได้จากอ้างอิง 2

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะ เกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 30 มี.ค. 2569
2. https://blog.sekoia.io/silver-fox-the-only-tax-audit-where-the-fine-print-installs-malware/?