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

มัลแวร์ GoGra ใน Linux ใช้ Microsoft Graph API เป็นช่องทางโจมตี

วันที่แจ้งเตือน 24 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานของนักวิจัยเกี่ยวกับ GoGra Malware ประเภท Linux Backdoor ซึ่งเชื่อมโยงกับผู้ไม่หวังดีกลุ่ม Harvester มุ่งเป้าโจมตีหน่วยงานจำนวนมาก

นักวิจัยระบุว่ามัลแวร์นี้สร้างขึ้นใหม่และใช้ Microsoft Graph API และโครงสร้างพื้นฐานของ Microsoft เช่น Outlook mailbox เป็นต้น เป็นช่องทางในการ payload เพื่อใช้ในการโจมตี โดยมัลแวร์จะใช้ประโยชน์จากเครื่องมือการยันยันตัวตนของ Active Directory เพื่อรับ OAuth2 token ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงและดำเนินการภายในระบบได้โดยยากต่อการถูกตรวจจับ

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบเฝ้าระวังการใช้งาน Microsoft Graph API และการเข้าถึง Outlook mailbox ภายในองค์กร รวมถึงเฝ้าระวังการใช้งานบัญชี Active Directory ที่อาจถูกนำไปใช้โดยไม่ได้รับอนุญาต และตรวจสอบพฤติกรรมการใช้งานระบบที่ผิดปกติ ตรวจสอบการเชื่อมต่อเครือข่ายที่ผิดปกติ พร้อมทั้งติดตามตรวจสอบบันทึกเหตุการณ์ (Log Monitoring) เพื่อให้สามารถตรวจจับและตอบสนองต่อความพยายามโจมตี และสามารถรับมือกับภัยคุกคามได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/new-gogra-malware-for-linux-uses-microsoft-graph-api-for-comms/
2. https://www.security.com/blog-post/harvester-new-linux-backdoor-gogra
3. https://securityaffairs.com/191153/uncategorized/microsoft-graph-api-misused-by-new-gogra-linux-malware-for-hidden-communication.html