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

Phishing Campaign ผ่าน Google Cloud Storage หลบเลี่ยงการตรวจจับ E-mail Filtering และแพร่มัลแวร์ Remcos RAT

วันที่แจ้งเตือน 16 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่ากลุ่มผู้ไม่หวังดีอาศัย Google Cloud Storage เพื่อโฮสต์หน้าฟิชชิง (Phishing) ที่ปล่อยมัลแวร์อันตราย Remcos RAT

รูปแบบการโจมตี (Attack Pattern)	ความเสี่ยง (Risks) และ ผลกระทบ (Impacts)
1. ส่งอีเมลฟิชชิง: ใช้โดเมนของ Google (storage.googleapis.com) เพื่อเลี่ยงการตรวจจับ 2. หน้าล็อกอินปลอม: นำเหยื่อไปยังหน้าเว็บที่หน้าตาเหมือน Google Drive เพื่อหลอกให้กรอกอีเมล รหัสผ่าน และ OTP 3. หลอกให้ดาวน์โหลดไฟล์สคริปต์ JavaScript (.js) 4. อาศัยการหลบเลี่ยงแบบหน่วงเวลา: ไฟล์ JS จะหน่วงเวลาการทำงาน เพื่อหลอกระบบ Sandbox อัตโนมัติ 5. รันสคริปต์ซ้อนสคริปต์ (Obfuscated) : สคริปต์จะเรียกใช้งาน VBS และ PowerShell โดยไม่ทิ้งร่องรอยเป็นไฟล์ไว้ (Fileless) 6. ฝังตัวในโปรเซสที่น่าเชื่อถือ: ใช้ไฟล์ .NET loader เพื่อนำเข้ามัลแวร์ในโปรเซส RegSvcs.exe ของ Microsoft เพื่อข้ามการตรวจจับแอนตี้ไวรัส 7. มัลแวร์ Remcos RAT ทำการเชื่อมต่อกลับไปยังเซิร์ฟเวอร์(C2) และฝังตัวใน Registry เพื่อทำงานอัตโนมัติเมื่อเปิดเครื่อง	• แคมเปญนี้มีความน่าเชื่อถือสูงมาก เพราะใช้โครงสร้างพื้นฐานของ Google ทำให้ผู้ใช้งานทั่วไปอาจไม่ทันระวังตัว • แอนตี้ไวรัสแบบดั้งเดิม (Signature-based) ที่อาศัยการตรวจสอบจาก file reputation หรือ ข้อมูลจาก known malicious domains มักตรวจไม่พบ เนื่องจากมัลแวร์ทำงานในหน่วยความจำ (In-memory) และใช้ไฟล์ที่ถูกรับรองเป็นเครื่องมือบังหน้า • ถูกขโมยข้อมูลสำคัญ เช่น ข้อมูลบัญชีและรหัสผ่าน เป็นต้น • ถูกสอดแนมผ่านการกดแป้นพิมพ์ (Keylogging) แคปหน้าจอ แอบเปิดไมโครโฟน/กล้องเว็บแคม • ข้อมูลรั่วไหล สูญเสียข้อมูลสำคัญ • ความเสียหายทางการเงิน หรือเรียกค่าไถ่ (Ransomware) • การลุกลามภายในเครือข่าย (Lateral Movement) • ความเสียหายต่อชื่อเสียง
แนวทางการป้องกันหรือแก้ไข (Prevention/Mitigation): 1. อัปเดตและใช้ระบบข้อมูลภัยคุกคามแบบเรียลไทม์ (Threat Intelligence Feeds) เพื่อบล็อก IP หรือรูปแบบพฤติกรรม (IOCs) ของมัลแวร์ที่ตรวจพบในระบบเครือข่าย หรือ พิจารณาใช้เครื่องมือ Interactive Sandbox เพื่อตรวจสอบพฤติกรรมของลิงก์และไฟล์ ต้องสงสัยแทนการพึ่งพาเพียงข้อมูลจากโดเมนต้องสงสัยหรือฐานข้อมูลไวรัส	2. ตรวจสอบลิงก์ที่มาจาก storage.googleapis.com ด้วยความระมัดระวัง (ไม่คลิก/กรอกข้อมูลหากไม่ได้เป็นผู้ร้องขอ) 3. ปรับจูนระบบ EDR/SIEM เพื่อเฝ้าระวังพฤติกรรมที่ผิดปกติของไฟล์ระบบ เช่น RegSvcs.exe PowerShell หรือ WScript ที่มีการเชื่อมต่อไปยังเครือข่ายภายนอก 4. ฝึกอบรมพนักงานเกี่ยวกับรูปแบบฟิชชิง และระวังการดาวน์โหลดไฟล์จากการแจ้งเตือนล็อกอินที่ผิดปกติ

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

ข้อมูลอ้างอิง

1. https://cybersecuritynews.com/hackers-using-google-cloud-storage-to-bypass-email-filters/
2. https://any.run/cybersecurity-blog/phishing-google-drive-remcos/
3. https://www.cryptika.com/hackers-using-google-cloud-storage-to-bypass-email-filters-and-deliver-remcos-rat/