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

แคมเปญฟิชชิ่งของกลุ่ม Sapphire Sleet หลอกอัปเดตโปรแกรม Zoom ปลอม ก่อนกระจายมัลแวร์ขโมยข้อมูลสำคัญ

วันที่แจ้งเตือน 20 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับแคมเปญการโจมตีแบบ Phishing และ Social Engineering ของกลุ่ม Sapphire Sleet มีเป้าหมายเป็นกลุ่มผู้ใช้โปรแกรม Zoom บนระบบปฏิบัติการ MacOS

ผู้ไม่หวังดีจะส่งคำเชิญเข้าร่วมประชุมที่มีลิงก์ดาวน์โหลดอัปเดตโปรแกรม Zoom ปลอม เมื่อผู้ใช้งานเปิดไฟล์ดังกล่าว Script Editor จะรันคำสั่ง shell เพื่อดาวน์โหลด payload เพิ่มเติมจากเซิร์ฟเวอร์ของผู้ไม่หวังดี และติดตั้งมัลแวร์ประเภท credential stealer ที่ใช้ขโมยข้อมูลสำคัญและส่งออกผ่าน Telegram Bot API เช่น รหัสผ่าน และข้อมูลทางการเงิน เป็นต้น รวมทั้งติดตั้ง backdoor เพิ่มเติม เช่น icloudz เพื่อใช้ควบคุมระบบได้จากระยะไกล และในขั้นตอนสุดท้ายของการโจมตี ระบบจะแสดงข้อความหลอกเพื่อให้ผู้ใช้งานเข้าใจว่าการอัปเดตเสร็จสมบูรณ์แล้ว

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินมาตรการที่เหมาะสม โดยสร้างความตระหนักให้แก่พนักงานเกี่ยวกับภัยคุกคามจากอีเมลหรือข้อความที่น่าสงสัย ดาวน์โหลดซอฟต์แวร์หรืออัปเดตระบบจากเว็บไซต์ทางการของผู้ผลิตเท่านั้น และเพิ่มการเฝ้าระวังพฤติกรรมการเชื่อมต่อที่ผิดปกติภายในเครือข่าย หรือการใช้งานเครื่องมือ Remote Access รวมทั้งควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์

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

ข้อมูลอ้างอิง

1. https://cybersecuritynews.com/fake-zoom-sdk-update-delivers-sapphire-sleet-malware/
2. https://www.microsoft.com/en-us/security/blog/2026/04/16/dissecting-sapphire-sleets-macos-intrusion-from-lure-to-compromise/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ