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

พบมัลแวร์บนระบบปฏิบัติการ Android มุ่งโจมตีแอปพลิเคชันทางการเงิน

วันที่แจ้งเตือน 13 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานของนักวิจัยด้าน Cybersecurity กรณีพบมัลแวร์บนระบบปฏิบัติการ Android จำนวน 6 กลุ่ม ที่ถูกพัฒนาขึ้นเพื่อโจมตีแอปพลิเคชันทางการเงิน ซึ่งสามารถใช้ในการขโมยข้อมูลสำคัญจากอุปกรณ์ของผู้ใช้และดำเนินการฉ้อโกงทางการเงินได้

มัลแวร์ที่พบเป็นทั้งประเภท Traditional Banking Trojan และ Fully Remote Administration Tool: RAT ได้แก่ มัลแวร์ PixRevolution, TaxiSpy RAT, BeatBanker, Mirax, Oblivion RAT และ SURXRAT โดย PixRevolution สามารถใช้เทคนิค overlay attack เพื่อแสดงหน้าจอปลอมบนอุปกรณ์ของเหยื่อ และหลอกลวงให้เหยื่อดำเนินการยืนยันธุรกรรม จากนั้นจะทำการเปลี่ยนเส้นทางการโอนเงินไปยังบัญชีของผู้ไม่หวังดี รวมทั้งมัลแวร์หลายรายการยังใช้ความสามารถของ Android Accessibility Service เพื่อควบคุมอุปกรณ์ของเหยื่อ อ่านข้อมูลบนหน้าจอ และดำเนินการส่งคำสั่งแทนผู้ใช้งาน ทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลบัญชีผู้ใช้ รหัสผ่าน รหัสยืนยันตัวตนแบบครั้งเดียว (OTP) และข้อมูลธุรกรรมทางการเงินได้ เป็นต้น

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินมาตรการด้านความมั่นคงปลอดภัยสำหรับอุปกรณ์เคลื่อนที่อย่างเหมาะสม โดยสร้างความตระหนักรู้ให้บุคลากรเพื่อพิจารณาติดตั้งแอปพลิเคชันจากแหล่งที่เชื่อถือได้เท่านั้น ตรวจสอบและจำกัดการให้สิทธิ์ Accessibility Service กับแอปพลิเคชันที่ไม่จำเป็น รวมทั้งอัปเดตระบบปฏิบัติการและแอปพลิเคชันให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ นอกจากนี้ควรเฝ้าระวังพฤติกรรมที่ผิดปกติของธุรกรรมทางการเงินและเพิ่มมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพื่อช่วยลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/03/six-android-malware-families-target-pix.html

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ