แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [ ] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนผู้ใช้งาน Android และ iOSระวังมัลแวร์ GoldPickaxe

วันที่แจ้งเตือน 27 กุมภาพันธ์ 2567

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานจากบริษัท Group-IB ผู้ให้บริการด้านนวัตกรรมและโซลูชันสำหรับการจัดการกับภัยคุกคามทางไซเบอร์ ที่ตรวจพบมัลแวร์ GoldPickaxe ซึ่งกลุ่มผู้ไม่หวังดี “GoldFactory” พัฒนาขึ้น โดยกำหนดเป้าหมายไปยังผู้ใช้งานระบบปฏิบัติการ Android และ iOS ในกลุ่มอุตสาหกรรมภาคการเงิน

กลุ่มผู้ไม่หวังดีดังกล่าวใช้วิธีการโจมตีแบบ Social Engineering ส่งข้อความหลอกลวง (Phishing) ผ่านทาง Short Message Service (SMS) แอบอ้างเป็นหน่วยงานของรัฐ เพื่อหลอกให้เหยื่อติดตั้งแอปพลิเคชันปลอม โดยให้ผู้ใช้งานสแกนใบหน้า ส่งข้อมูล หรือเอกสารประจำตัว และนำข้อมูลดังกล่าวไปสวมรอยเป็นเหยื่อ(สร้าง Deepfake) เพื่อเข้าถึงบัญชีธนาคารของเหยื่อ รวมถึงสามารถดักขโมยข้อความ SMS เพื่อใช้ยืนยันการทำธุรกรรมผ่าน Mobile Banking

ทั้งนี้ เป้าหมายการโจมตี คือ ผู้ใช้งานระบบปฏิบัติการ Android และ iOS โดยเฉพาะประเทศในแถบภูมิภาค Asia-Pacific รวมถึงประเทศไทย และเวียดนาม

สำหรับผู้ใช้งานระบบปฏิบัติการ Androidผู้ไม่หวังดีจะส่งลิงก์สำหรับดาวน์โหลดแอปพลิเคชันปลอม ผ่านทาง SMS โดยตรง และสำหรับผู้ใช้งานระบบปฏิบัติการ iOS ผู้ไม่หวังดีจะหลอกให้เหยื่อติดตั้งโปรแกรมบริหารจัดการอุปกรณ์เคลื่อนที่ (Mobile Device Management : MDM) ซึ่งโปรแกรมจะอนุญาตให้ผู้ไม่หวังดีสามารถเข้าควบคุมอุปกรณ์เคลื่อนที่ของเหยื่อได้จากระยะไกล เช่น การล้างข้อมูลระยะไกล การติดตามอุปกรณ์ การจัดการแอปพลิเคชัน และสามารถดึงข้อมูลที่ต้องการได้ เป็นต้น

ThaiCERT แนะนำให้ผู้ที่ใช้งานระบบปฏิบัติการ Android และ iOS เฝ้าระวัง เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศ เพื่อป้องกันผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่ดังกล่าว และลดความเสี่ยงในการถูกโจมตี

นอกจากนี้บริษัท Group-IB ได้มีคำแนะนำ และรายการตัวบ่งชี้การโจมตี (Indicators of compromise: IOCs) เพื่อเป็นแนวทางสำหรับองค์กรและผู้ใช้งาน ในการป้องกันและเฝ้าระวังภัยคุกคามจากมัลแวร์ GoldPickaxe (อ้างอิง 2)

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 23 ก.พ. 2567
2) https://www.group-ib.com/blog/goldfactory-ios-trojan/
3) https://www.bankinfosecurity.com/banking-trojan-goldpickaxe-harvests-facial-biometrics-a-24370
4) https://www.forbes.com/sites/zakdoffman/2024/02/15/apple-iphone-15-iphone-16-upgrade-warning-faceid-ios-17-and-ios-18/?sh=26ad3fe6615e