การควบคุมเครื่องเหยื่อ จุดเริ่มต้นของการขโมยตัวตนดิจิทัล

1. บทนำ

การควบคุมเครื่องเหยื่อ (อุปกรณ์ของเหยื่อ เช่น สมาร์ตโฟน) โดยไม่ได้รับอนุญาต เป็นหนึ่งในภัยคุกคามร้ายแรงต่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (digital ID) การควบคุมอุปกรณ์ปลายทาง (device takeover) ทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลส่วนตัว แอบอ้างตัวตน เข้าบัญชีธนาคาร ทำธุรกรรม หรือยึดสิทธิ์ในการทำธุรกรรมทางอิเล็กทรอนิกส์ของเหยื่อได้ โดยไม่จำเป็นต้องโจมตีที่ระบบของผู้ให้บริการโดยตรง

ภัยคุกคามนี้มักเริ่มจากการโจมตีแบบ วิศวกรรมสังคม (social engineering) โดยการหลอกให้เหยื่อติดตั้งแอปพลิเคชันปลอมที่แฝง malware ซึ่งแอปพลิเคชันเหล่านี้จะขอสิทธิ์ในการควบคุมอุปกรณ์ผ่าน Accessibility Service และอาจใช้เทคนิค Screen Overlay เพื่อซ้อนทับหน้าจอ เพื่อไม่ให้เหยื่อรู้ตัวว่ากำลังถูกควบคุมอุปกรณ์อยู่

จากรายงานของศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector Computer Emergency Response Team: TB-CERT) และการสัมภาษณ์ผู้เชี่ยวชาญ พบว่าเหยื่อจำนวนมากถูกล่อลวงโดยผู้ไม่หวังดีที่แอบอ้างเป็นหน่วยงานรัฐหรือธนาคาร เพื่อชักชวนให้ดาวน์โหลดแอปพลิเคชันปลอมและมอบสิทธิ์ที่นำไปสู่การควบคุมอุปกรณ์

การเข้าใจกลไก เทคนิค และผลกระทบของการควบคุมอุปกรณ์จึงเป็นสิ่งจำเป็นสำหรับผู้ให้บริการ Digital ID หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ และผู้กำหนดนโยบาย เพื่อออกแบบมาตรการป้องกันที่มีประสิทธิภาพ และลดความเสี่ยงจากการโจมตีในลักษณะนี้อย่างเป็นระบบ รวมถึงประชาชนควรมีความรู้พื้นฐานเกี่ยวกับรูปแบบการหลอกลวงและหมั่นสังเกตความผิดปกติของอุปกรณ์อย่างสม่ำเสมอ เพื่อป้องกันการตกเป็นเหยื่อโดยไม่รู้ตัว

2. ผลกระทบของการถูกควบคุมเครื่อง

การควบคุมอุปกรณ์ของเหยื่อสามารถนำไปสู่การขโมยตัวตนดิจิทัล (digital identity theft) ซึ่งสามารถส่งผลกระทบอย่างรุนแรงทั้งต่อตัวเหยื่อเองและผู้ที่เกี่ยวข้อง โดยเฉพาะเมื่ออุปกรณ์นั้นเป็นช่องทางหลักในการยืนยันตัวตนเพื่อเข้าถึงบริการดิจิทัลต่าง ๆ

- **ผลกระทบโดยตรงต่อเหยื่อ:** เมื่ออุปกรณ์ของเหยื่อถูกควบคุมโดยผู้ไม่หวังดี ผู้ไม่หวังดีสามารถใช้สิทธิ์และข้อมูลในอุปกรณ์นั้นในการยืนยันตัวตนแทนเจ้าของที่แท้จริงได้ เพื่อทำธุรกรรมทางอิเล็กทรอนิกส์ต่าง ๆ เช่น การทำธุรกรรมทางการเงิน หรือการควบคุมบัญชี social media การโจมตีในลักษณะนี้ส่งผลให้เหยื่อสูญเสียความเป็นส่วนตัวและทรัพย์สินทางการเงิน และอาจเผชิญกับผลกระทบทางกฎหมายหรือการสูญเสียชื่อเสียงได้
- **การขยายผลไปยังผู้ที่อยู่รอบตัวของเหยื่อ:** เมื่อผู้ไม่หวังดีสามารถควบคุมอุปกรณ์และ digital ID ของเหยื่อได้แล้ว ผู้ไม่หวังดีสามารถขยายขอบเขตการโจมตีไปยังบุคคลอื่นในเครือข่ายของเหยื่อ เช่น บุคคลในรายชื่อติดต่อหรือเพื่อนใน social media โดยผู้ไม่หวังดีสามารถใช้ข้อมูลที่ได้จากอุปกรณ์เพื่อดำเนินการหลอกลวงเพิ่มเติม เช่น การส่งลิงก์ปลอม การแอบอ้างตัวตน หรือการแพร่กระจาย malware การขยายผลในลักษณะนี้สามารถสร้างความเสียหายในวงกว้าง และเพิ่มความซับซ้อนในการตรวจสอบและควบคุมความเสียหาย เนื่องจากการโจมตีไม่ได้จำกัดอยู่แค่เหยื่อรายแรก แต่ยังแพร่กระจายไปยังผู้ที่เกี่ยวข้องกับเหยื่อผ่านช่องทางการสื่อสารที่เชื่อมโยงกัน

3. ประเภทของการโจมตีที่เกี่ยวข้องกับการควบคุมเครื่องเหยื่อ

ในยุคปัจจุบันที่สมาร์ตโฟนเป็นส่วนหนึ่งของการใช้ชีวิตและการทำธุรกรรมต่าง ๆ ทำให้สมาร์ตโฟนเป็นเป้าหมายหลักในการขโมยตัวตนดิจิทัล [1] ซึ่งมีหลากหลายเทคนิคและวิธีการที่มักถูกนำมาใช้ในการควบคุมอุปกรณ์ของเหยื่อ ทั้งในเชิงจิตวิทยาและเชิงเทคนิค ดังนี้

- **Social Engineering**: เป็นวิธีการทางจิตวิทยาในการหลอกลวงเหยื่อ เพื่อให้เหยื่อเปิดเผยข้อมูลที่เป็นความลับ หรือดำเนินการบางอย่างโดยสมัครใจ โดยวิธีการที่มักพบเจอได้บ่อย ได้แก่
    - **Phishing และ Smishing:** เป็นการส่งข้อความหลอกลวง ซึ่งมักส่งผ่านอีเมล (phishing) หรือ SMS (smishing) โดยมีลิงก์หรือไฟล์แนบที่ออกแบบมาเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น การส่งอีเมลปลอมเพื่อขอข้อมูลส่วนตัวของเหยื่อ หรือ SMS ที่มีเนื้อหาที่ชักชวนให้หลงเชื่อ เช่น การตกเป็นผู้ต้องสงสัยในคดีที่ปั้นแต่งขึ้นมาโดยผู้ไม่หวังดี
    - **Pretexting:** เป็นเทคนิคที่ผู้ไม่หวังดีสร้างสถานการณ์โดยการแอบอ้างเป็นบุคคลที่มีอำนาจหรือบุคคลที่มีสิทธิ์จะทราบข้อมูลที่เป็นความลับของเหยื่อ เช่น เจ้าหน้าที่สนับสนุนด้านไอที หรือเจ้าหน้าที่รัฐ เพื่อหลอกลวงให้เหยื่อยอมเปิดเผยข้อมูลที่ละเอียดอ่อน โดยผู้ไม่หวังดีมักใช้เทคนิคนี้ระหว่างการสนทนากับเหยื่อโดยตรงผ่านโทรศัพท์หรือ chat ในแอปพลิเคชันต่าง ๆ
- **Malware และ RAT (Remote Access Trojan)**: เป็นการโจมตีเชิงเทคนิค โดยใช้ซอฟต์แวร์หรือแอปพลิเคชันที่ออกแบบมาเพื่อทำอันตรายแก่อุปกรณ์ของเหยื่อโดยที่เหยื่อไม่รู้ตัว (malicious

software) เช่น การขโมยข้อมูลส่วนตัวหรือข้อมูลในแอปพลิเคชันธนาคาร (หมายเลขบัญชี เลขรหัสส่วนตัว (PIN) และข้อมูลบัตรเครดิต) และการเปิดช่องโหว่ให้ผู้ไม่หวังดีเข้ามาควบคุมอุปกรณ์ได้

หนึ่งใน malware ที่ถูกนำมาใช้เพื่อควบคุมอุปกรณ์ของเหยื่อคือ Remote Access Trojans (RAT) ซึ่งเป็น malware ประเภทโทรจัน (trojan) ที่ออกแบบมาให้ผู้ไม่หวังดีสามารถเข้าถึงและควบคุมเครื่องของเหยื่อได้โดยไม่ถูกตรวจพบ เนื่องจากถูกออกแบบมาให้ดูเหมือนแอปพลิเคชันทั่วไป เมื่อเหยื่อนำไปติดตั้งในอุปกรณ์ของตนจะทำให้ผู้ไม่หวังดีสามารถขโมยข้อมูลต่าง ๆ เช่น ข้อมูลแอปพลิเคชันที่ติดตั้งในอุปกรณ์, ประวัติการโทร, รายชื่อติดต่อ, ประวัติการท่องเว็บ และ SMS นอกจากนี้ RAT ยังสามารถควบคุมการทำงานต่าง ๆ ของอุปกรณ์ เช่น การส่ง SMS, เปิดใช้งานกล้อง บันทึกข้อมูล GPS รวมถึงดำเนินการคำสั่งที่เป็นอันตรายต่าง ๆ [4] ตัวอย่างของ RAT เช่น ResolverRAT เป็น RAT ที่ดำเนินการในหน่วยความจำของอุปกรณ์เพื่อขโมยข้อมูล รวมถึงสามารถแก้ไขการจัดการทรัพยากรของอุปกรณ์เพื่อหลีกเลี่ยงการตรวจจับได้ [5]

- **Sideload Application**: เป็นการโจมตีเชิงผสมผสานระหว่างวิธีการทางเทคนิคและจิตวิทยา โดยผู้ไม่หวังดีจะสร้างแอปพลิเคชันปลอมที่แฝงด้วย malware หรือมีการออกแบบมาเพื่อขโมยข้อมูลและควบคุมอุปกรณ์ของเหยื่อ จากนั้นผู้ไม่หวังดีจะหลอกล่อให้เหยื่อติดตั้งแอปพลิเคชันปลอมนี้

  ข้อสังเกตคือ sideload application มักจะมาจาก application marketplace ที่ไม่เป็นทางการ ซึ่งมักไม่ผ่านกระบวนการตรวจสอบความปลอดภัย ทำให้มีความเสี่ยงสูงว่าจะมี malware แฝงอยู่ เช่น TeaBot และ Flubot ซึ่งสามารถอ่านข้อความ, ขโมยรหัสผ่าน และควบคุมอุปกรณ์ของเหยื่อได้ [8] โดยส่วนใหญ่ เหยื่อมักจะพลาดไปโหลดแอปพลิเคชันเหล่านี้จากการคลิกลิงก์ phishing หรือการดาวน์โหลดจากเว็บไซต์ที่ไม่น่าเชื่อถือ

- **Accessibility Service Abuse:** เป็นการโจมตีเชิงเทคนิคโดยอาศัยการใช้สิทธิ์ที่ออกแบบมาเพื่อช่วยผู้พิการในการควบคุมอุปกรณ์ที่ใช้ระบบปฏิบัติการ Android โดยผู้ไม่หวังดีสามารถใช้สิทธิ์นี้ในการขโมยข้อมูลต่าง ๆ จากเหยื่อ เช่น การดักจับ SMS รหัสผ่าน ข้อมูลส่วนตัว อ่านข้อมูลที่ละเอียดอ่อน และกดยืนยันการทำธุรกรรม [2] ตัวอย่างของ malware ที่โจมตีผ่าน accessibility service เช่น AntiDot ซึ่งสามารถบันทึกหน้าจอของอุปกรณ์และดักจับข้อความ SMS ได้ [6] และ MMRat ซึ่งสามารถควบคุมอุปกรณ์ของเหยื่อจากระยะไกลเพื่อทำธุรกรรมทางการเงิน [7]

- **Screen Overlay**: เป็นการโจมตีเชิงเทคนิคที่ผู้ไม่หวังดีสร้างหน้าจอปลอมมาซ้อนทับหน้าจอของแอปพลิเคชันจริง เพื่อหลอกลวงเหยื่อให้ป้อนข้อมูลที่ละเอียดอ่อน และทำการขโมยข้อมูลนั้น เช่น ข้อมูลในแอปพลิเคชันด้านการเงิน หรือแม้แต่การหลอกให้เหยื่อกดปุ่มเพื่อมอบสิทธิ์ในการควบคุมอุปกรณ์เพิ่มเติม Godfather เป็นตัวอย่างหนึ่งของ malware ที่ใช้การโจมตีแบบ overlay เพื่อขโมยข้อมูลประจำตัว [9]

4. ขั้นตอนการควบคุมเครื่องเหยื่อ

จากการศึกษาโดย TB-CERT [3] เรื่องพฤติกรรมและขั้นตอนของผู้ไม่หวังดี ในการหลอกล่อเหยื่อเพื่อขโมยข้อมูลและเข้าควบคุมอุปกรณ์ ผู้ไม่หวังดีมักจะเริ่มจากการแอบอ้างเป็นเจ้าหน้าที่หน่วยงานของรัฐ หรือ

พนักงานของหน่วยงานผู้ให้บริการต่าง ๆ แล้วจึงปั้นแต่งเรื่อง สร้างสถานการณ์ที่น่าเชื่อถือ ร่วมกับใช้วิธีการต่าง ๆ เพื่อหลอกล่อให้เหยื่อหลงเชื่อและยอมทำตามสิ่งที่ผู้ไม่หวังดีหลอกให้ทำ เช่น การขอข้อมูลส่วนตัว ข้อมูลธุรกรรมทางการเงิน และรหัสผ่าน จากนั้นจึงหลอกให้เหยื่อติดตั้งแอปพลิเคชั่นปลอมที่ขอสิทธิ์ในการเข้าถึง accessibility service ของระบบปฏิบัติการ เมื่อเหยื่อทำตามขั้นตอนที่ผู้ไม่หวังดีได้กำหนดไว้ ผู้ไม่หวังดีจะสามารถควบคุมอุปกรณ์ของเหยื่อ และทำธุรกรรมผิดกฎหมายต่าง ๆ ได้ เช่น การโอนเงิน การขโมยบัญชี social media และการขโมยข้อมูลผู้ติดต่อของเหยื่อ

ในปัจจุบัน รูปแบบการควบคุมอุปกรณ์ของเหยื่อ สามารถแบ่งออกเป็น 2 รูปแบบ คือ การหลอกล่อเหยื่อแล้วควบคุมอุปกรณ์ทันที และ การหลอกล่อเหยื่อแล้วควบคุมอุปกรณ์ในภายหลัง

- **ขั้นตอนของผู้ไม่หวังดี ในการการหลอกล่อเหยื่อแล้วควบคุมอุปกรณ์ทันที**
    1. หลอกล่อเหยื่อให้หลงเชื่อในสถานการณ์ที่สร้างขึ้น
    2. ชักชวนเหยื่อให้ Chat ต่อใน LINE (หรือแอปพลิเคชันอื่น ๆ ที่ใช้รับส่งข้อความได้) เพื่อให้สามารถส่งลิงก์ดาวน์โหลดแอปพลิเคชันปลอมได้
    3. หลอกล่อเหยื่อให้ยอมติดตั้งแอปพลิเคชันปลอม
    4. หลอกให้เหยื่อตั้งรหัสผ่านหลายครั้ง โดยไม่ซ้ำกัน เพื่อหวังว่าเหยื่อจะใช้รหัสผ่านเดียวกันกับที่ใช้ในแอปพลิเคชันอื่น ๆ
    5. แอปพลิเคชันปลอมจะขอสิทธิ์ในการควบคุมอุปกรณ์ผ่าน accessibility service
    6. แอปพลิเคชันแสดง screen overlay และทำให้หน้าจออุปกรณ์ค้าง เพื่อไม่ให้เหยื่อมองเห็นว่าอุปกรณ์กำลังถูกควบคุมอยู่
- **ขั้นตอนของผู้ไม่หวังดี ในการการหลอกล่อเหยื่อแล้วควบคุมอุปกรณ์ในภายหลัง**
    1. หลอกล่อเหยื่อให้หลงเชื่อในสถานการณ์ที่สร้างขึ้น
    2. ชักชวนเหยื่อให้ Chat ต่อใน LINE (หรือแอปพลิเคชันอื่น ๆ ที่ใช้รับส่งข้อความได้) เพื่อให้สามารถส่งลิงก์ดาวน์โหลดแอปพลิเคชันปลอมได้
    3. หลอกล่อเหยื่อให้ยอมติดตั้งแอปพลิเคชันปลอม
    4. แอปพลิเคชันปลอมจะขอสิทธิ์ในการควบคุมอุปกรณ์ผ่าน accessibility service
    5. แอปพลิเคชันปลอมจะแจ้งเหยื่อว่าติดตั้งไม่สำเร็จ เพื่อให้เหยื่อตายใจ แต่ที่จริงแล้วแอปพลิเคชันปลอมติดตั้งสำเร็จ แต่ไม่แสดงให้เหยื่อเห็นโดยง่าย
    6. แอปพลิเคชันเปิดช่องทางลับให้ผู้ไม่หวังดีแอบขโมยข้อมูลของเหยื่อ หรือเข้ามาควบคุมอุปกรณ์ในภายหลัง

5. ตัวอย่างเหตุการณ์จริง

กรณีศึกษาในรายงานของ TB-CERT และการสัมภาษณ์ผู้เชี่ยวชาญ เปิดเผยว่าในช่วงการยื่นแบบแสดงรายการภาษีเงินได้บุคคลธรรมดาและการขอคืนภาษี ผู้ไม่หวังดีมักจะใช้โอกาสนี้ในการแอบอ้างเป็นเจ้าหน้าที่ของกรมสรรพากร แล้วหลอกลวงเหยื่อด้วยวิธีการต่าง ๆ เพื่อขโมยข้อมูลส่วนตัว หรือเปิดช่องทางให้ผู้ไม่หวังดีสามารถเข้ามาควบคุมอุปกรณ์ของเหยื่อได้ โดยมีรูปแบบที่ผู้ไม่หวังดีมักนำมาใช้ ดังนี้ [10]

- ใช้เบอร์โทรศัพท์ของกรมสรรพากรในการส่ง SMS เพื่อหลอกเอาเงินจากเหยื่อ
- ใช้บัญชี LINE ปลอม โดยใช้รูปผู้บริหารกรมสรรพากรเป็นภาพประจำตัว เพื่อหลอกเหยื่อให้หลงเชื่อและกดลิงก์ที่ผู้ไม่หวังดีส่งมาให้
- ส่ง Email ปลอม อ้างเป็นฝ่ายสนับสนุนลูกค้าของกรมสรรพากรหลอกให้เหยื่อกดลิงก์ เพื่อรับสิทธิประโยชน์ e-Tax
- ส่งข้อความผ่านทาง SMS หรือ Email โดยแอบอ้างเป็นกรมสรรพากร หลอกให้เหยื่อกดลิงก์ เพื่อดำเนินการต่างๆ เช่น การส่งเอกสารเพิ่มเติม การยืนยันสิทธิขอคืนภาษี หรือการให้ข้อมูลส่วนบุคคล
- โทรศัพท์ติดต่อเหยื่อโดยตรง เพื่อแจ้งการได้รับสิทธิในการขอคืนภาษี และหลอกให้ดำเนินการธุรกรรมต่างๆ ผ่านตู้ ATM ตามขั้นตอนที่ผู้ไม่หวังดีวางแผนไว้

6. สัญญาณเตือนความเสี่ยงว่ากำลังถูกควบคุมเครื่อง

อุปกรณ์ที่ถูกควบคุมมักจะแสดงสัญญาณผิดปกติซึ่งเจ้าของอุปกรณ์สามารถสังเกตอาการเหล่านี้เองได้เพื่อลดความเสี่ยงและความเสียหายจากการถูกควบคุมอุปกรณ์ [11]

- มีแอปพลิเคชันที่ไม่รู้จักกำลังขอใช้สิทธิ์ accessibility service
- หน้าจออุปกรณ์ค้างหรือมีการซ้อนทับโดยแอปพลิเคชันที่ไม่รู้จัก
- แอปพลิเคชันธนาคารทำงานผิดปกติ เช่น เปิดแล้วปิดทันที หรือแสดงพฤติกรรมไม่คาดคิด
- มีการโอนเงินหรือธุรกรรมที่ไม่ได้ทำเองเกิดขึ้น
- แบตเตอรี่หมดเร็วกว่าปกติ หรือมีการใช้งานข้อมูลอินเทอร์เน็ตที่ผิดปกติ
- สมาร์ตโฟนร้อนผิดปกติแม้ไม่ได้ใช้งานหนัก

7. สรุป

การควบคุมเครื่องเหยื่อเป็นหนึ่งในภัยคุกคามที่ร้ายแรงต่อ Digital ID ซึ่งทำให้ผู้ไม่หวังดีสามารถสวมรอยเป็นเหยื่อและเข้าถึงบริการต่าง ๆ ได้ วิธีที่ใช้มักเกี่ยวข้องกับ social engineering และเทคนิคต่าง ๆ เช่น accessibility service abuse, screen overlay, การหลอกให้ติดตั้งแอปพลิเคชันจาก application marketplace ที่ไม่เป็นทางการ และ malware ซึ่งล้วนออกแบบมาเพื่อเข้าควบคุมอุปกรณ์และขโมยข้อมูลส่วนตัว ตลอดจนข้อมูลการเงินของเหยื่อ

ผลกระทบของการโจมตีลักษณะนี้ครอบคลุมทั้งระดับบุคคล ระบบดิจิทัล และเศรษฐกิจ เช่น การแอบอ้างตัวตน การฉ้อโกงทางการเงิน และการขยายการโจมตีไปยังผู้ที่เกี่ยวข้องกับเหยื่อ กรณีศึกษาในไทยพบว่าผู้ไม่หวังดีมักจะแอบอ้างเป็นหน่วยงานรัฐเพื่อหลอกล่อเหยื่อให้ติดตั้งแอปพลิเคชันปลอม ซึ่งส่งผลไปสู่การขโมยข้อมูลส่วนตัว ข้อมูลทางการเงิน และถูกควบคุมอุปกรณ์ในที่สุด

อ้างอิง

[1] “How Thailand’s banks are using biometric tech to fight cybercrime”, FinTech Global. Accessed: Jun. 24, 2025. [Online]. Available: https://fintech.global/2025/03/26/how-thailands-banks-are-using-biometric-tech-to-fight-cybercrime/

[2] “How to Detect Accessibility Service Abuse on Android Apps Using AI”, Appdome. Accessed: Jun. 24, 2025. [Online]. Available: https://www.appdome.com/how-to/account-takeover-prevention/android-and-ios-trojans/detect-malware-privilege-escalation-to-accessibilityservice/

[3] “กลโกงมิจฉาชีพ หลอกติดตั้งแอปพลิชันดูดเงิน และการยกระดับมาตรการป้องกันร่วมกับหน่วยงานต่าง ๆ”, Thailand Banking Secter CERT. Accessed: Jun. 24, 2025. [Online]. Available: https://www.tba.or.th/wp-content/uploads/pdf/TB-Cert_Presentation_16.10_ForPress_blur.pdf

[4] “What is Mobile Malware?”, Palo Alto Networks. Accessed: Jun. 24, 2025. [Online]. Available: https://www.paloaltonetworks.co.uk/cyberpedia/what-is-mobile-malware

[5] A. Ribeiro, “ResolverRAT malware attacks pharma and healthcare organizations via phishing and DLL side-loading”, Industrial Cyber. Accessed: Jun. 24, 2025. [Online]. Available: https://industrialcyber.co/ransomware/resolverrat-malware-attacks-pharma-and-healthcare-organizations-via-phishing-and-dll-side-loading/

[6] The Hacker News, “New Android Malware Surge Hits Devices via Overlays, Virtualization Fraud, and NFC Theft”, The Hacker News. Accessed: Jun. 24, 2025. [Online]. Available: https://thehackernews.com/2025/06/new-android-malware-surge-hits-devices.html

[7] The Hacker News, “MMRat Android Trojan Executes Remote Financial Fraud Through Accessibility Feature”, The Hacker News. Accessed: Jun. 24, 2025. [Online]. Available: https://thehackernews.com/2023/08/mmrat-android-trojan-executes-remote.html

[8] D. S. Expert, “The Risks of Sideloading Apps: Why It’s a Bad Idea”, Device Safety. Accessed: Jun. 24, 2025. [Online]. Available: https://devicesafety.org/the-risks-of-sideloading-apps-why-its-a-bad-idea/

[9] “In-depth analysis of overlay attacks and prevention strategies”, Group-IB, Accessed: Jun. 24, 2025. [Online]. Available: https://www.group-ib.com/resources/knowledge-hub/overlay-attacks/

[10] “กรมสรรพากรเตือนภัยมิจฉาชีพแอบอ้างชื่อหลอกลวงผ่าน SMS อีเมล LINE และโทรศัพท์”, ผู้จัดการออนไลน์. Accessed: Jun. 24, 2025. [Online]. Available: https://mgronline.com/stockmarket/detail/9680000025641

[11] “สมาคมธนาคารไทยเผยยอดความเสียหายแอปดูดเงิน 500 ล้าน ผนึกหน่วยงานรัฐ-เอกชนยกระดับมาตรการป้องกัน”, สมาคมธนาคารไทย. Accessed: Jun. 24, 2025. [Online]. Available: https://www.tba.or.th/%E0%B8%AA%E0%B8%A1%E0%B8%B2%E0%B8%84%E0%B8%A1%E0%B8%98%E0%B8%99%E0%B8%B2%E0%B8%84%E0%B8%B2%E0%B8%A3%E0%B9%84%E0%B8%97%E0%B8%A2%E0%B9%80%E0%B8%9C%E0%B8%A2%E0%B8%A2%E0%B8%AD%E0%B8%94%E0%B8%84%E0%B8%A7/