เรื่อง Juice Jacking ชาร์จแบตโทรศัพท์มือถือผิดที่ อาจสูญข้อมูล
ทดสอบและเรียบเรียงโดย กิติศักดิ์ จิรวรรณกูล และ ปณิธาน เขินอำนวย
เรียบเรียงวันที่ 21 มิถุนายน 2559

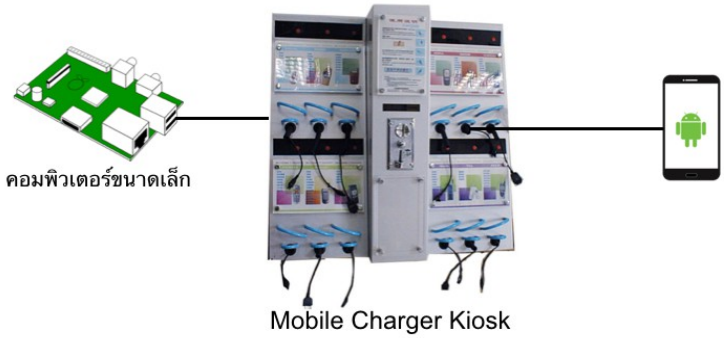
ปัจจุบันปัญหาหนึ่งของผู้ใช้งานโทรศัพท์มือถือ สมาร์ทโฟน คือแบตเตอรี่หมดอย่างรวดเร็ว ผู้ใช้จึงต้องหาแหล่งพลังงานเพื่อชาร์จแบตเตอรี่ และมีผู้ให้บริการชาร์จแบตเตอรี่เพิ่มขึ้นอย่างมาก ซึ่งมีบริการทั้งแบบฟรีและเสียเงิน เมื่อเหยื่อมาหลงใช้บริการ อาจส่งผลทำให้ถูกขโมยข้อมูลได้ เทคนิคนี้เรียกว่า Juice Jacking

ลักษณะการโจมตี

เทคนิค Juice Jacking นี้เริ่มต้นเมื่อปี 2554 ในงานสัมนา DefCon ที่ลาสเวกัส Brain Krebs ได้นำเสนอการทดลองเทคนิคการโจมตีด้วยวิธีนี้ โดยติดตั้งเครื่องให้บริการชาร์จโทรศัพท์มือถือสาธารณะ แต่เบื้องหลังของเครื่องนี้ได้ติดตั้งคอมพิวเตอร์ขนาดเล็กสำหรับดักเก็บข้อมูลของโทรศัพท์ที่ถูกนำมาต่อเพื่อชาร์จแบตเตอรี่ ดังภาพที่ 1

ภาพที่ 1 ผลงานนำเสนอ Juice Jacking ของ Brain Krebs

แต่เนื่องด้วยเทคโนโลยีคอมพิวเตอร์มีขนาดเล็กลง จนมีขนาดใกล้เคียงกับแผงวงจรขนาดเล็ก ทำให้การซ่อนคอมพิวเตอร์นี้ในตู้ให้บริการชาร์จแบตเตอรี่ของโทรศัพท์นี้ยากต่อการตรวจพบ จากนั้นผู้ประสงค์ร้ายเชิญชวนให้เหยื่อมาใช้บริการชาร์จ แล้วเครื่องคอมพิวเตอร์ขนาดเล็กนี้จะทำหน้าที่ดึงข้อมูลของโทรศัพท์หรือแพร่กระจายมัลแวร์ให้แก่โทรศัพท์ที่ถูกนำมาชาร์จได้ ดังภาพที่ 2



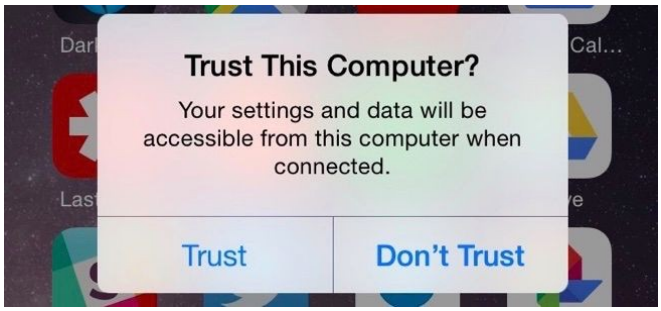
ภาพที่ 2 แสดงลักษณะของการทำงานแบบ Juice Jacking

ผลกระทบที่อาจเกิดขึ้น

1. ถูกขโมยข้อมูล เมื่อเชื่อมต่อโทรศัพท์มือถือเข้ากับคอมพิวเตอร์ จะเห็นข้อมูลที่อยู่ภายในโทรศัพท์ ดังนั้นผู้ประสงค์ร้ายสามารถพัฒนาโปรแกรมในการคัดลอกข้อมูลจากโทรศัพท์ได้อย่างอัตโนมัติได้
2. ถูกฝังมัลแวร์มารันในเครื่อง การเชื่อมต่อโทรศัพท์มือถือเข้ากับคอมพิวเตอร์นี้ ผู้ประสงค์ร้ายสามารถคัดลอกมัลแวร์ไปฝังไว้ในเครื่อง และสั่งให้รันได้ โดยที่เหยื่อไม่รู้ตัว
3. โทรศัพท์อาจได้รับความเสียหาย เนื่องจากภัยนี้มีความเกี่ยวข้องกับแบตเตอรี่ ซึ่งอาจจะส่งผลกระทบต่อการชาร์จและคลายประจุที่บางครั้งอาจจะมากหรือน้อยเกินไป หรืออาจจะไม่สม่ำเสมอ จนส่งผลทำให้เครื่องโทรศัพท์เกิดความเสียหายทางกายภาพได้

วิธีการป้องกัน

1. ห้ามชาร์จจากแหล่งจ่ายไฟที่ไม่น่าเชื่อถือ เช่น ไม่เห็นหัวแปลงไฟ หรือไม่สามารถระบุอุปกรณ์ที่จ่ายไฟ
2. หากจำเป็นต้องชาร์จ ให้เลือกชาร์จจากแบตเตอรี่สำรองหรือรถยนต์แทน
3. เปิดโหมด Charge only สำหรับโทรศัพท์แอนดรอยด์ เมื่อเชื่อมต่อคอมพิวเตอร์และโทรศัพท์ผ่าน USB
4. ห้ามกด Trust เมื่อปรากฏหน้าไดอะล็อก Trust This Computer? ดังภาพที่ 3 สำหรับโทรศัพท์ไอโฟน เมื่อเชื่อมต่อคอมพิวเตอร์และโทรศัพท์ผ่าน USB



ภาพที่ 3 หน้าไดอะล็อก Trust This Computer?

สรุป

ภัยคุกคามนี้เป็นภัยคุกคามที่อาจจะไม่ได้สร้างความเสียหายมากในวงกว้าง แต่มีความเสียหายต่อการละเมิดข้อมูลส่วนบุคคลอย่างมาก นอกจากนี้ยังผู้ใช้งานอาจจะไม่สามารถรู้ว่าตนเองได้ถูกขโมยข้อมูลส่วนตัวไปเรียบร้อยแล้ว หากเชื่อถือเครื่องให้บริการชาร์จโทรศัพท์มือถือสาธารณะ ดังนั้นเพื่อป้องกันไม่ให้ตกเป็นเหยื่อของภัยคุกคามนี้จำเป็นต้องสังเกตและปฏิบัติตามคำแนะนำข้างต้นด้วย อนึ่งสามารถดูตัวอย่างการใช้ภัยคุกคามนี้ในการโจรกรรมข้อมูลจากภาพยนต์เรื่อง CSI: Cyber. Season 1: Episode 9 ตอน "L0M1S"

เอกสารอ้างอิง

1. https://en.wikipedia.org/wiki/Juice_jacking
2. http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/
3. http://gizmodo.com/csi-cyber-and-the-juice-jacking-airplane-wi-fi-white-wh-1701339838