ถอดรหัส กลโกง BIN Attack

เผยแพร่วันที่ 9 พฤศจิกายน 2564

ในขณะที่รูปแบบการชำระเงินได้มีการเปลี่ยนแปลงไปสู่การชำระเงินทางอิเล็กทรอนิกส์ หรือ Electronic Payment มากขึ้น และการชำระเงินด้วยบัตรเครดิตและบัตรเดบิตก็มีอัตราการใช้งานบนโลกออนไลน์ที่เพิ่มสูงขึ้น เพื่อให้เกิดความตระหนักในการใช้งานบัตรเครดิตและบัตรเดบิตอย่างปลอดภัย บทความนี้จะมาอธิบาย BIN Attack คืออะไร ลักษณะการทำงานเป็นอย่างไร และเราจะป้องกันกลโกง BIN Attack นี้ได้อย่างไร

BIN Attack คืออะไร ก่อนอื่นเรามาทำความเข้าใจประเภทบัตรเครดิตและบัตรเดบิตกันก่อน

บัตรเครดิต คือ บัตรแทนเงินสดอิเล็กทรอนิกส์รูปแบบหนึ่ง ซึ่งสามารถใช้ในการรูดซื้อสินค้าหรือบริการแทนเงินสด และลูกค้าต้องทำการชำระคืนธนาคารในภายหลัง

บัตรเดบิต คือ บัตรแทนเงินสดอิเล็กทรอนิกส์อีกรูปแบบ สามารถนำมาใช้รูดซื้อสินค้าและบริการได้เช่นกัน สิ่งที่แตกต่างจากบัตรเครดิต คือ วงเงินที่ใช้จ่ายในบัตรเดบิตจะ**ถูกหักจากบัญชีธนาคารทันที**เหมือนการใช้เงินสด และบัตรเดบิตนี้สามารถใช้งานบนตู้ถอนเงินสด หรือตู้ ATM ได้ด้วยไม่ว่าจะเป็นการถอนเงิน โอนเงิน สอบถามยอดจากบัญชีธนาคาร เป็นต้น ดังนั้นหลายธนาคารจึงได้ให้บริการบัตรเดบิตเป็นบัตรใบเดียวกับบัตรเอทีเอ็ม

บัตรแต่ละประเภท ต่างกันยังไง?	ถอนเงินที่ตู้ ถอนเงินสด	รูดซื้อสินค้า และบริการ	ตัดเงินจากบัญชี เงินฝากทันที
บัตรเอทีเอ็ม	✓	✗	✓
บัตรเดบิต	✓	✓	✓
บัตรเครดิต	✓	✓	✗

รูปที่ 1 แสดงตารางความแตกต่างของบัตรแต่ละประเภท

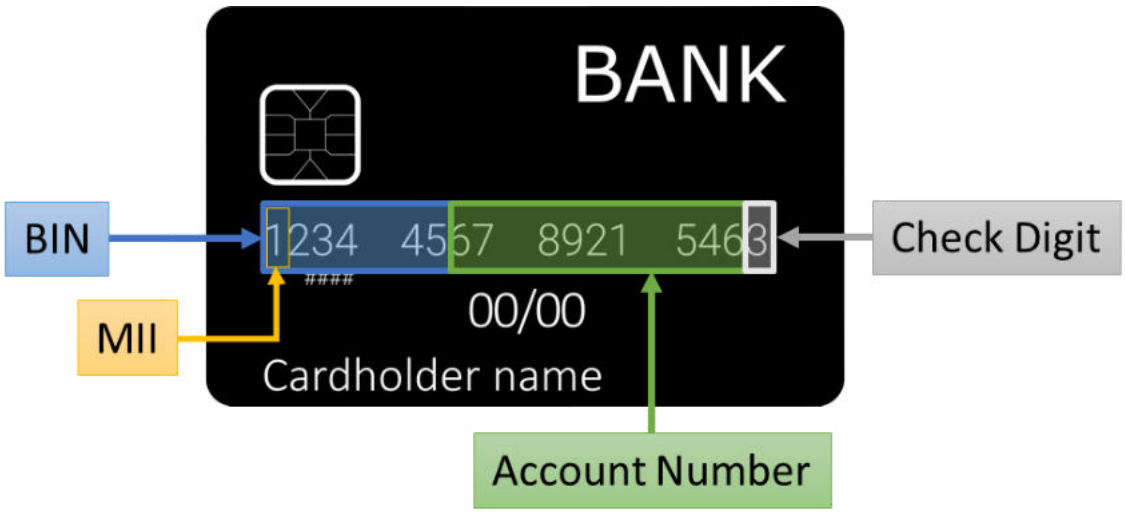
(ที่มา https://www.bot.or.th/Thai/PaymentSystems/Publication/payment_insight/Documents/Bi-monthly_report_Vol4-2020_August.pdf)

การรูดซื้อสินค้าและบริการของบัตรเครดิตและบัตรเดบิตในที่นี้ หมายรวมถึงการใช้บัตรซื้อสินค้าและบริการผ่านช่องทางเครื่องชำระเงิน EDC (Electronic Data Capture) ซึ่งการใช้บัตรผ่านช่องทาง EDC นี้จะต้องแสดงบัตรและต้องมีการรูดบัตรที่ร้านค้า ในขณะที่การใช้บัตรชำระเงินผ่านช่องทางออนไลน์ เป็น

ช่องทางที่ได้รับความนิยมเพิ่มขึ้นตามอัตราการใช้งานบนโลกออนไลน์ที่เพิ่มสูงขึ้น โดยการใช้บัตรในช่องทางออนไลน์นี้ไม่สามารถแสดงตัวบัตรให้กับร้านค้าเพื่อรูดบัตรได้หรือเรียกว่าธุรกรรมแบบ Card Not Present ทางผู้ให้บริการบัตรเครดิตและบัตรเดบิตรายใหญ่เช่น VISA MasterCard American Express จึงพัฒนาเทคโนโลยี 3D Secure (อ้างอิง AW21-06_3D Secure_v1.0_released (tba.or.th) เพื่อยกระดับความปลอดภัยในการใช้บัตรช่องทางออนไลน์ โดยผู้ให้บริการบัตรเครดิตและบัตรเดบิตพยายามผลักดันให้ร้านค้าออนไลน์หันมาใช้เทคโนโลยี 3D Secure กันให้มากขึ้น แต่ยังคงมีกลุ่มร้านค้าที่ขายสินค้ามูลค่าไม่สูงมากจะยังไม่ได้ใช้เทคโนโลยี 3D Secure นี้

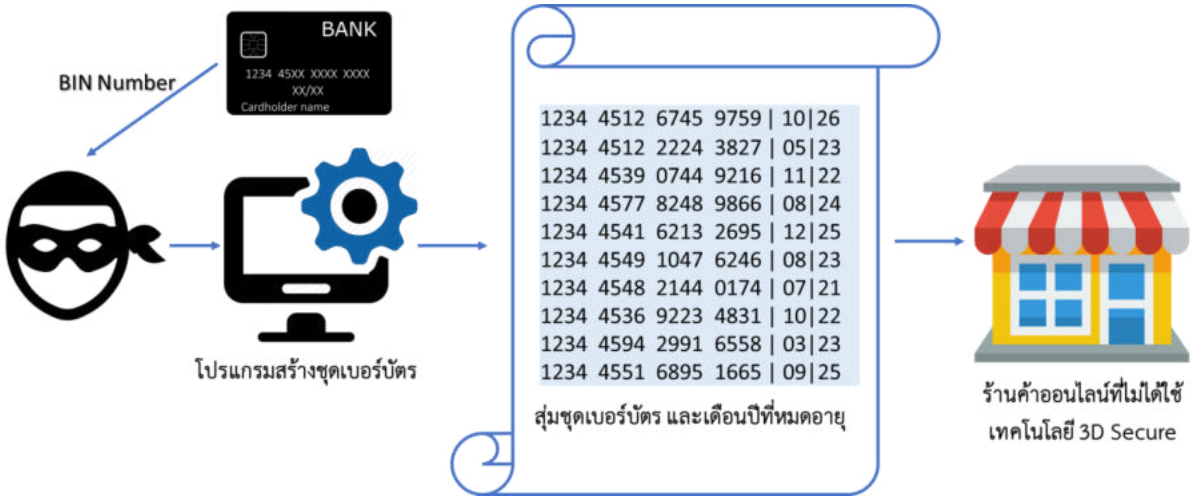
สำหรับข้อมูลบนหน้าบัตรเครดิตและบัตรเดบิตจะมีลักษณะคล้ายกัน โดยข้อมูลบนหน้าบัตรนั้นจะประกอบด้วย ชื่อธนาคารผู้ออกบัตร, ชื่อผู้ใช้งาน, เบอร์บัตร และเดือนปีที่บัตรหมดอายุ โดยแต่ละตำแหน่งของตัวเลขบนเบอร์บัตรจะระบุถึงข้อมูลดังนี้

- ตัวเลขตำแหน่งที่ 1 คือ MII ย่อมาจาก Major Industry Identifier ระบุประเภทของอุตสาหกรรมที่ออกบัตร เช่น เลข 4 and 5 หมายถึง อุตสาหกรรมประเภท Banking and Financial Services
- ตัวเลขตำแหน่งที่ 1-6 คือ BIN ย่อมาจาก Bank Identification Number หรือ IIN ย่อมาจาก Issuer Identification Number ระบุหมายเลขประจำตัวผู้ออกบัตร หรือหมายเลขประจำตัวธนาคารผู้ออกบัตร
- ตัวเลขตำแหน่งที่ 7-15 คือ Account Number ระบุหมายเลขบัญชีลูกค้า
- ตัวเลขตำแหน่งที่ 16 ตำแหน่งสุดท้าย คือ Check Digit ระบุค่าตรวจสอบตัวเลข สำหรับตรวจสอบความถูกต้องของชุดข้อมูลเบอร์บัตรตำแหน่งที่ 1-15



รูปที่ 2 แสดงโครงสร้างเบอร์บัตร

ดังนั้นในชุดข้อมูลเบอร์บัตรนี้ ชุดตัวเลขที่ระบุจำเพาะไปยังหมายเลขที่ใช้เชื่อมโยงถึงบัญชีลูกค้า จะเริ่มจากตำแหน่งที่ 7 จนถึงตำแหน่งที่ 15 สำหรับกลโกงประเภท BIN Attack ก็คือ การโกงด้วยวิธีการใช้ข้อมูล BIN เป็นค่าตั้งต้น แล้วใช้โปรแกรมสร้างชุดตัวเลขที่เหลือ ได้แก่ หมายเลขบัญชีลูกค้า และค่าตรวจสอบ Check digit หลักสุดท้ายให้ถูกต้อง เมื่อได้ชุดตัวเลขครบทั้ง 16 หลักแล้ว โจรจะนำชุดตัวเลข 16 หลักนี้ พร้อมกับการสุ่มเดือนปีที่หมดอายุของบัตรไปลองใช้กับกลุ่มร้านค้าออนไลน์ที่ขาดความระมัดระวังด้านความปลอดภัยในการพัฒนาระบบ เพื่อตรวจสอบว่าเบอร์บัตร 16 หลักนั้นถูกต้องหรือไม่ เมื่อโจรสุ่มข้อมูลจนทราบเบอร์บัตร 16 หลักที่ถูกต้องแล้ว จากนั้นโจรก็จะเดาสุ่มเดือนปีที่หมดอายุของบัตร โดยปกติเดือนปีที่หมดอายุของบัตรจะถูกกำหนดไว้สูงสุดไม่เกิน 5 ปี และเบอร์บัตรที่มีชุดตัวเลขใกล้กันจะมีเดือนปีที่หมดอายุของบัตรเป็นเดือนและปีเดียวกัน ดังนั้นหากโจรรู้เบอร์บัตร 16 หลัก และเดือนปีที่หมดอายุของบัตรสักหนึ่งใบ สำหรับเบอร์บัตรที่มีชุดตัวเลขใกล้กัน จึงมีความเป็นไปได้ที่จะมีเดือนปีที่หมดอายุของบัตรเป็นเดือนปีเดียวกัน ทำให้สามารถเดาเดือนปีที่หมดอายุของบัตรได้ไม่ยาก โดยข้อมูลบัตรเหล่านี้จะถูกส่งด้วยคำสั่งซื้อที่มีมูลค่าต่ำ เพื่อหลบการตรวจจับจากระบบเฝ้าระวังความผิดปกติของธนาคาร สุดท้ายเมื่อโจรสุ่มได้ข้อมูลบัตรที่ถูกต้องครบถ้วนได้แก่ เบอร์บัตร 16 หลัก และเดือนปีที่บัตรหมดอายุ โจรก็จะนำชุดข้อมูลนี้ไปทำรายการซื้อสินค้าและบริการที่ต้องการ เสมือนเป็นการทำรายการจากเจ้าของบัตรจริง กับร้านค้าออนไลน์ที่ไม่ได้ใช้เทคโนโลยี 3D Secure หรือร้านค้าออนไลน์ที่ไม่มีขั้นตอนการยืนยันตัวตนจากลูกค้าเจ้าของบัตรอีกครั้ง หรือไม่มีการใช้รหัสผ่าน OTP ในการทำรายการชำระเงิน



รูปที่ 3 แสดงขั้นตอน กลโกง BIN Attack

ข้อสังเกตลักษณะของเหตุการณ์ BIN Attack สำหรับร้านค้าออนไลน์และธนาคารผู้ให้บริการบัตรเครดิตและบัตรเดบิต

1. มีธุรกรรมมูลค่าต่ำเกิดขึ้นติดต่อกันจำนวนมากในช่วงระยะเวลาหนึ่ง และมีรายการถูกปฏิเสธเกิดขึ้นจำนวนมากในช่วงเวลาเดียวกัน โดยธุรกรรมเหล่านี้จะมาจากร้านค้าออนไลน์ที่ไม่ได้ใช้เทคโนโลยี 3D Secure หรือร้านค้าออนไลน์ที่ไม่มีขั้นตอนการยืนยันตัวตนจากลูกค้าเจ้าของบัตรอีกครั้ง หรือไม่มีการใช้รหัสผ่าน OTP ในการทำรายการชำระเงิน
2. มีรายการจากเบอร์บัตรที่มีชุดตัวเลขเรียงกันหรือใกล้เคียงกัน ถูกส่งมาทำรายการซ้ำๆ เพื่อสุ่มเดือนปีที่หมดอายุของบัตร

คำแนะนำเพื่อป้องกัน BIN Attack สำหรับลูกค้าที่มีบัตรเครดิตและบัตรเดบิต

1. ตั้งค่าวงเงินสำหรับการชำระสินค้าให้เหมาะสมกับการทำธุรกรรมการเงินในโลกออนไลน์ หรือปรับลดวงเงินชำระสินค้าเป็นศูนย์ชั่วคราว หากยังไม่มีความต้องการจะใช้ชำระค่าสินค้า ซึ่งสามารถดำเนินการผ่านช่องทางดังนี้
    - ติดต่อศูนย์บริการสมาชิกบัตรผ่านระบบอัตโนมัติ (เบอร์ติดต่อศูนย์บริการจะปรากฏบนหลังบัตร) หรือระบบ Call Center ของธนาคาร

      (https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/Pages/CallCenter.aspx)
    - เปลี่ยนแปลงแก้ไขวงเงินบนแอปพลิเคชัน Mobile Banking ของธนาคาร
2. สังเกตการแจ้งเตือนเงินเข้า-เงินออกจากบัญชีธนาคาร และหมั่นตรวจสอบยอดการใช้จ่ายผ่านบัตรเครดิตและบัตรเดบิตอย่างสม่ำเสมอ
3. หากพบรายการบัญชีผิดปกติ ควรติดต่อธนาคารเจ้าของบัตรโดยตรง หรือหากมีข้อสงสัย สามารถติดต่อสอบถามผ่านช่องทางบริการต่าง ๆ ของธนาคาร
4. ติดตามข่าวสารจากช่องทางที่เป็นทางการของธนาคาร และ TB-CERT