เรื่อง: แนวโน้มภัยร้ายเกี่ยวกับบาร์โค้ด 2 มิติ
เรียบเรียงโดย: กิติศักดิ์ จิรวรรณกูล ณัฐพงษ์ แสงเลิศศิลปชัย และดร.โกเมน พิบูลย์โรจน์
เผยแพร่เมื่อ: 13 มีนาคม 2549

ปัจจุบันเทคโนโลยีโทรศัพท์มือถือได้เปลี่ยนแปลงไปจากในอดีตอย่างมาก เริ่มด้วยการพัฒนาจากเดิมที่โทรศัพท์มือถือมีหน้าจอขาวดำมาเป็นหน้าจอสี มีกล้องถ่ายรูปในตัว สามารถฟังเพลงและวิทยุได้ เชื่อมต่อกับเครื่องคอมพิวเตอร์ได้ หรือแม้กระทั่งเข้าสู่โลกอินเทอร์เน็ตได้อย่างง่ายดาย ประกอบกับราคาเครื่องโทรศัพท์มือถือและค่าบริการที่ไม่แพงเกินไปนัก ผู้ใช้ทั่วไปสามารถหาซื้อไว้ใช้งานได้ ดังนั้นบริการที่มีความแปลกใหม่จึงถูกพัฒนาออกมาอย่างต่อเนื่อง เพื่อตอบสนองกับความสามารถของโทรศัพท์มือถือที่เพิ่มขึ้น และการเติบโตของจำนวนผู้ใช้งานโทรศัพท์มือถือในประเทศไทยที่นับวันมีจำนวนมากขึ้นเป็นทวีคูณ หนึ่งในบริการรูปแบบใหม่ที่ถูกนำเข้ามาใช้งานในประเทศไทยคือ "การให้บริการเกี่ยวกับบาร์โค้ด 2 มิติ (2 Dimension Barcode)" ซึ่งแน่นอนว่าเมื่อบริการนี้ได้รับความนิยม สิ่งที่ตามมาคือภัยคุกคามต่างๆ ที่อาจเกิดขึ้น ดังนั้นก่อนที่จะใช้บริการนี้ควรศึกษาให้ดีก่อนว่าภัยคุกคามที่อาจเกิดขึ้นนั้นมีอะไรบ้างและจะป้องกันตนเองจากภัยคุกคามเหล่านั้นอย่างไร

ในบทความนี้จะกล่าวถึงเทคโนโลยีบาร์โค้ด 2 มิติ ตัวอย่างการใช้บาร์โค้ด 2 มิติในรูปแบบต่างๆ แนวโน้มรูปแบบภัยคุกคามที่อาจเกิดขึ้นเมื่อมีการให้บริการบาร์โค้ด 2 มิติบนโทรศัพท์มือถือ รวมทั้งวิธีการป้องกันตัวเองเมื่อใช้บริการนี้ด้วย

เทคโนโลยีบาร์โค้ด 2 มิติ

บนสินค้าแทบทุกประเภทที่วางขายในปัจจุบันมักมีบาร์โค้ด 1 มิติ ซึ่งมีลักษณะดังรูปที่ 1 ติดไว้ที่ตัวสินค้าหรือหีบห่อ เพื่อความสะดวกในการเรียกดูราคาสินค้าหรือตรวจสอบปริมาณสินค้าที่มีอยู่ โดยข้อมูลทั้งหมดจะถูกเก็บไว้ในฐานข้อมูลและใช้รหัสที่ได้จากบาร์โค้ดเป็นกุญแจในการเรียกดูข้อมูลที่ต้องการ เมื่อปริมาณการใช้งานมีจำนวนมาก การเคลื่อนย้ายฐานข้อมูลขนาดใหญ่ เพื่อให้บาร์โค้ดรหัสเดียวกันใช้งานได้ย่อมเป็นเรื่องที่ยุ่งยาก จึงเกิดแนวคิดเรื่องการนำข้อมูลของสินค้าบรรจุแทรกเข้าไปในบาร์โค้ดโดยตรง และพื้นที่ที่ใช้ในการติดบาร์โค้ดที่สินค้าต้องมีขนาดน้อยกว่าหรือเท่ากับของเดิม ผลลัพธ์หนึ่งจากแนวคิดนี้คือ บาร์โค้ด 2 มิติ ซึ่งมีหลายประเภทดังตัวอย่างในรูปที่ 2 (อ่านรายละเอียดเพิ่มเติมได้จากบทความ "แนะนำเทคโนโลยีบาร์โค้ด 2 มิติ" <http://www.thaicert.org/paper/basic/2dbarcode_intro.pdf>)

รูปที่ 1 แสดงตัวอย่างบาร์โค้ด 1 มิติ

รูปที่ 2 แสดงตัวอย่างบาร์โค้ด 2 มิติ ประเภท QR Code [1] (ซ้าย) Data Matrix [2] (กลาง) และ InterCode [3] (ขวา)

เนื่องจากบาร์โค้ด 2 มิติสามารถบรรจุข้อมูลได้มากกว่าบาร์โค้ด 1 มิติถึง 100 เท่าและชนิดข้อมูลที่ไม่ได้มีเพียงแค่ตัวเลขหรืออักษรภาษาอังกฤษ [4] ในพื้นที่ที่เล็กกว่าหรือเท่ากับของเดิม จึงส่งผลให้การใช้งานบาร์โค้ด 2 มิติมีเพิ่มมากขึ้น นอกจากนี้การพัฒนาโปรแกรมสำหรับโทรศัพท์มือถือที่มีกล้องถ่ายรูปในตัวให้สามารถถอดรหัสบาร์โค้ด 2 มิติได้ ส่งผลให้บาร์โค้ด 2 มิติตอนนี้ไม่ได้ใช้แค่ติดตั้งลงบนสินค้าเพื่อดูราคาเท่านั้น ยังสามารถประยุกต์ไปใช้ในด้านอื่นๆ ได้อีกหลากหลายด้วย

ตัวอย่างการใช้บาร์โค้ด 2 มิติ

บอกข้อมูลสินค้าทั้งการค้าแบบปลีก แบบส่ง รวมทั้งการส่งออกหรือนำเข้าในปริมาณมาก

บาร์โค้ด 2 มิติสามารถนำมาใช้ในการให้ข้อมูลต่างๆ ของสินค้า เช่น ราคา ชนิด บริษัทผู้ผลิต หรือบริษัทส่งออก เป็นต้น ดังรูปที่ 3 [5] ได้เช่นเดียวกับบาร์โค้ด 1 มิติ โดยไม่ต้องอาศัยฐานข้อมูลในเครื่องคอมพิวเตอร์เพื่อเก็บข้อมูลของสินค้า

รูปที่ 3 แสดงการใช้งานบาร์โค้ด 2 มิติบนสินค้าและผลิตภัณฑ์ต่างๆ

บอกข้อมูลอื่นๆ ตามสิ่งที่ติดตั้งบาร์โค้ด

นอกจากสินค้าประเภทต่างๆ บาร์โค้ด 2 มิติยังใช้ติดบนสิ่งอื่นเพื่อบอกข้อมูลที่เกี่ยวกับของสิ่งนั้นอย่างชื่อ สถานที่ หรือเว็บไซต์ที่สามารถหาข้อมูลเพิ่มเติมของสิ่งนั้นได้ ตัวอย่างสิ่งที่สามารถนำบาร์โค้ด 2 มิติไปติดตั้ง เช่น

บอร์ดนิทรรศการ เพื่อให้ข้อมูลที่เกี่ยวข้องกับนิทรรศการ ผู้จัดงาน หรือวิธีดาวน์โหลดรูปในนิทรรศการลงโทรศัพท์มือถือ ดังรูปที่ 4 [6]

รูปที่ 4 แสดงการใช้บาร์โค้ด 2 มิติบนบอร์ดนิทรรศการ

ป้ายโฆษณา เพื่อให้ข้อมูล ส่วนลดหรือเป็นบัตรผ่านเข้าร่วมกิจกรรมส่งเสริมการขายต่างๆ
พื้นถนน เพื่อให้ข้อมูลของสถานที่หรืออาจจะเป็นแผนที่ของเมือง ดังรูปที่ 5 [7]

รูปที่ 5 แสดงการใช้งานบาร์โค้ด 2 มิติ บนถนนในประเทศญี่ปุ่น

สถานีรถไฟ เพื่อให้ข้อมูลเส้นทางเดินรถ ราคาค่าโดยสารหรือสถานที่ที่น่าสนใจ เป็นต้น

ให้ข้อมูลติดต่อส่วนบุคคลหรือใช้สำหรับระบุตัวตน

บางครั้งการบันทึกหมายเลขโทรศัพท์หรืออี-เมล์ที่ได้รับมาในรูปนามบัตรลงบนโทรศัพท์มือถืออาจไม่สะดวกสบายนัก เพราะต้องทำการพิมพ์ข้อมูลเหล่านั้นเข้าไปในโทรศัพท์มือถือเองโดยตรง แต่หากแนบบาร์โค้ด 2 มิติที่บรรจุข้อมูลสำหรับการติดต่อเหล่านั้นไปบนนามบัตร เพียงถ่ายรูปบาร์โค้ดด้วยกล้องถ่ายรูปบนโทรศัพท์มือถือข้อมูลต่างๆ ก็จะถูกถอดรหัสและบันทึกเข้าไปในเครื่องโทรศัพท์มือถือทันที ตัวอย่างนามบัตรที่มีบาร์โค้ด 2 มิติดังรูปที่ 6 [8] และจากรูปจะเห็นตราประทับใช้แทนการเซ็นชื่อในประเทศญี่ปุ่น ก็สามารถใช้บาร์โค้ด 2 มิติแทนได้เช่นกัน

รูปที่ 6 แสดงการใช้งานบาร์โค้ด 2 มิติบนนามบัตรและตราประทับ

ใช้แทนบัตรผ่านเพื่อเข้าในสถานที่เฉพาะหรือในงานที่ถูกจัดขึ้น

ในประเทศเกาหลีมีบางที่ใช้บาร์โค้ด 2 มิติในรูปแบบที่ต่างออกไปคือแทนที่จะใช้โทรศัพท์มือถือ เพื่อถอดรหัสบาร์โค้ด 2 มิติ กลับใช้โทรศัพท์มือถือถ่ายรูปบาร์โค้ด 2 มิตินั้นเก็บไว้แล้วใช้แทนบัตรผ่านประตูแทน ดังรูปที่ 7 [9]

รูปที่ 7 แสดงการใช้งานบาร์โค้ด 2 มิติ เพื่อเป็นบัตรผ่านประตู

ให้ข้อมูลชื่อเว็บไซต์สำหรับการเชื่อมต่อเว็บไซต์หรือดาวน์โหลดข้อมูล

จากตัวอย่างที่ผ่านมามีส่วนหนึ่งใช้ข้อมูลในบาร์โค้ด 2 มิติโดยตรง เช่น ราคาสินค้า หรือข้อมูลติดต่อส่วนบุคคล เป็นต้น และก็ยังมีอีกประเภทที่ใช้ข้อมูลในบาร์โค้ด 2 มิติโดยอ้อม นั่นคือการให้บาร์โค้ดบอกชื่อเว็บไซต์ข้อมูล แล้วใช้การเชื่อมต่อผ่านทางโทรศัพท์มือถือเพื่อเข้าถึงข้อมูลนั้นๆ ซึ่งวิธีนี้ทำให้สามารถเข้าถึงข้อมูลที่มีปริมาณมากกว่าข้อมูลในบาร์โค้ด 2 มิติได้ ตัวอย่างการใช้เช่น การดาวน์โหลดภาพ เพลง เสียงเรียกเข้า หรือเกม

สำหรับโทรศัพท์มือถือ เป็นต้น ซึ่งมีการให้บริการในประเทศไทยด้วยเช่นกัน ดังรูปที่ 8 [10] โดยการที่โทรศัพท์มือถือสามารถเชื่อมต่อเว็บไซต์หรือดาวน์โหลดข้อมูลที่ระบุในบาร์โค้ด 2 มิติได้ เครื่องโทรศัพท์นั้นจำเป็นต้องมีกล้องถ่ายรูปในตัว มีโปรแกรมสำหรับถอดรหัสบาร์โค้ด และต้องเปิดใช้บริการเชื่อมต่อระบบเครือข่ายข้อมูลจากผู้ให้บริการเครือข่ายโทรศัพท์มือถือก่อน

รูปที่ 8 แสดงเว็บไซต์ที่รวบรวมบาร์โค้ด 2 มิติสำหรับดาวน์โหลดข้อมูลต่างๆ บนโทรศัพท์มือถือในประเทศไทย

รูปแบบภัยคุกคามที่อาจเกิดขึ้นจากการใช้งานบาร์โค้ด 2 มิติ

การปลอมแปลง (Spoofing)

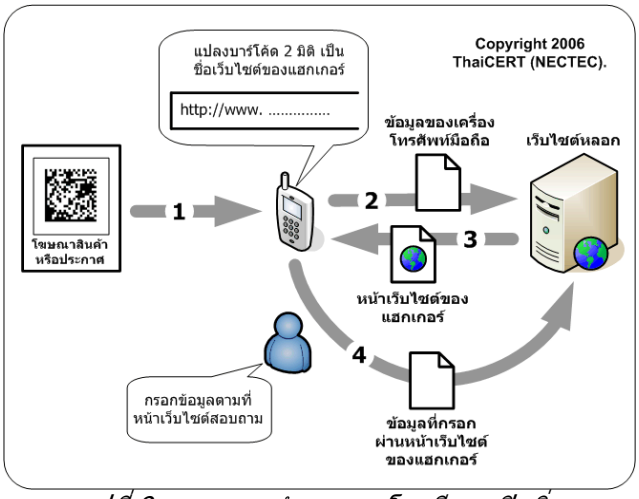
ถ้าเทคโนโลยีบาร์โค้ด 2 มิติได้รับความนิยมและมีการใช้งานอย่างแพร่หลายจนอาจนำบาร์โค้ด 2 มิตินี้มาใช้แทนนามบัตรในการให้ข้อมูลส่วนบุคคล เช่น อี-เมล์ หมายเลขโทรศัพท์มือถือ หรือชื่อเว็บไซต์ เป็นต้น การปลอมแปลงอาจเกิดขึ้นในลักษณะการปลอมแปลงข้อมูลที่เข้ารหัสเป็นบาร์โค้ด 2 มิติด้วยค่าที่ผิดๆ เช่น เว็บไซต์ปลอมที่แฮกเกอร์ตั้งขึ้นโดยเปลี่ยนแปลงชื่อเพียงเล็กน้อยจากเว็บไซต์จริง (ตัวอย่าง การใช้ชื่อเว็บไซต์ www.thalcert.org แทน www.thaicert.org) หรือชื่อเว็บไซต์ปลอมที่ยาวเกินขนาดช่องที่หน้าจอโทรศัพท์มือถือจนการตรวจสอบทำได้ยาก เป็นต้น

การปลอมแปลงในลักษณะอื่น เช่น การปลอมแปลงที่อาศัยข้อจำกัดของโทรศัพท์มือถือที่จะแสดงแต่หัวเรื่องเว็บไซต์ (Title) ที่ถอดรหัสมาได้โดยไม่แสดงชื่อเว็บไซต์จริง (Uniform Resource Locators หรือ URL) ซึ่งอาจไม่ตรงกับหัวเรื่อง การปลอมแปลงที่ตัวบาร์โค้ด 2 มิติโดยตรง กรณีที่แฮกเกอร์มีความสามารถที่จะเติมจุดบนบาร์โค้ด 2 มิติในประกาศที่ถูกติดไว้เพื่อให้ข้อมูลที่จะถอดรหัสเปลี่ยนแปลงไปตามต้องการได้ หรือการปลอมแปลงที่ตัวโปรแกรมถอดรหัสให้แสดงผลลัพธ์ออกมาเป็นชื่อเว็บไซต์ที่ตั้งปลอมไว้แทนที่จะปลอมแปลงที่ตัวบาร์โค้ด 2 มิติ เป็นต้น

การปลอมแปลงทั้งหมดที่เกิดขึ้นจะกลายเป็นจุดเริ่มต้นของภัยคุกคามอื่นๆ อันได้แก่ ฟิชชิ่ง ข่าวไวรัส หลอกลวง และมาลแวร์ ตามหลักจิตวิทยาที่ว่า ผู้ใช้จะปฏิบัติตามคำแนะนำของผู้ที่ตนคุ้นเคยหรือไว้วางใจโดยไม่ระมัดระวัง

ฟิชชิ่ง (Phishing)

เป็นที่ทราบกันดีว่าในปัจจุบันปัญหาฟิชชิ่ง [11] ได้กลายเป็นปัญหาใหญ่พอสมควรในโลกอินเทอร์เน็ต ลักษณะฟิชชิ่งด้วยบาร์โค้ด 2 มิติที่อาจเกิดขึ้นคือ แฮกเกอร์ทำการตั้งเว็บไซต์ปลอมขึ้นมาจากนั้นก็สร้างบาร์โค้ด 2 มิติที่บรรจุชื่อเว็บไซต์ปลอมแนบไปพร้อมกับใบประกาศหรือสื่อต่างๆ โดยข้อความในใบประกาศหรือสื่อต่างๆ นั้นอาจบอกให้ต้องเข้าไปเว็บไซต์ปลอมดังกล่าวเพื่ออัพเดตข้อมูลหรือขอรับบริการกับทางบริษัท เมื่อเหยื่อทำการเชื่อมต่อไปยังเว็บไซต์ปลอม ข้อมูลของโทรศัพท์มือถือของเหยื่อ เช่น หมายเลขโทรศัพท์มือถือ รุ่นหรือยี่ห้อของโทรศัพท์มือถือ เป็นต้น จะถูกส่งโดยอัตโนมัติไปพร้อมกับข้อมูลส่วนต้น (Header) ในการเชื่อมต่อกับเซิร์ฟเวอร์ และถ้าเหยื่อกรอกข้อมูลความลับของตัวเองแล้วส่งกลับไป ก็จะทำให้แฮกเกอร์ได้ข้อมูลความลับไปทั้งหมด ดังรูปที่ 9



รูปที่ 9 แสดงแบบจำลองการโจมตีแบบฟิชชิ่ง

ในบางครั้งชื่อเว็บไซต์ที่ได้จากการถอดรหัสบาร์โค้ด 2 มิตินั้นอาจเป็นชื่อเว็บไซต์ซึ่งยาวเกินขีดจำกัดที่หน้าจอของโทรศัพท์มือถือจะมองเห็นทั้งหมดหรือส่วนแสดงชื่อเว็บไซต์อาจมีขนาดตัวหนังสือเล็ก ทำให้เหยื่อไม่ให้ความสำคัญกับความถูกต้องของเว็บไซต์ อาจถูกหลอกได้โดยง่าย

ข่าวไวรัสหลอกลวง (Hoax)

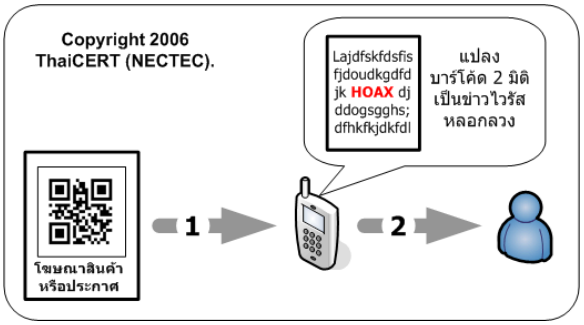
เมื่อกล่าวถึงข่าวไวรัสหลอกลวง [12] โดยทั่วไปมักเป็นข้อความข่าวที่ส่งผ่านกันทางอี-เมล์หรือห้องสนทนาต่างๆ เพื่อก่อความวุ่นวาย ซึ่งข้อความเหล่านั้นไม่เป็นความจริงและไม่มีอันตรายตามที่ข้อความอ้างถึง แต่อาจมีบางข้อความที่สร้างความเสียหายแก่ข้อมูลหรือเครื่องของผู้หลงเชื่อได้ เช่น ข่าวไวรัสหลอกลวงเกี่ยวกับไฟล์ Jdbgmgr.EXE [13] หรือข่าวไวรัสหลอกลวงเกี่ยวกับไฟล์ SULFNBK.EXE [14] ที่หลอกลวงให้ผู้ใช้ที่หลงเชื่อลบไฟล์ที่จำเป็นต่อการทำงานของระบบปฏิบัติการวินโดวส์ทิ้ง เป็นต้น

เมื่อเทคโนโลยีของบาร์โค้ด 2 มิติบนโทรศัพท์มือถือเกิดขึ้น ภัยคุกคามของข่าวไวรัสหลอกลวงในรูปแบบบาร์โค้ด 2 มิติอาจเกิดขึ้นตามมา ซึ่งบาร์โค้ด 2 มิติของข่าวไวรัสหลอกลวงนี้อาจเป็นข้อความของข่าวไวรัสหลอกลวงเอง (รูปที่ 10ก.) หรือเป็นชื่อเว็บไซต์ที่มีข่าวไวรัสหลอกลวงก็ได้ (รูปที่ 10ข.) ตัวอย่างของข่าวไวรัสหลอกลวงที่เป็นอันตรายซึ่งอาจเกิดขึ้น เช่น

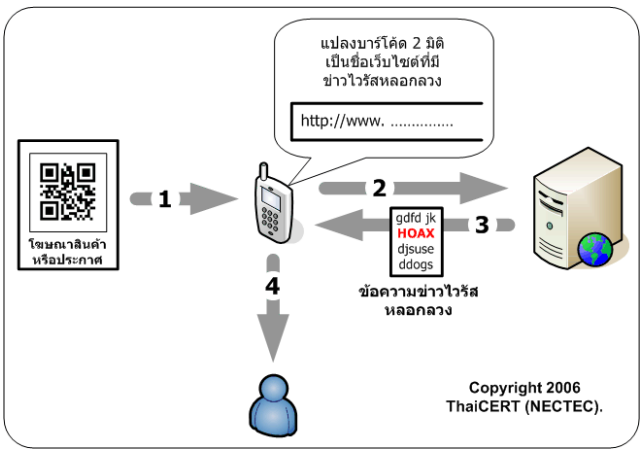
1) โฆษณาในหน้าหนังสือพิมพ์ "*รวมเทคนิค เคล็ดลับสำหรับโทรศัพท์มือถือ*" -- ข้อความในบาร์โค้ด 2 มิติ "**ลดค่าใช้บริการโทรศัพท์ต่อครั้งมากสุด 80% กด *#XXXX#**" โดย *#XXXX# อาจเป็นรหัสที่ใช้ในการลบข้อมูลทั้งหมดของเครื่องโทรศัพท์มือถือ

หรือ 2) ประกาศทั่วไป "*เตือนภัย ไวรัสบนมือถือ*" -- ข้อความบนเว็บไซต์ที่ได้จากบาร์โค้ด 2 มิติ "**ขณะนี้ได้มีไวรัสระบาดในโทรศัพท์มือถือเป็นวงกว้าง มีรายงานจากเอไอเอส ดีแทค ออเร้นจ์ และโนเกีย ว่าผู้ใช้บริการในประเทศไทยติดไวรัสตัวนี้แล้วกว่า 5 หมื่นราย หากไม่ต้องการที่จะติดไวรัสตัวนี้ให้ติดตั้งโปรแกรมแอนตี้ไวรัส ซึ่งดาวน์โหลดได้ฟรีจาก http://www.xxx.com/mobile/antivirus.sis ทั้งนี้ขอความร่วมมือส่งต่อเว็บหรือโปรแกรมนี้ เพื่อป้องกันการลุกลามของไวรัสด้วย**" โดยที่ไฟล์ antivirus.sis เป็นไฟล์ของมาลแวร์ เป็นต้น

หากผู้ใช้หลงเชื่อข่าวไวรัสหลอกลวงและปฏิบัติตามแล้วอาจสูญเสียข้อมูลในเครื่องโทรศัพท์มือถือ เสียค่าบริการโดยไม่ได้ตั้งใจ หรืออย่างเลวร้ายที่สุดอาจทำให้เครื่องโทรศัพท์ไม่สามารถใช้งานได้เลยก็ได้ ความร้ายแรงของข่าวไวรัสหลอกลวงเหล่านี้ นอกจากจะวัดจากความเสียหายที่ได้รับเมื่อปฏิบัติตามแล้ว ยังวัดจากความน่าเชื่อถือของข้อความอีกด้วย หากมีการอ้างว่าได้ข้อมูลจากผู้ที่น่าเชื่อถือหรือผู้ที่ผู้ใช้ไว้วางใจก็จะทำให้ผู้ใช้หลงเชื่อและปฏิบัติตามได้ง่ายยิ่งขึ้น



(ก.)



(ข.)

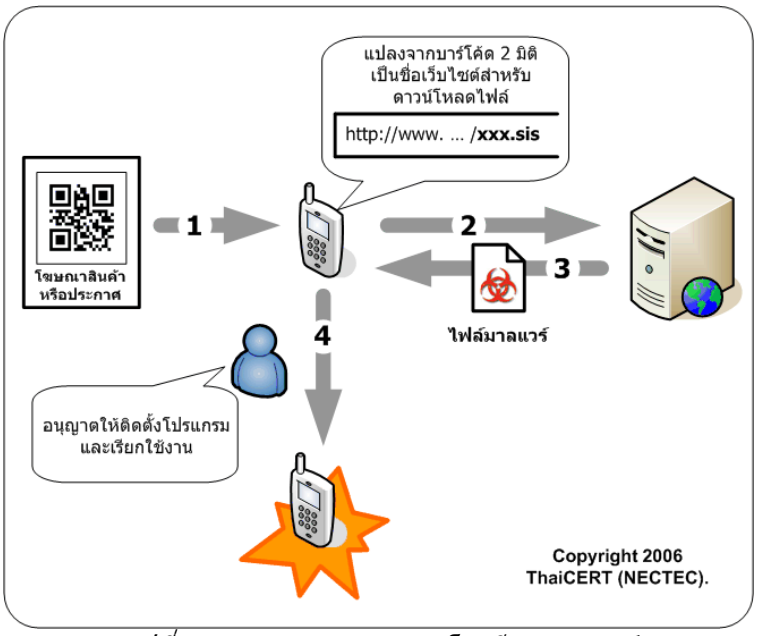
รูปที่ 10 แสดงแบบจำลองภัยคุกคามของข่าวไวรัสหลอกลวง

มาลแวร์ (Malicious Software หรือ Malware)

ในปี 2547 เริ่มมีการแพร่กระจายของมาลแวร์บนโทรศัพท์มือถือในรูปแบบต่างๆ [15] ส่วนมากจะเป็นพวกโทรจัน เช่น โทรจันที่ทำการเปลี่ยนไอคอนบนหน้าจอเครื่องโทรศัพท์มือถือ โทรจันที่ส่งตัวเองออกทางบลูทูธ (Bluetooth) เป็นต้น ซึ่งยังมีข้อจำกัดอย่างเช่นต้องเปิดการใช้งานบลูทูธ รองรับบริการส่งข้อความมัลติมีเดีย (Multimedia Messaging Service หรือ MMS) หรือต้องรู้ที่อยู่เว็บไซต์ที่จะดาวน์โหลดข้อมูล (ที่ไม่รู้ว่าเป็นมาลแวร์) เป็นต้น ทำให้การแพร่กระจายมีอยู่ในวงที่จำกัด แต่หากมีเทคโนโลยีของบาร์โค้ด 2 มิติ การแพร่กระจายของมาลแวร์บนโทรศัพท์มือถืออาจขยายวงกว้างขึ้นเทียบเท่ามาลแวร์บนเครื่องคอมพิวเตอร์ทั่วไปได้

ตัวอย่างวิธีการแพร่กระจาย เช่นในรูปที่ 11 บาร์โค้ด 2 มิติของมาลแวร์อาจถูกทำขึ้นและแฝงรวมอยู่ในแหล่งบริการดาวน์โหลดข้อมูลรูปหน้าจอ เสียงเรียกเข้า รูปเคลื่อนไหว โปรแกรมพักหน้าจอ หรือเกมของโทรศัพท์มือถือเหมือนกับที่มีแบบเป็นรหัสกด ซึ่งผู้ใช้จะไม่มีทางรู้เลยว่าชื่อเว็บไซต์ที่ได้จากบาร์โค้ด 2 มิตินั้นถูกปลอมแปลงมาหรือไม่ จนกว่าจะได้โหลดไฟล์ข้อมูลที่คิดว่าต้องการมาและติดตั้งจนเสร็จเรียบร้อยแล้ว หรืออีกวิธีหนึ่ง ชื่อเว็บไซต์ในบาร์โค้ด 2 มิติเป็นชื่อเว็บไซต์จริงไม่ได้ถูกปลอมแปลง แต่ไฟล์ข้อมูลบนเว็บไซต์นั้นกลับถูกเปลี่ยนเป็นไฟล์ของมาลแวร์แทน ทำให้การตรวจสอบไฟล์ข้อมูลที่ดาวน์โหลดมาทำได้ยากมากขึ้น เป็นต้น

จะเห็นว่าความน่ากลัวในการแพร่กระจายของมาลแวร์เพิ่มขึ้นหลายเท่าตัว ถ้ารวมวิธีการแพร่กระจายเข้ากับเทคนิคอื่น เช่น การปลอมแปลง หรือข่าวไวรัสหลอกลวง เป็นต้น จะทำให้การแพร่กระจายเพิ่มขึ้นอีก และหากเทคโนโลยีบาร์โค้ด 2 มิติพัฒนาขึ้นจนสามารถเปลี่ยนบาร์โค้ด 2 มิติที่จับภาพมาให้กลายเป็นไฟล์บนเครื่องโทรศัพท์มือถือได้ทันทีแล้ว เพียงแค่ถ่ายภาพบาร์โค้ด 2 มิติของมาลแวร์เท่านั้น ไฟล์มาลแวร์อาจเข้าติดตั้งบนโทรศัพท์มือถือทันทีโดยไม่มีเวลาให้ผู้ใช้ได้ตรวจสอบหรือทำการป้องกันเลย



รูปที่ 11 แสดงแบบจำลองการโจมตีของมาลแวร์

ภัยคุกคามอื่นๆ

นอกจากภัยคุกคามที่กล่าวมาข้างต้น อาจมีภัยคุกคามในรูปแบบอื่นที่อาศัยความสามารถ ช่องโหว่หรือจุดอ่อนของโปรแกรมถอดรหัสในการคุกคามผู้ใช้ เช่น โปรแกรมที่ใช้ถอดรหัสบาร์โค้ด 2 มิติรุ่นใหม่บางโปรแกรมสามารถทำการเชื่อมต่อไปยังที่อื่นๆ ได้โดยอัตโนมัติเมื่อนำโทรศัพท์ถ่ายภาพบาร์โค้ด 2 มิติ ถ้าข้อมูลจากการถอดรหัสบาร์โค้ด 2 มิติเป็นชื่อเว็บไซต์ โปรแกรมจะทำการเชื่อมต่อไปยังเว็บไซต์นั้นทันที หรือถ้าข้อมูลที่ได้เป็นหมายเลขโทรศัพท์ก็หมุนโทรศัพท์ไปที่เลขหมายนั้นโดยอัตโนมัติ ผลที่ตามมาทำให้เสียค่าใช้จ่ายในการเชื่อมต่อในลักษณะต่างๆ โดยที่เจ้าของโทรศัพท์มือถือไม่ทันรู้ตัว ผลกระทบนี้จะเหมือนความเสียหายจากโปรแกรมประเภท Dialer ซึ่งเป็นสปายแวร์ประเภทหนึ่ง ที่ทำให้เหยื่อเสียค่าโทรศัพท์ไปต่างประเทศหรือที่ใดในโลกนี้โดยไม่ได้เป็นคนต่อสายโทรออก เป็นต้น

วิธีการป้องกันภัยคุกคามจากบาร์โค้ด 2 มิติ

1. ตรวจสอบแหล่งที่มาของบาร์โค้ดให้แน่ใจก่อนทำการถอดรหัสทุกครั้ง
2. ใช้โปรแกรมในการถอดรหัสจากผู้ให้บริการหรือแหล่งที่น่าเชื่อถือ
3. ปิดโปรแกรมถอดรหัสบาร์โค้ด 2 มิติทุกครั้งหลังการใช้งาน เนื่องจากหากนำกล้องผ่านบาร์โค้ดโดยไม่ตั้งใจ อาจทำให้เกิดการเชื่อมต่ออัตโนมัติโดยที่ผู้ใช้งานไม่รู้ตัว
4. หลังจากที่ถอดรหัสได้แล้ว ควรตรวจสอบข้อมูลที่ได้ให้ครบถ้วนก่อน เช่น ชื่อเว็บไซต์ เป็นต้น
5. ไม่ควรเข้าเว็บไซต์ที่ได้จากการถอดรหัสบาร์โค้ดที่ไม่ทราบแหล่งที่มา หรือเว็บไซต์ที่ไม่น่าไว้วางใจ
6. ระงับการดาวน์โหลดหรือติดตั้งโปรแกรม ที่ไม่ทราบแหล่งที่มา หรือมีที่มาที่ไม่น่าไว้วางใจ
7. หาความรู้เพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยบนโทรศัพท์มือถือ
8. หากมีปัญหาเกี่ยวกับความปลอดภัยในการใช้งานหรือสงสัยว่าได้รับภัยคุกคามจากบาร์โค้ด 2 มิติ ให้ติดต่อผู้สร้างบาร์โค้ดชิ้นนั้นหรือศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)

เอกสารอ้างอิง

[1] QR Code.com <http://www.denso-wave.com/qrcode/index-e.html>, 01, 26; 2006.
[2] Products - SIMATIC Sensors – Siemens <http://www.rvsi.net/DM%20Basics.html>, 01, 26; 2006.
[3] The mobile marketing & solution enabler ▒▒▒▒▒▒▒▒ 아이콘랩 홈페이지에 오신것을 환영합니다. <http://www.iconlab.co.kr/>, 01, 26; 2006.
[4] Tan Jin Soon, **An Introduction to Bar Code** <http://www.itsc.org.sg/synthesis/2001/itsc-synthesis2001-jinsoon-bar-coding.pdf>, 02, 07; 2006.
[5] Case Study Manufacturing <http://www.denso-wave.com/qrcode/app-prod-e.html>, 01, 26; 2006.
[6] Active Print : Home <http://www.activeprint.org/index.html>, 02, 07; 2006.
[7] 活用事例 サービス編2 <http://www.denso-wave.com/qrcode/app-service2.html>, 01, 26; 2006.
[8] ぷりんと王国でデジタルプリント < http://www.print-k.com/index.html>, 01, 26; 2006.
[9] 방송자료 <http://www.iconlab.co.kr/main_promotion.html#>, 02, 07; 2006.
[10] mobileLIFE : Barcode Access <http://www.mobilelife.co.th/mobilelife/t/barcodeaccess/index.html>, 02, 07; 2006.
[11] เทคนิคการโจมตีแบบ "Phishing" <http://www.thaicert.org/paper/basic/phishing.php>, 01, 26; 2006.
[12] ThaiCERT : เอกสารเผยแพร่ : Hoax (ข่าวไวรัสหลอกลวง) <http://www.thaicert.org/paper/hoax.php>, 01, 26; 2006.
[13] Hoax : Jdbgmgr.EXE Warning <http://www.thaicert.org/paper/hoax/Jdbgmgr.EXE.php>, 01, 26; 2006.
[14] Hoax : SULFNBK.EXE <http://www.thaicert.org/paper/hoax/sulfnbk.php>, 01, 26; 2006.
[15] ช่องทางใหม่ ไวรัสร้ายบนโทรศัพท์มือถือ <http://www.thaicert.org/paper/virus/ViruswWthMobile.pdf>, 01, 26; 2006.