Hacker : เจาะข้อมูล รอจังหวะสวมรอย คอยคว้าเงิน

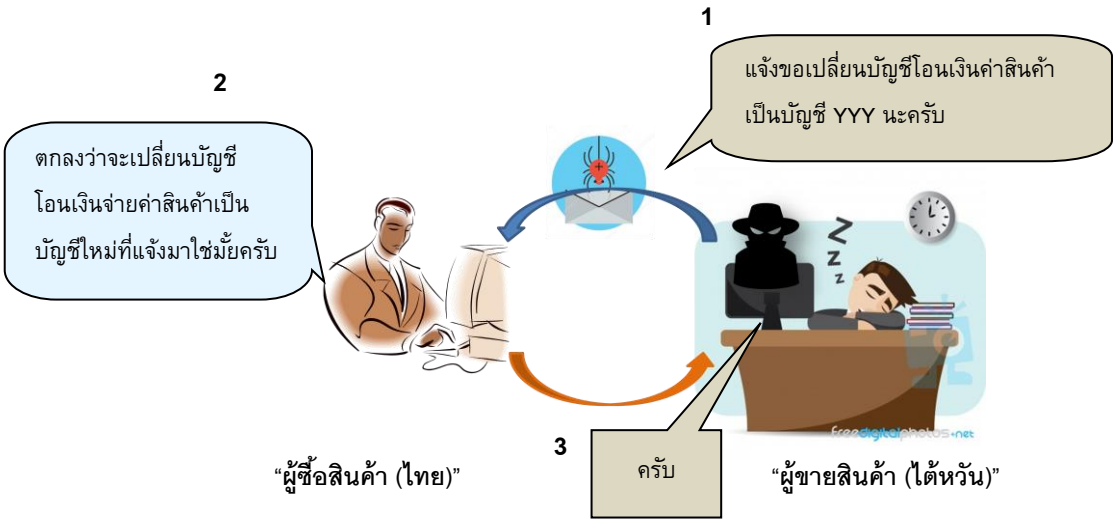
การโจมตีบนโลกไซเบอร์หรือการเจาะเข้าสู่ระบบคอมพิวเตอร์โดย Hacker ถือเป็นภัยคุกคามที่ร้ายแรงและสร้างความเสียหายให้พบเห็นกันได้อยู่เนืองๆ ทั้งการล้วงข้อมูลบัตรเครดิต สร้าง website ธนาคารปลอม โยกย้ายเงินในบัญชี หรือล่าสุดที่ก้าวล้ำไปถึงการใช้ ransomware โจมตีระบบคอมพิวเตอร์ขององค์กรชั้นนำเพื่อเรียกค่าไถ่ข้อมูลที่เป็นข่าวดังไปทั่วโลก ไม่เว้นแม้กระทั่งแวดวงการค้าระหว่างประเทศก็ยังถูก Hacker รุกรานจนได้รับความเสียหายเช่นกัน โดยรูปแบบการสร้างความเสียหายให้แก่ผู้ประกอบการที่มักพบกันบ่อยๆ คือ การที่ Hacker เจาะข้อมูลเข้ามาเพื่อรอจังหวะที่จะมีการโอนเงิน แล้วจึงสวมรอยเป็นผู้ขายแจ้งขอเปลี่ยนบัญชีที่รับโอนเงินจากผู้ซื้อให้เข้ามาในบัญชีของ Hacker แทน ซึ่งกว่าผู้ซื้อจะรู้ตัวก็สูญเงินไปแล้ว ทั้งนี้ นับตั้งแต่ต้นปี 2560 เป็นต้นมา EXIM Bank พบว่ามีผู้ทำการค้าระหว่างประเทศประสบปัญหาจาก Hacker เพิ่มขึ้นอย่างผิดสังเกต ซึ่งกลุ่มที่พบปัญหานี้บ่อยๆ คือ ผู้นำเข้าสินค้าจากประเทศในแถบเอเชีย แต่ยังไม่พบรูปแบบที่เฉพาะเจาะจง ทั้งประเภทสินค้า หรือประเทศคู่ค้า

ทั้งนี้ รูปแบบการจู่โจมของ Hacker มักเริ่มจากการเจาะเข้าสู่ระบบ email ของผู้ที่มีการติดต่อธุรกรรมต่างๆ โดยใช้ email เป็นหลัก ดังเช่นกรณีของผู้ประกอบการนำเข้ารายหนึ่งที่ติดต่อสั่งซื้อสินค้าจากผู้ขายสินค้าในไต้หวันซึ่งรู้จักค้าขายกันมานาน โดยใช้ email เป็นช่องทางหลักในการติดต่อสั่งซื้อสินค้าและส่งเอกสารระหว่างกัน เหตุการณ์ผ่านไปโดยราบรื่น โดยไม่รู้ตัวเลยว่ามี Hacker แอบลอบเข้าสู่ระบบ email ของพวกตนแล้ว

หลังจากเจาะระบบเข้าไปได้แล้ว Hacker จะคอยติดตามความเคลื่อนไหวของทั้งสองฝ่ายอย่างเงียบๆ ตลอดเวลา และรับรู้รายละเอียดแทบทุกอย่าง นับตั้งแต่ประเภทของสินค้าที่สั่งซื้อ จำนวนเงินค่าสินค้าที่ต้องโอนให้กัน ตลอดจนชื่อธนาคารและเลขที่บัญชีที่ต้องโอนเงินให้ จนกระทั่งถึงช่วงจังหวะเวลาสำคัญที่ Hacker รอคอย คือ เมื่อผู้ขายสินค้าในไต้หวันแจ้งให้ผู้นำเข้าไทยโอนเงินค่าสินค้าไปให้

ขั้นตอนถัดมา Hacker จะสวมรอยโดยกระทำเสมือนว่าตนเองเป็นผู้ขายสินค้าในไต้หวัน โดยจะ email ให้ผู้นำเข้าไทยเชื่อว่าเป็นการติดต่อกับผู้ขายสินค้าในไต้หวันรายเดิมอยู่ แล้วจัดแจงแจ้งเปลี่ยนรายละเอียดบัญชีโอนเงินค่าสินค้า โดยให้โอนมาที่บัญชีของ Hacker ซึ่งที่พบบ่อยในระยะหลัง คือ Hacker จะแจ้งให้โอนเงินเข้าบัญชีที่มีชื่อเหมือนกับชื่อบัญชีผู้ขายสินค้าจากไต้หวันตามที่เคยแจ้งไว้ แต่เปลี่ยนแปลงชื่อธนาคาร เลขที่บัญชี และประเทศรับเงินปลายทางเป็นประเทศในยุโรป แทนที่จะเป็นไต้หวันเช่นเดิม

ที่ผ่านมาหลายกรณีผู้นำเข้าเกิดความสงสัยและขอยืนยันการเปลี่ยนแปลงรายละเอียดการโอนเงิน โดยส่ง email กลับไปถามจากคู่ค้าอีกครั้งหนึ่ง ก็จะได้รับ email ยืนยันการเปลี่ยนแปลงจากคู่ค้า โดยไม่ทราบเลยว่าแท้จริงแล้ว Hacker เป็นผู้สวมรอยเป็นคู่ค้าและตอบยืนยันแทน จนทำให้ผู้นำเข้ามั่นใจ จึงได้ทำการโอนเงินไปต่างประเทศ ซึ่งกว่าที่ผู้จ่ายเงินจะรู้ตัวว่าพลาดไปแล้วก็ตอนที่ผู้ขายสินค้าแจ้งว่ายังไม่ได้รับค่าสินค้านั่นเอง



ในกรณีนี้ EXIM Bank ในฐานะที่เป็นธนาคารของผู้นำเข้า สังเกตพิรุธจากใบคำขอโอนเงินไปประเทศปลายทางที่คู่ค้าในไต้หวันให้โอนเงินไปยังธนาคารในยุโรป จึงได้แจ้งให้ผู้นำเข้าตรวจสอบกลับไปยังคู่ค้าอีกครั้งเพื่อให้ยืนยันบัญชีที่ให้โอนเงินค่าสินค้าให้ โดย Exim Bank แนะนำให้ผู้นำเข้าใช้ช่องทางอื่นนอกจากทาง email อาทิ โทรศัพท์ หรือ Fax เพื่อติดต่อกับคู่ค้า เป็นการป้องกันการสวมรอย และเมื่อตรวจสอบไปก็พบว่าคู่ค้าไม่ได้แจ้งขอเปลี่ยนบัญชีและบัญชีที่แจ้งเปลี่ยนไม่ใช่บัญชีที่แท้จริงของคู่ค้า ทำให้ผู้นำเข้ารายนี้ไม่ต้องสูญเสียเงินค่าสินค้าให้กับ Hacker ทั้งนี้ หากไม่มีการตรวจสอบอีกครั้งและเงินได้ถูกโอนไปแล้ว โอกาสที่จะติดตามเงินคืนกลับมาได้มีน้อยมาก โดยเฉพาะธนาคารในยุโรปซึ่งส่วนใหญ่ใช้ระบบการโอนเงินแบบ Straight through Processing ซึ่งหมายความว่า หากระบบพบว่าเลขที่บัญชีถูกต้อง ระบบจะนำเงินเข้าบัญชีของลูกค้าธนาคารโดยไม่ต้องตรวจสอบหรือผ่านการคัดกรองด้วยบุคคลเลย

เพื่อเป็นการลดความเสี่ยงจากการบุกรุกของ Hacker ผู้ประกอบการควรเปลี่ยน Password อย่างสม่ำเสมอ ตั้ง Password ที่เดาได้ยาก ระมัดระวังการติดตั้งหรือดาวน์โหลดโปรแกรมที่สุ่มเสี่ยง ไม่น่าเชื่อถือ และที่สำคัญ คือ ควรหมั่นสังเกตความผิดปกติต่างๆ ซึ่งหากมีข้อสงสัยควรตรวจสอบให้แน่ชัดผ่านช่องทางอื่นเพิ่มเติมนอกเหนือจากการติดต่อคู่ค้าทาง email แต่เพียงอย่างเดียว