ตอนที่ ๑๓

Malware บน Facebook

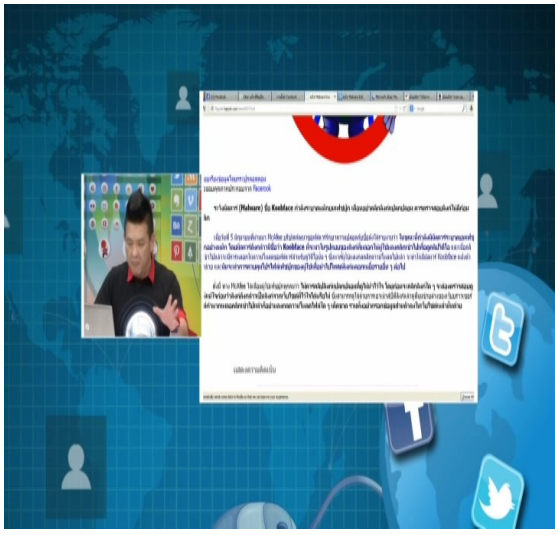
วิทยากร

“หนุ่ย” พงศ์สุข หิรัญพฤกษ์
“พี่หลามจิ๊กโก๋ไอที” ที่รัก บุญปรีชา

ในตอนนี้เป็นเรื่องของพิษภัยบน Facebook หลังจากที่คนโดนหลอกเราไปเปิดเผยข้อมูลตัวเองมากเกินไปทีนี้จะมีอีกรูปแบบหนึ่งครับ Malware Malware เป็น Subset ชนิดหนึ่งของไวรัสสิ่งที่เป็นอันตรายบนคอมพิวเตอร์ เราจะคุ้นเคยว่าไวรัสมากกว่าจริงๆ ไวรัส คือ ไฟล์ๆ หนึ่งโปรแกรมที่ส่งมาโจมตีคอมพิวเตอร์สั่งให้คอมพิวเตอร์ทำงานผิดเพี้ยนไปเขียนโปรแกรมเหมือนกันแต่เป็นโปรแกรมที่เปิดปั๊บมันทำให้เครื่องเพี้ยน แต่ Malware เป็นอีกแบบหนึ่งเนื่องจากไวรัสมันมีมากมายหลายชนิดมีทั้ง Worm Trojan Remove ชื่อทั้งหมดที่ฟังทำไมเราจะต้องจำอะไรเยอะแยะจริง ๆ มีคำแปลนะ Worm คือ หนอนเป็นการเจาะเข้ามาผ่านระบบเหมือนหนอน Trojan ถ้าจำได้ม้าเมืองทรอยมีการ

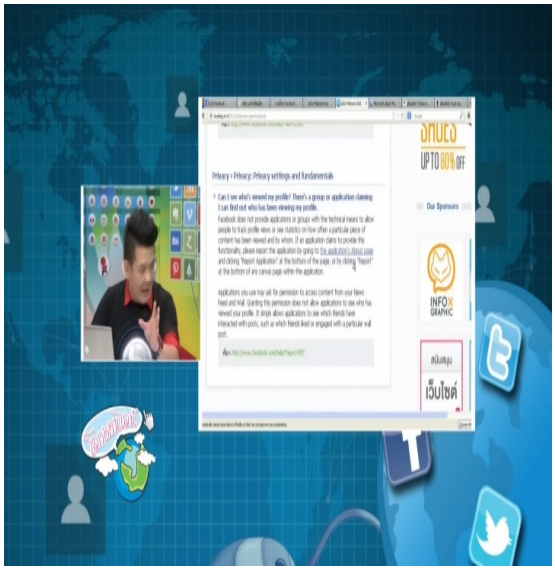
ส่งของขวัญ เครื่องพันธนาการจะโจมตีกันโจมตีไม่ได้สักที วันหนึ่งทำฟอร์มเป็นสงบศึกส่งของขวัญเป็นม้าเมืองทรอย ม้าไม้เข้าไปอยู่เขาก็เปิดประตูเมืองรับ เขาก็เข้าไปพอผ่านไปไม่นานทหารซ่อนตัวอยู่ในม้าไม้แล้วออกมาโจมตีเมืองทรอยอย่างย่อยยับ ซึ่งนั่นคือการโจมตีอย่าง Trojan คือแอบแฝงเข้ามาในเครื่องก่อนเสร็จปั๊บก็ทำลายตัวเอง แล้วขโมยของบางอย่างออกไป ส่วน ransom ware คือ ค่าไถ่ วิธีการคือมายึดเครื่องเรา เราจะปลดล็อกนี้เราต้องจ่ายค่าไถ่มันส่งเงินออนไลน์มาหลายคนคิดว่าไม่มีจริง หลายคนเคยโดนถ้าเราไปร้องเรียนเขาก็คืน account ให้เราครับตอนนี้ไม่ว่าจะเป็น twitter อะไรต่างๆครับ คืน account ได้ถ้าเราพิสูจน์ว่าเป็นของจริงอาการติด Malware เป็นอย่างไร บน Facebook เข้าผ่านเว็บเป็นคราวเซอร์วิส Facebook เขาไม่ได้อยู่เครื่องเราสักหน่อย Facebook นี่มีแอพด้วยใช่ไหมครับ มีบริการอื่นๆ ที่เป็นคนอื่นที่ผลิตเข้ามาแล้วสร้างเข้ามาเป็นบริการเสริมเข้ามาแอพบน Facebook ก็เป็นเกมไง เวลาเล่นเกมเหมือนกดแอพติด Malware ได้ใช่ไหมครับ เกมมีบริการต่าง ๆ มากมายหนึ่งในนั้นก็ คือ Malware ครับ หลอกว่าเป็นบริการชนิดหนึ่งข่าวสารโน่นนี่ พอเราไปคลิกติดตั้งก็แปลงร่างกลายเป็นตัวชั่วร้ายเลย ตอนนี้มี ๕ ตัวอย่าง การบุกไปในเครื่องเราหลากหลายวิธีการด้วยกัน ตัวแรก คูกเฟสเคยระบาดหนัก Malware แต่ละแบบมีวิธีการบุกไปในเครื่องเราหลากหลายวิธีการด้วยกันตัวแรกคูกเฟสเคยระบาดหนัก

ตรงนี้จะหลอก คือ อะไร คนทั่วไปไม่รู้อยู่แล้ว คนส่วนใหญ่ถูกหลอกให้คลิก link ปลอม ซึ่ง McAfee เป็นบริษัทที่ตรวจสอบไวรัส ไปค้นพบคูกเฟสจะเป็นคลิก link หลอกให้ผู้ใช้เข้าไปดูคลิปวิดีโอ มันเป็นเรื่องดึงดูดใจตั้งหัวข้อดูร้าย ๆ เอาหน้าคลิปนะสาวๆสวยๆ แค่นี้ก็อยากจะดูอยู่แล้ว ชวนให้เราคลิกเข้าไป แต่พอคลิกเข้าไป มันไม่พาเราไปดูทันที มันให้เราติดตั้งแอพตัวใดตัวหนึ่งหลายคนเห็นมันคืออะไร คนไทยเป็นเน็กเจนเนอเรชั่นก็กดเน็กเลยอยากดูจะให้ทำอะไรก็ตกลงไปหมดแอพแบบนี้จะเป็นเขาจะมีให้แต่ละแอพแสดงเจตจำนงว่า คุณจะเข้าถึงสิทธิ์ต่าง ๆ ที่ใช้อะไรบ้างคุณต้องแจงมาเป็นภาษาอังกฤษเราอ่านไม่รู้เรื่องเขาจะเขียนไว้เลยว่าแอพนี้มีสิทธิ์โพสต์ Facebook แทนคุณแอพตัวนี้มีสิทธิ์เอาโปรไฟล์ส่วนตัวของคุณไปใช้ประโยชน์ได้ แอพตัวนี้มีสิทธิ์โฆษณามาถึงคุณได้ด้วย แอพตัวนี้มี

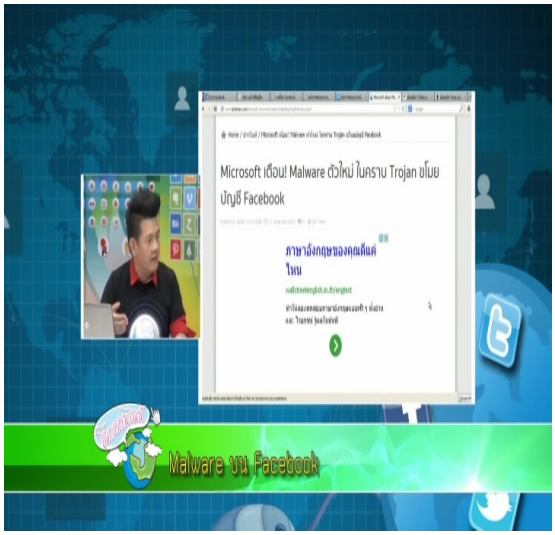


สิทธิ์พาคนไปซื้อของได้ด้วยแอพตัวนี้สามารถทำให้คุณมีซิดแพกได้ คือ แอปโดมิไนเซอร์แล้วแต่มันจะเรียกร้องมาจะขอเบอร์โทรศัพท์การเข้าถึงที่อยู่ คือ Facebook ให้แสดงเจตจำนงถ้าผู้ใช้ไม่ให้เขาก็ไม่มีสิทธิ์ได้มันเป็นวิธีการป้องกันของ Facebook ใช่ไหมครับแต่พอกดโอเคโดยไม่อ่าน เขาก็จะมาเข้าเอาสิทธิ์เหล่านั้นไง ความรอบคอบก็จะหายไป ความรอบคอบจะสู้ความวู่วามไม่ได้เลยผมแนะนำอย่าไปยุ่งกับวีดีโอ สมมุติว่า คุณไปคลิก link อะไรก็ตาม เป็นวิดีโอที่วาบหวิวคลิกเข้าไปว่าให้ไปติดตั้งอะไรก่อนนะให้รู้ไว้เลยว่าหลอกถ้าวิดีโอจริงเขาให้ดูไปแล้ว คนจะแชร์วิดีโอก็ทำไปทำไมต้องเรื่องมาก คนที่แชร์มาให้เราเหมือนเป็นเพื่อนเราจริงๆแล้วเขาถูกโพสต์โดยโปรแกรม อันนี้ Automatic เขาโดนมาแล้ว ไม่ใช่เขามาหวังดีกับเรา สมัครสมาชิกนี่สิ เขาเป็นคนขายตรง เขาไปกดโอเคเพื่อจะดูวิดีโออันหนึ่ง ตัวเขาก็ไปยิงข้อความอันนี้เพื่อจะไปหาคนอื่นโดยเจ้าตัวไม่รู้ เพื่อนเราไว้ใจได้แล้วคุณก็กลายเป็นซอมบี้ เหมือนกับเขา ตัวนี้นอกจากจะให้เราส่งต่อได้ ต้องดาวน์โหลดไฟล์เพื่อจะดูวิดีโอนี้โดยเฉพาะ เนื่องจากเป็นไฟล์พิเศษ ต้องดาวน์โหลดโปรแกรมเพื่อที่จะดูบนพีซีวิดีโอก็แค่คลิกเข้าไปพอเปิด YouTube พอคลิกเข้าไปดาวน์โหลดติดตั้ง ตอนติดตั้งเราก็ติดตั้งไวรัสทั้งหลายเข้าไปในเครื่องมันเป็นบริการที่โควกับคนเขียนไวรัสอีกทีหนึ่ง คูเฟรน เปิดตัวว่าสามารถพาไวรัสเข้าสู่เครื่องคนได้แล้วก็มาหลอกเราอีกหน้าตาของคนที่ทำไวรัส ยังไปจ้างคนอื่นที่มาทำไวรัสต่อขนาดไวรัสยังมีสื่อพาไป

เผยแพร่อีกหรือต้องมีพลับบิกเซอร์เพราะว่าโลกนี้ไวรัสเขียนง่ายไง ไวรัสเป็นโปรแกรมที่เขียนมาให้การทำงานของเครื่องผิดเพี้ยน นี่คือรูปแบบที่ ๑ คือ อย่าไปคลิก link นะครับมีอีกหลายตัวที่หลอกมาผ่านคลิก link ตัวนี้จะหลอกให้เรารู้ว่า คือ คนบางคนระแวง เล่น Facebook แล้วมีโจทย์เยอะแล้วกลัวว่าคนโน้นคนนี้จะมาดูโปรไฟล์เรา อยากรู้ว่ามีใครเข้ามาดูข้อมูลของเราบ้าง ตัวนี้ก็มาดู ติดตั้งแอพตัวนี้สิ



เพื่อดูใครที่เข้ามาเยี่ยมชมเราหลังบ้านบ้างดูว่าคนนี้เข้ามาดูบ้างหรือเปล่า คลิกไปเลย เขาก็จะพาไปดูหน้าแรกนะครับ คุณอยากรู้ไหมว่าใครมาดูโปรไฟล์ของคุณ จากนั้นจะให้เรายอมรับเราต้องตรวจสอบข้อมูลเชิงลึกของคุณนะ ดักอยู่ว่าใครมาดูข้อมูลบ้างก็จะมี e-mail มาบอกเราว่าสมมุติว่าเรายอมรับบริการมันทุกอย่างนะครับมันก็ได้สิทธิ์ในการครอบครองข้อมูลของเราแล้ว หลักการแรกมันส่งเมล์มาบอกเราก่อน Alert แจ้งเตือนมาก่อน มีใครสักคนกำลังดูโปรไฟล์คุณอยู่แจ้งเลยมีคนดูอยู่แล้วมันรายงานทุกอย่างสมมุติมีคนมาโพสต์บน wall ง่าย ๆ ก็ไปดึงสคริปบน Facebook นั่นแหละ ว่าวันหนึ่งคนเราก็ต้องมีคนมาคุยด้วยอยู่แล้วก็แค่ไป capture มาแล้วส่งมาให้คุณ แล้วกลับมาหาเราคนนี้โพสต์ใน wall ทำได้จริงถ้าอยากได้ข้อมูลที่ลึกกว่านี้คุณต้องยอมรับข้อมูลที่ลึกกว่านี้อีกมันจะมีขั้นตอนที่สองที่ส่งมาดักเราอีกว่าเปิด account โปรเลยไหม



คือ อยากรู้มากขึ้นจ่ายเงิน เขาบอกว่าแค่ให้คุณยอมรับเป็นภาษาอังกฤษ เหมือนว่าแทบจะเอา account เราไปขายเลยครับ รับโฆษณาทุกอย่าง โพสต์ทุกอย่างแทนคนอื่น รับจ้างกด like เป็นบอกกด like ให้คนอื่นได้ด้วยโดนทั่วโลกเลย หลายคนมีปัญหาเรื่องภูมิหลังนั่งระแวงตัวเองมาสืบอะไรกับเราหรือเปล่าใจอ่อนก็จะโดน Malware ตัวนี้ครับถัดมาตัวที่ ๓ เป็นตัวที่คุณหนุ่ยเล่ามาว่าเป็นม้าศึกโทรจันคือTrojan ไม่ได้บุกเข้ามาทาง Facebook นะครับ อันนี้มาจากด้านนอกเลยแต่มาเกี่ยวพันกับ Facebook จน Facebook ต้องออกมาเตือนเลยว่าเป็นไวรัสตัวใหม่มาดู Malware ตัวนี้นะครับตัวนี้จะมีผลต่อผู้ใช้ Facebook ซึ่งไปเริ่มต้นที่ประเทศบราซิล สเป็คบอกแล้วว่าเป็นการขโมยข้อมูลตัวนี้มาในส่วนขยายหรือเอ็กเทนชั่นของ Google Chrome กับ Firefox บางคนก็เปิด browser ผ่านinternet ก็จะมี popup ขึ้นมาติดตั้งปลั๊กอินตัวนี้แล้วปลั๊กอินจะเสริมประสิทธิภาพกับของคุณ

คิดว่าเป็นเรื่องดี เพราะว่าเป็นส่วนเสริมก็คลิกติดตั้งเข้าไปครับ มันก็จะแทรกซึมข้อมูลของเรามันขโมย Account Facebook มันขโมยล็อกอินแอบเอา Password และเป็นม้าสีน้ำเงินด้วยมันชั่วร้ายตรงที่มันดักจับ Facebook อย่างเดียว คนส่วนใหญ่ให้จำ user name เพื่อที่เปิดมาจะได้เข้า Facebook ได้

สะดวกเลยมันไม่ต้องรอให้คุณเข้านะทันทีที่ติดตัวนี้ลงไปในบราวเซอร์ก็วิ่งไปหา Account Facebook แล้วมันก็ยืด Account Facebook ไปเลย หลายคนสงสัยว่าอยู่ดีๆถูก Account Facebook มันจะเอา user name กับ Password save ไว้ในเครื่อง ๆ ผมก็อยู่ในบ้านผมไม่เคยมีใครมาขโมยได้ คุณนั่นแหละไปเชิญเขามาเอง ติ๊กถูกตัวนี้เอ็กเทนชั่นเกี่ยวกับการลงโปรแกรมทั่วไปคุณต้องอ่านเท่านั้นเลย ผมมีคำสำคัญให้คุณพ้นภัย ของการติดตั้งซอฟแวร์ที่คุณไม่รู้ที่มาอ่าน อ่าน อ่าน แล้วก็อ่านครับมันต้องอ่านครับถ้าคุณไม่อ่านคุณก็เสร็จครับแล้ว เป็นข้อมูลภาษาอังกฤษฝึกกันได้ภาษาอังกฤษคุณดีแค่ไหน ตัวนี้ก็แปลกดีหลายคนส่วนใหญ่คิดว่า Malwareหรือไวรัสจะมาจาก Facebook ได้นี่มาผ่านทาง browser เลยนะครับเพราะฉะนั้นระวัง

ถ้า browser ของคุณพอมีอะไรอัพเดท ถ้าเด้งขึ้นมากรุณาอ่านให้ละเอียดว่ามันเป็น link ที่คุณควรจะอัพเดทหรือเปล่าหรือว่าปลั๊กอินถ้าจะติดตั้งเข้าไปดูดีเทลว่าปลั๊กอินส่วนเสริมส่วนขยายตัวนี้มันทำอะไรให้กับเราได้บ้างเข้าไปดูชื่อดูบริษัทไปดูเว็บไซต์เขาไปดูตัวอย่าง DEMO ไปดูสกรีนช็อทก่อนว่าที่ทำขึ้นมาดูสมจริงสมจังซึ่งถ้าไวรัสลงทุนขนาดว่าสร้างเว็บขึ้นมา มีสกรีนช็อทเขียนเป็นส่วนเสริมขึ้นมาจริง ๆ นั้นก็ให้มันไปมาดูตัวอย่างต่อมาตัวนี้เป็นภัยที่มาจาก Facebook แชทหลักการ คือ จะปลอมตัวเข้ามาจะมี App Messenger ต่างหาก ความหมาย ก็คือว่า Facebook ปกติแล้วคุณตอบข้อความเป็น In box จะไป เปิดแอพเลยเรียกว่า Facebook messenger Facebook ทำให้ทุกคนถึงแม้ไม่ได้เป็นเพื่อนกันสามารถส่งข้อความได้ไม่ต้อง add friend เหมือนกล่องไปรษณีย์มันเป็นโอกาสติดต่อที่เราสามารถติดต่อใครก็ได้ มันอาศัยช่องโหว่ตรงนี้ สร้างเป็น account ปลอม ถ้าคุณเป็นผู้หญิงก็ทำ account เป็นอวต้าผู้ชายที่หล่อมาก ๆ จะส่ง messenger เข้ามาคำแรกหลักการของเจ้าตัวนี้ ถ้าเราตอบกลับก็จะมาหลอก chat เสร็จแล้วจะมี link มาให้คลิกคือถ้าเราตอบกลับไปพวกนี้ไม่ได้เป็นคนนะ เป็นอัตโนมัติ ตัวนี้โชคดีอยู่อย่างคือคนไทยไม่ค่อยโดนหลอก เราตอบไปมั่วๆ ก็จะไม่มา

คุยกับเราถ้าเราตอบหนึ่งใน ๑๐ นี้ก็คุยได้จะค่อยๆส่ง link แนบมาและติดไวรัสกลับไปน่าให้ตอบเป็นภาษาไทยและตอบอีกคนละเรื่องถาม Hi how are you ! ตอบแกเป็นใคร ไม่ตอบได้ไหม ไม่ตอบก็จบ บางทีเราไม่รู้มาดีมาร้าย อย่างบางคนรู้เลยส่ง link มา เพื่อนเรานี่คุยมาเป็นภาษาไทยตลอด ทักเป็นภาษาอังกฤษ ไม่ใช่แล้วปกติคุยกับเราเป็นภาษาไทยตลอด เพราะฉะนั้นโดนหลอกแน่ ๆ บน Facebook อย่าคลิก link ง่ายๆตรวจสอบให้ดีก่อน ตอนนี้เราจบเพียงแค่นี้