จากม้าโทรจันสู่ไวรัสคอมพิวเตอร์

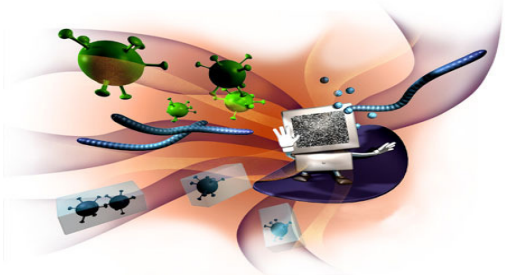
ผศ.สุพล พรหมมาพันธุ์
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ลงตีพิมพ์ในหนังสือพิมพ์ไทยโพสต์ ปีที่ 14 ฉบับที่ 5033 วันศุกร์ที่ 13 สิงหาคม พ.ศ. 2553 หน้า 4

ข่าวใหญ่ทางโทรทัศน์และหนังสือพิมพ์เมื่อช่วงวันที่ 9 -10 สิงหาคม พ.ศ. 2553 ที่ผ่านมา คือตำรวจกองปราบฯ ได้บุกจับกุม "**แก๊งแฮกเกอร์**" ซึ่งเป็นชาย 2 คนชาวเยอรมัน ได้ทำการเจาะข้อมูลธุรกรรมการเงินโดยใช้แผนส่ง "**ไวรัสโทรจัน**" ข้ามทวีป มาทะลวงเจาะข้อมูลเหยื่อ พอได้รหัสสำคัญแล้ว จะรีบโอนเข้าบัญชีของทีมงานในเมืองไทย เพื่อนำไปกดเงินออกทันที สาเหตุเกิดจากเหยื่อผู้เสียหายเข้าใช้บริการบัวหลวง ไอ แบงก์กิ้งของธนาคารกรุงเทพ ทำธุรกรรมการเงินผ่านทางอินเทอร์เน็ต แล้วจู่ ๆ เงินในบัญชีเงินฝากธนาคารกรุงเทพ สูญหายไปร่วม 7 แสนบาท วิธีการของแก๊งแฮกเกอร์จะใช้วิธีปล่อย "ไวรัสโทรจัน" (โปรแกรม ที่ถูกออกแบบขึ้นมาเพื่อแอบแฝง กระทำ การบางอย่าง) ประเภทที่เรียกว่า "ไซเรน แบงเกอร์" หรือนายธนาคารเงียบ มีฟังก์ชั่นตรวจสอบผู้ที่ติดไวรัสตัวนี้ว่ามีธุรกรรมทางการเงินหรือไม่ ส่วนผู้ที่ทำ "แฮกเกอร์" เข้าไปเจาะบัญชีพบว่าอยู่ที่ประเทศรัสเซียจะคอยมอนิเตอร์หรือติดตามกลุ่มผู้ติดไวรัส โทรจัน เมื่อสามารถเจาะบัญชีเหยื่อได้แล้วจะรีบอัพเดท เปลี่ยนรหัสหมายเลขบัญชีเป็นของบัญชีอื่น หลังจากโอนเงินสำเร็จจะให้ "ม้า" หรือผู้วิ่งกดเงินรีบไปกดเงินที่ตู้เอทีเอ็มทันที เพื่อไม่ให้เหยื่อสามารถอายัดการทำธุรกรรมได้ทัน (www.bloggang.com) ผมดูข่าวแล้วนึกในใจว่า "**มันมาอีกแล้ว**" เหตุการณ์อย่างนี้เกิดขึ้นแล้วหลายครั้งหลายคราแล้ว ไวรัส วายร้ายตัวฉกาจออกมาอาละวาดอีกแล้ว การกระทำของแก๊งแฮกเกอร์ต่างชาติเหล่านี้ทราบว่าได้ทำมานานแล้วและได้สร้างความเสียหายให้กับเศรษฐกิจไทยร่วม 100 ล้านบาทเลยทีเดียว

คราวนี้มาดูประวัติความเป็นมาของม้าโทรจัน (Trojan Horse) บ้างว่า มีประวัติความเป็นมาอย่างไรก่อนจะมาเป็นไวรัสคอมพิวเตอร์ที่น่ากลัวอยู่ในปัจจุบัน ใครที่เคยชมภาพยนตร์เรื่อง "**ทรอย** (Troy)" คงต้องนึกภาพออกอย่างแน่นอน เพราะในเรื่องมีเกี่ยวกับม้าโทรจันอยู่ **ม้าโทรจัน** คือ โปรแกรมที่สร้างความเสียหายที่หลอกลวงผู้ใช้ว่าตัวมันเป็น (หรืออาจซ่อนอยู่ภายใน) ซอฟต์แวร์ที่ไม่มีอันตราย อันที่จริงแล้วโปรแกรมประเภทหนอนคอมพิวเตอร์และไวรัสนั้นอาจซ่อนตัวอยู่ในม้าโทรจันก็ได้ แท้ที่จริงม้าโทรจันนั้นไม่ใช่ไวรัส เพราะมันไม่สามารถสร้างตัวเองได้ใหม่และแพร่กระจายออกไป ได้เหมือนกับที่ไวรัสทำ คนส่วนใหญ่จึงเข้าใจว่าเป็นไวรัส อย่างไรก็ดีไวรัสในปัจจุบันมีความสามารถหลากหลายมากขึ้น และบางครั้งมันก็ได้รวมเอาการทำงานของโปรแกรมประเภทม้าโทรจันและหนอนอินเทอร์เน็ตเข้าไปไว้ในตัวมันด้วย คำว่า **ม้าโทรจันนี้** มาจากตำนานเกี่ยวกับสงครามระหว่างกรีก และชาวโทรจัน เรื่องในตำนานนั้นมีอยู่ว่า นักรบชาวกรีก ซ่อนตัวเองอยู่ในม้าไม้และตั้งม้าไม้ทิ้งไว้หน้าประตูของกรุงทรอย โดยหลอกชาวโทรจันว่าม้าไม้นี้เป็นของบรรณาการ ชาวโทรจันหลงเชื่อตามนั้น และเปิดประตูเพื่อนำม้าไม้เข้ามาภายในเมือง หลังจากนั้นนักรบชาวกรีกที่ซ่อนอยู่ภายในม้าไม้ก็กรูกันออกมา และสร้างความโกลาหล รบราฆ่าฟันผู้คนที่อยู่ในเมืองตายเป็นจำนวนมาก จนในที่สุดชาวกรีกสามารถยึดกรุงทรอยได้สำเร็จ โปรแกรมประเภทม้าโทรจันทำงานโดยอาศัยหลักการเดียวกันนี้ โปรแกรมนั้นอาจจะมองดูไม่เป็นพิษเป็นภัย และดูน่าสนใจเพื่อหลอกให้ผู้ใช้อย่างเราให้ทำสำเนา หรือดาวน์โหลดซอฟต์แวร์นี้มา และเมื่อเรา execute โปรแกรมเหล่านี้ มันอาจสร้างความเสียหายให้กับเราขึ้นมาได้ ม้าโทรจันอาจจะอยู่ในรูปแบบของเกมคอมพิวเตอร์ หรือซอฟแวร์ประเภทอื่น ยกตัวอย่างเช่น ครั้งหนึ่งมีสมาชิกของกลุ่มแฮกเกอร์ที่ชื่อว่า Inner Circle Club สร้างโปรแกรมเกมหมากรุกที่เป็นม้าโทรจัน กลุ่มแฮกเกอร์เหล่านี้ใช้โปรแกรมดังกล่าวเพื่อ

เล่นหมากรุกับผู้ดูแลระบบที่จับพวกเขาได้ ในขณะที่พวกเขาพยายามจะแฮกเข้าไปในระบบคอมพิวเตอร์ ผู้ดูแลระบบนั้นคิดว่าตัวเองฉลาดมากที่สามารถติดตาม และจับแฮกเกอร์ได้ จึงไม่น่ามีอันตรายอะไรในการเล่นโปรแกรมหมากรุกกับแฮกเกอร์เหล่านี้ ความประมาทนี้เองที่ทำให้เขาต้องเสียใจ เพราะในขณะที่โปรแกรมหมากรุกกำลังทำงานไปนั้น ซอฟต์แวร์ม้าโทรจันก็แก้ไขระบบให้พวกแฮกเกอร์ สามารถแกะเข้าไปสู่แอ็กเคาต์ที่มีระดับความสำคัญสูงได้ โปรแกรมตัวกลางสำหรับม้าโทรจันที่นิยมใช้อีกอย่างก็คือ โปรแกรมที่มีภาพกราฟิกสวยๆ นี่คือตัวอย่างของความเสียหายที่เกิดขึ้นจากโปรแกรมม้าโทรจัน อีกอย่างก็คือ กรณีที่ผู้บริหารระดับสูงผู้หนึ่งก๊อปปี้โปรแกรมกราฟิกมาจาก Bulletin Board มาใช้ในเครื่องคอมพิวเตอร์ของเขา หลังจากนั้นไม่นานผู้บริหารคนนั้นก็พบว่าโปรแกรมที่ดาวน์โหลดมานั้นเป็นม้าโทรจัน โชคไม่ดีที่เขาพบความจริงข้อนี้หลังจากไวรัสที่ซ่อนอยู่ข้างในได้ทำลายไฟล์ในเครื่องของเขาไปถึง 900 ไฟล์ และการที่เขารู้ว่าโปรแกรมนี้เป็นม้าโทรจันก็เพราะ หลังจากที่ไวรัสทำลายข้อมูลไปแล้ว มันก็ส่งข้อความขึ้นมาเยาะเย้ยเขาทางจอมอนิเตอร์นั่นเอง โดยทั่วไปโปรแกรมม้าโทรจันจะฉลาดกว่าโปรแกรมอื่นๆ สามารถเข้ามาสืบความลับหรือทำลายข้อมูลทางธุรกิจได้ ม้าโทรจันนั้นนิยมใช้เพื่อเจาะระบบของธนาคารเพื่อสร้างอาชญากรรมที่เรียกกันว่า "Salame Slicing" คือการโอนเงินจำนวนน้อยๆ เพื่อไม่ให้ตกเป็นที่สังเกตไปจากบัญชีของลูกค้าธนาคารหลายๆ คนและถ่ายโอนเงินเหล่านี้ไปยังบัญชีลับที่สร้างขึ้นโดยเจาะระบบเข้ามา ช่วงเทศกาลสำคัญๆ มักเป็นช่วงที่มีการอาละวาดของโปรแกรมประเภทม้าโทรจันจำนวนมาก เพราะในช่วงเทศกาลนั้นเรามักส่งการ์ดอวยพรอิเล็คทอรนิกส์หรือโปรแกรมตลกๆ ไปให้เพื่อนๆ ดูเล่นกันอยู่แล้ว ดังนั้นเราจึงไม่ค่อยระมัดระวังตัวกันเท่าไหร่เลยตกเป็นเหยื่อของไวรัสกันง่ายๆ ที่เห็นกันโดยทั่วไป เช่นไม่ต้องมีการเขียนไวรัสอะไรหรอกแค่เขียนไฟล์ที่ติดไปกับอีเมล์แล้วเมื่อไฟล์นี้ทำงานจะไปกระตุ้นให้โปรแกรมตรวจสอบไวรัสทำงานแล้วฟ้องว่าไฟล์ของระบบบางไฟล์ติดไวรัสให้รีบลบออก ถ้าผู้ใช้ไม่เฉลียวใจไปลบออก ในการเปิดเครื่องครั้งต่อไปก็จะไม่สามารถเข้าเครื่องได้ ทำให้ต้องเสียเวลาลงระบบใหม่ทั้งหมด พวกนักเขียนไวรัสชอบใช้ช่วงหน้าเทศกาลในการปล่อยไวรัสออกมา (www.expert2you.com)



ในโลกของคอมพิวเตอร์จะเห็นได้ว่า มีสัตว์หลายชนิดเข้ามาเกี่ยวข้องอย่างเช่น Bug ที่แปลว่า **แมลง** ก็มีการนำเอาใช้กันในแวดวงของคอมพิวเตอร์เช่นกัน Bug คือ ข้อผิดพลาดที่อาจเกิดขึ้นจากขั้นตอน หรือการเขียนโปรแกรมทั้งในฮาร์ดแวร์และซอฟต์แวร์ ซึ่งเป็นผลทำให้การทำงานผิดพลาดไป ไม่เป็นไปตามต้องการ ถ้าปัญหาเกิดขึ้นในซอฟต์แวร์ก็แก้ไขโดยโปรแกรม ถ้าเกิดขึ้นกับฮาร์ดแวร์ก็ต้องออกแบบและสร้างวงจรกันใหม่ ข้อผิดพลาดบางอย่างอาจทำให้โปรแกรมหยุดทำงานหรือข้อมูลสูญหายไป บางอย่างอาจเพียงแค่รบกวน และส่วนมากอาจจะไม่เคยสังเกตเห็น ดังนั้น ม้าโทรจันก็เช่นเดียวกัน จะเห็นได้ว่า จากม้าโทรจัน_สู่ไวรัสคอมพิวเตอร์นั้น ได้สร้างความเสียหายให้กับสังคมและเศรษฐกิจของประเทศต่างๆ ทั่วโลกเป็นจำนวนมาก ซึ่งเมื่อดูความเป็นมาแล้ว มีประวัติอันยาวนานมาหลายร้อยหลายพันปีเลยทีเดียว.