Malware เรียกค่าไถ่ “WannaCry” อาชญากรรมคอมพิวเตอร์

ในโลกที่ชีวิตของเราต้องเกี่ยวข้องกับอินเทอร์เน็ต สิ่งหนึ่งที่ทำให้บุคคลทั่วไปเกิดความกังวลคืออาชญากรรมคอมพิวเตอร์ (Computer Crime) หลายท่านอาจเคยได้ยินคำนี้ แต่หลายท่านก็ยังคงไม่เข้าใจอย่างชัดเจนว่าอาชญากรรมคอมพิวเตอร์มันคืออะไร จึงขอขยายความดังนี้ อาชญากรรมคอมพิวเตอร์ คือ การกระทำที่ผิดกฎหมาย โดยใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือ หรือการกระทำที่ผิดกฎหมายที่ก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ การกระทำของอาชญากรรมคอมพิวเตอร์เราเรียกว่าการโจมตี (Attack) การโจมตีคือ การกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ เพื่อเข้าควบคุมการทำงานของระบบ เพื่อให้ระบบเกิดความเสียหายหรือโจรกรรมสารสนเทศ อาชญากรรมคอมพิวเตอร์มีหลายรูปแบบ แต่ที่เราได้ยินกันบ่อยๆมี 2 ชนิดคือ Malware กับ Virus ทั้งสองคำเรามักจะได้ยินคำว่า Virus มากกว่า ส่วนคำว่า Malware เพิ่งจะได้ยินจนคุ้นหูเมื่อสัปดาห์ที่ผ่านมานี่เอง (ประมาณวันศุกร์ที่ 12 พฤษภาคม 2560)

Malware คือ ซอฟแวร์หรือโปรแกรมคอมพิวเตอร์ที่ถูกสร้างขึ้นมาโดยมีจุดมุ่งหมายเพื่อที่จะทำลายหรือสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือทรัพย์สินและข้อมูลของผู้ใช้งานคอมพิวเตอร์ เรียกได้อีกอย่างหนึ่งว่า “Malicious Software” ส่วน Virus คือ โปรแกรมคอมพิวเตอร์ที่มุ่งร้ายต่อโปรแกรมหรือไฟล์ โดยจะสามารถสำเนาตัวเองไปกับข้อมูลหรือไฟล์เป้าหมาย เมื่อไฟล์ถูกรันโค้ด Virus ก็จะเริ่มทำงานตามคำสั่งที่บรรจุในโค้ด เช่น ลบไฟล์หรือแก้ไขค่าบางอย่าง เป็นต้น Virus มีโครงสร้างประกอบด้วย 4 ส่วนดังนี้ (1) Mark ทำหน้าที่ป้องกันการติดเชื้อ Virus อื่น (2) Infection Mechanism กลไกทำหน้าที่คัดลอกตัวเองไปฝังหรือแนบกับไฟล์อื่น (3) Trigger คือ เงื่อนไขในการกระตุ้นให้ไวรัสทำงาน และ (4) Payload คือ การกระทำที่มุ่งร้ายต่อเป้าหมาย

ดราวนี้คงพอแยกได้ว่า Malware กับ Virus มันแตกต่างกันอย่างไรแล้ว เราลองมาทำความเข้าใจเกี่ยวกับเหตุการณ์ที่เพิ่งเกิดขึ้นและทำความกังวลให้กับคนในวงการคอมพิวเตอร์อย่างมากในช่วงกลางเดือนพฤษภาคม 2560 ที่ผ่านมา นั่นคือเมื่อวันที่ 12 พฤษภาคม 2560 บริษัท Avast ได้รายงานการแพร่ระบาดของ Malware เรียกค่าไถ่ชื่อ WannaCry โดยMalware ดังกล่าวมีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้

สิ่งที่น่ากังวลเป็นพิเศษสำหรับ Malware นี้คือความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ระบบ SMB (Server Message Block) ของระบบปฏิบัติการ Windows ผู้ใช้งานที่ไม่ update ระบบปฏิบัติการ Windows มีความเสี่ยงที่จะติด Malware นี้ ช่องโหว่ที่ถูกใช้ในการแพร่กระจาย Malware เป็นช่องโหว่ที่ถูกเปิดเผยสู่สาธารณะตั้งแต่ช่วงเดือนเมษายน 2560 และถึงแม้ทาง Microsoft จะเผยแพร่ update แก้ไขช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แล้ว แต่ก็ยังพบว่าปัจจุบันมีเครื่องคอมพิวเตอร์ที่ยังไม่ได้ update ดังกล่าวและถูกโจมตีจาก Malware ตัวนี้มากกว่า 500,000 เครื่อง ใน 99 ประเทศ โดยเกิดผลกระทบสูงต่อหน่วยงานสาธารณสุขของประเทศอังกฤษ ในประเทศไทยพบผู้ติด Malware ตัวนี้อยู่บ้าง แต่ยังไม่พบการแพร่กระจายในวงกว้าง

จากข้อมูลของ Microsoft ระบบปฏิบัติการที่มีช่องโหว่ในระบบ SMB เวอร์ชั่น 1 ที่ถูกใช้ในการโจมตีโดย Malware นี้ มีตั้งแต่ Windows XP, Windows Server 2003 ไปจนถึง Windows 10 และ Windows Server 2016 แต่เมื่อเดือนมีนาคม 2560 ทาง Microsoft ไม่ได้ออก update แก้ไขช่องโหว่นี้ให้กับ Windows XP และ Windows Server 2003 เนื่องจากสิ้นสุดระยะเวลาสนับสนุนไปแล้ว อย่างไรก็ตาม เนื่องจากปัจจุบันยังมีเครื่องคอมพิวเตอร์ที่ใช้งานสองระบบปฏิบัติการดังกล่าวและยังเชื่อมต่อกับอินเทอร์เน็ตอยู่ จึงทำให้ถูกโจมตีได้ Microsoft จึงออก update ฉุกเฉินมาเพื่อแก้ไขปัญหานี้ โดยผู้ใช้สามารถดาวน์โหลด update ดังกล่าวได้จากเว็บไซต์ของ Microsoft

พฤติกรรมของมัลแวร์ WannaCry

ปัจจุบันพบข้อมูลรายงานการตรวจสอบ Malware จากเว็บไซต์ Hybrid Analysis ซึ่งให้บริการวิเคราะห์ Malware มีผลลัพธ์ของการวิเคราะห์ไฟล์ต้องสงสัย ซึ่งผู้ใช้งานตั้งชื่อว่า wannacry.exe โดยผลลัพธ์แสดงให้เห็นว่าเป็น Malware ประเภท Ransomware และมีสายพันธุ์สอดคล้องกับ Malware WannaCry ที่แพร่ระบาดอยู่ในปัจจุบัน ซึ่งมีฟังก์ชั่นที่พบเรื่องการเข้ารหัสลับข้อมูลไฟล์เอกสารบนเครื่องคอมพิวเตอร์ การแสดงผลข้อความเรียกค่าไถ่ เป็นต้น

ข้อแนะนำในการป้องกัน

1.ติดตั้งแพตช์แก้ไขช่องโหว่ SMBv1 จาก Microsoft โดย Windows Vista, Windows Server 2008 ถึง Windows 10 และ Windows Server

2.หากไม่สามารถติดตั้ง update ได้ เนื่องจาก Malware เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ SMBv1 ซึ่งถูกใช้ใน Windows เวอร์ชั่นเก่า เช่น Windows XP, Windows Server 2003 หรือระบบเซิร์ฟเวอร์บางรุ่น หากใช้งาน Windows เวอร์ชั่นใหม่และไม่มีความจำเป็นต้องใช้ SMBv1 ผู้ดูแลระบบอาจพิจารณาปิดการใช้งาน SMBv1

3.หากไม่สามารถติดตั้ง update ได้ ผู้ดูแลระบบควรติดตามและป้องกันการเชื่อมต่อพอร์ต SMB (TCP 137, 139 และ 445 UDP 137 และ 138) จากเครือข่ายภายนอก อย่างไรก็ตาม การบล็อกพอร์ต SMB อาจมีผลกระทบกับบางระบบที่จำเป็นต้องใช้งานพอร์ตเหล่านี้ เช่น file sharing, domain, printer ผู้ดูแลระบบควรตรวจสอบก่อนบล็อกพอร์ตเพื่อป้องกันไม่ให้เกิดปัญหา

4.Update ระบบปฏิบัติการให้เป็นเวอร์ชั่นล่าสุดอยู่เสมอ หากเป็นได้ได้ควรหยุดใช้งานระบบปฏิบัติการ Windows XP, Windows Server 2003 และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ

5.ติดตั้ง Anti-Virus และ update ฐานข้อมูลอย่างสม่ำเสมอ ปัจจุบัน Anti-Virus ส่วนใหญ่ (รวมถึง Windows Defender ของ Microsoft) สามารถตรวจจับ Malware WannaCry สายพันธุ์ที่กำลังมีการแพร่ระบาดได้แล้ว

เรียบเรียงโดย : รองศาสตราจารย์ ดร.เอื้อน ปิ่นเงิน
ผู้อำนวยการสถาบันคอมพิวเตอร์