ภัยร้าย WannaCry Ransomware สอนอะไรเรา

อ. นพ.นวนรรน ธีระอัมพรพันธุ์

อาจารย์ ภาควิชาเวชศาสตร์ชุมชน และผู้ช่วยคณบดีฝ่ายนโยบายและสารสนเทศ

คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี

จากเหตุการณ์การแพร่ระบาดของภัยร้าย มัลแวร์เรียกค่าไถ่ (ransomware) ที่ชื่อ Wanna Decryptor หรือที่นิยมเรียกกันว่า WannaCry ที่เริ่มระบาดเมื่อวันที่ 12 พ.ค. 2560 โดยในเวลาเพียงไม่ถึง 24 ชั่วโมง มีรายงานเครื่องที่ถูกโจมตีแล้วกว่า 75,000 เครื่องใน 99 ประเทศ การระบาดใหญ่ในเครื่องคอมพิวเตอร์ของโรงพยาบาลต่างๆ ในเครือ National Health Service (NHS) ของอังกฤษ กว่า 40 แห่ง ทำให้ระบบสารสนเทศของ รพ. ใช้งานไม่ได้ การให้บริการผู้ป่วยหยุดชะงัก การให้บริการที่ไม่เร่งด่วนถูกยกเลิก และบาง รพ. แนะนำให้ผู้ป่วยที่ไม่จำเป็นหลีกเลี่ยงการมารับบริการหรือให้ไป รพ. อื่นแทน นอกจากนี้ยังระบาดหนักในหน่วยงานทั้งภาครัฐและเอกชนของรัสเซีย สเปน ไต้หวัน จีน เป็นต้น ด้วย

กลไกการทำงานของ WannaCry คือ เมื่อมันเข้ามาติดในเครื่องใดที่ใช้ระบบปฏิบัติการ Microsoft Windows มันจะเข้ารหัสล็อกไฟล์ข้อมูลภายในเครื่อง เพื่อให้ผู้ใช้งานเปิดไฟล์ของตัวเองไม่ได้ และจะปรากฏข้อความเรียกค่าไถ่ (ดังภาพ) เป็นเงิน 300 ดอลลาร์สหรัฐฯ (ในสกุลเงินออนไลน์ที่เรียกว่า Bitcoin) เพื่อให้ผู้ใช้งานยอมจ่ายเงินแลกกับรหัสในการ unlock ไฟล์ข้อมูลของตน สิ่งที่ทำให้มัลแวร์ตัวนี้ระบาดในวงกว้างทั่วโลกอย่างรวดเร็ว คือ การที่ hacker ผู้พัฒนามัลแวร์ตัวนี้ ใช้ “ช่องโหว่ความปลอดภัย” (security vulnerability) ซึ่งเป็น bug อันหนึ่ง[1-2] ของ Windows

แม้ Microsoft จะเคยออก update เพื่ออุด (patch) ช่องโหว่ดังกล่าวแล้วตั้งแต่เดือน มี.ค. 2560 แต่เนื่องจากเครื่องคอมพิวเตอร์ส่วนใหญ่ของผู้ใช้งานที่บ้านและภายในองค์กร มักไม่ได้อุดช่องโหว่ (update patches) เป็นประจำ ทำให้ช่องโหว่ดังกล่าวยังคงมีอยู่ในเครื่องส่วนใหญ่ทั่วโลก เมื่อเครื่องหนึ่งใน network ถูกโจมตีด้วยมัลแวร์ตัวนี้ มันก็จะอาศัยช่องโหว่ดังกล่าวแพร่ไปยังเครื่องอื่นๆ ในเครือข่ายที่ไม่ได้อุดช่องโหว่ดังกล่าวเช่นกัน จึงเกิดการระบาดใหญ่ทั่วโลก

ในประเทศไทยเรา มีรายงานการระบาดของ WannaCry แล้วจำนวนหนึ่ง แม้ในขณะที่เขียนนี้จะยังไม่มีการระบาดรุนแรงในวงกว้างก็ตาม แต่ก็มีบางหน่วยงานที่ได้รับผลกระทบไปแล้ว ในมหาวิทยาลัยมหิดลยังไม่มี

รายงานว่ามีการระบาดเกิดขึ้น ซึ่งส่วนหนึ่งน่าจะมาจากการเตรียมการรับมือของกองเทคโนโลยีสารสนเทศของมหาวิทยาลัย และหน่วยงานด้านไอทีของส่วนงานต่างๆ ตลอดจนความตระหนักและร่วมมือของชาวมหิดล

วิธีป้องกันจาก WannaCry ที่สำคัญที่สุด คือ การอุดช่องโหว่ที่เป็นปัญหา[1-6] โดยอาจอัปเดตผ่าน Windows Update ของ Windows หรือดาวน์โหลด patch update ในระบบปฏิบัติการที่ตรงกันโดยตรง[1] แม้เป็น Windows เก่าๆ เช่น Windows XP, Windows Server 2003 ซึ่ง Microsoft ไม่ support แล้ว ทำให้ไม่สามารถอัปเดตผ่าน Windows Update ได้ แต่ก็สามารถดาวน์โหลด patch update สำหรับช่องโหว่นี้เป็นกรณีพิเศษได้จากเว็บไซต์[7] นอกจากนี้เอกสารอ้างอิงต่างๆ ยังมีรายละเอียดวิธีการทางเทคนิคที่อาจช่วยลดความเสี่ยงลงได้โดยเฉพาะสำหรับผู้ดูแลระบบ อย่างไรก็ดี ผู้เขียน**ไม่แนะนำ**ให้ผู้ใช้งานทั่วไปดาวน์โหลดโปรแกรมอื่นที่อ้างว่าป้องกัน WannaCry ได้มาใช้ป้องกันเอง หรือใช้วิธีการป้องกันที่ปรากฏตามสื่อต่างๆ นอกจากจะใช้การอุดช่องโหว่ที่เป็นปัญหาโดยตรง เพราะบางวิธีอาจได้ผลเพียงเฉพาะมัลแวร์บางสายพันธุ์หรือไม่ยืนยันประสิทธิผล และอาจทำให้ผู้ใช้งานชะล่าใจว่าปลอดภัย ทั้งๆ ที่ไม่ได้แก้ไขที่ต้นเหตุ ยกเว้นเสียแต่ว่าผู้ใช้งานจะมีข้อจำกัดในการอัปเดต patch ดังกล่าวและมีความเข้าใจทางเทคนิคมากพอที่จะประเมินและจัดการความเสี่ยงของตนเอง นอกจากนี้ยังควรอัปเดตระบบปฏิบัติการและ applications ต่างๆ อย่างสม่ำเสมอ ใช้ Antivirus ที่ถูกลิขสิทธิ์และอัปเดตเป็นปัจจุบัน สำรองข้อมูลเก็บไว้นอกเครื่อง (offline backup) เป็นประจำ และหลีกเลี่ยงการเปิดไฟล์แนบของอีเมลหรือ link ที่ไม่มั่นใจในความปลอดภัย (“คิดก่อนคลิก”)

สุดท้ายนี้ ผู้เขียนเชื่อว่า ภัยคุกคามเช่นนี้ จะมีเพิ่มมากขึ้นในอนาคตอันใกล้ และน่าจะเป็นโลกแห่งความจริงในวงการไอทีที่เราต้องยอมรับและปรับตัวให้ทัน องค์กรต่างๆ จึงควรหาทางยกระดับมาตรการรักษาความมั่นคงปลอดภัยของระบบ ประเมินและจัดการความเสี่ยงของระบบรวมทั้งอุปกรณ์เครื่องมือเฉพาะด้านต่างๆ เช่น เครื่องมือแพทย์ที่เชื่อมต่อกับระบบเครือข่าย ให้ดีขึ้น หมั่นสร้างความตระหนักในหมู่บุคลากร และเตรียมพร้อมรับมือกับภัยคุกคามเหล่านี้อย่างเต็มที่

เอกสารอ้างอิง

1. https://technet.microsoft.com/library/security/MS17-010
2. https://www.us-cert.gov/ncas/current-activity/2017/03/16/Microsoft-SMBv1-Vulnerability
3. https://www.thaicert.or.th/alerts/user/2017/al2017us001.html
4. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_WannaCry_Ransomware.pdf
5. https://www.thaicert.or.th/downloads/files/info_WannaCry-User.png
6. https://www.thaicert.or.th/downloads/files/info_WannaCry-Admin.png

7. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/