Petya มัลแวร์เรียกค่าไถ่ตัวใหม่

ปกิณกะ IT

มหันตภัยมัลแวร์ PetYa

คงจำกันได้เมื่อประมาณกลางเดือนพฤษภาคมที่ผ่านมามีข่าวใหญ่ในวงการไอที นั่นคือ ข่าวการแพร่กระจายของมัลแวร์ WannaCry ที่ถูกส่งไปยังเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน ทำให้ระบบคอมพิวเตอร์ของหน่วยงานนั้น ไม่สามารถทำงานได้ จนกว่าหน่วยงานจะจ่ายเงินตามที่ผู้ส่งมัลแวร์กำหนดมา กระแสข่าวเงียบไประยะหนึ่ง จนเมื่อปลายเดือนมิถุนายนที่ผ่านมา มีมัลแวร์เรียกค่าไถ่ตัวใหม่ที่ชื่อ Petya ซึ่งกล่าวกันว่าร้ายแรงกว่ามัลแวร์ WannaCry มากนัก เพียงแค่ 72 ชั่วโมง พบคอมพิวเตอร์ทั่วโลกถูกจับเป็นตัวประกันแล้วมากกว่า 3 แสนเครื่อง ล็อคข้อมูลทั้งฮาร์ดดิสก์เป็นตัวประกัน มีการแจ้งข้อมูลแล้วว่าระบาดหนักในประเทศ รัสเซีย ยูเครน อินเดีย และกลุ่มประเทศในยุโรป ส่วนใหญ่ที่ได้รับผลกระทบ คือ ธุรกิจธนาคาร บริษัทด้านพลังงาน สนามบิน และล่าสุดในประเทศไทยก็เริ่มมีพบคอมพิวเตอร์ในองค์กรธุรกิจ อเจนซี่ ติดมัลแวร์ตัวนี้แล้ว

ถึงแม้ว่ามัลแวร์ตัวนี้จะอาศัยช่องโหว่เดียวกันกับที่ WannaCry เคยใช้ แต่จะต่างกันตรงที่ WannaCry ผู้ใช้จะยังสามารถบู๊ตเครื่องเข้า Windows และยังมองเห็นไฟล์เอกสารที่โดนล็อคอยู่ แต่ Petya จะรุนแรงกว่าเพราะมันจะล็อคข้อมูลทั้งฮาร์ดดิสก์ และไม่อนุญาตให้บู๊ตเครื่องเข้าสู่ระบบปฏิบัติการ เมื่อเปิดเครื่องขึ้นมาจะเป็นหน้าจอสีดำ ตัวหนังสือสีแดง โดยมีข้อความแจ้งมีเนื้อหาว่า ข้อมูลทั้งหมดได้ถูกเข้ารหัสไว้แล้ว ไม่มีใครสามารถกู้คืนข้อมูลได้ ถ้าหากต้องการได้ข้อมูลคืน ให้ทำการส่งเงิน $300 หรือ ประมาณ 10,000 บาท ผ่านทาง Bitcoin เพื่อทำการปลดรหัสที่ล็อคข้อมูลเอาไว้ มีข้อมูลว่ามีคนยอมที่จะจ่ายเงินค่าไถ่ $300 ไปทางอีเมล์ wowsmith123456@posteo.net ที่ระบุอยู่บนหน้าจอ แต่ก็ไม่สามารถติดต่อไปยังอีเมล์ดังกล่าวได้

วิธีป้องกันมัลแวร์ Petya

การแพร่กระจายของมัลแวร์ตัวนี้ สามารถวิ่งไปยังคอมพิวเตอร์อื่นๆ ได้โดยอัตโนมัติ ผ่านช่องโหว่ระบบ SMBv1 ที่มีใน Windows รุ่นเก่าๆ อย่าง Windows XP, Windows Server 2003 และ Windows Vista

วิธีป้องกัน ก่อนที่จะติดมัลแวร์นั้น ก็เหมือนกับก่อนหน้านี้ คือ

1. จัดการติดตั้งแพตซ์แก้ไขช่องโหว่ SMBv1 ทันที ซึ่งตอนนี้ Microsoft ได้ออกแพตซ์เพื่ออุดรูรั่วนี้แล้ว

1.1 Windows Vista, Windows Server 2008 ถึง Windows 10 และ Windows Server 2016 ดาวน์โหลดที่ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

1.2 Windows XP และ Windows Server 2003 ดาวน์โหลดอัปเดตได้จาก https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

2. ติดตั้งโปรแกรมแอนติไวรัส และอัพเดตฐานข้อมูลให้เป็นเวอร์ชั่นล่าสุด

3. Back Up ข้อมูลที่สำคัญในคอมพิวเตอร์เอาไว้สม่ำเสมอ โดยพื้นที่เก็บข้อมูลสำรองนี้จะต้องไม่เชื่อมต่อกับคอมพิวเตอร์อื่น, ระบบเครือข่าย หรือต่อออนไลน์

4. ปัจจุบันยังไม่ทราบแน่ชัดว่า มัลแวร์ตัวนี้สามารถแพร่กระจายผ่านทางอีเมล์ได้หรือไม่ แต่เพื่อความปลอดภัย แนะนำให้หลีกเลี่ยงการเปิดไฟล์ ที่ต้องสงสัยที่แนบมากับอีเมล์

วิธีแก้ Petya ถ้าหากเครื่องติดมัลแวร์

ณ เวลานี้ ต้องบอกว่า ยังไม่มีเครื่องมือ หรือ Tools ใดๆ ที่จะถอดรหัสมัลแวร์ตัวนี้ได้ ถ้าหากเครื่องคอมพิวเตอร์ของท่านพลาดติดมัลแวร์นี้ไปแล้ว สิ่งแรกที่ควรทำ คือ ทำการถอดสาย LAN และปิด Wi-Fi (ทำการออฟไลน์ออกจากระบบ) เพื่อป้องกันไม่ให้มันแพร่ไปสู่คอมพิวเตอร์อื่นๆ ในวงแลน หรือ องค์กรของท่าน แต่ยังไม่ต้องปิดเครื่อง ให้ทำการแบคอัพไฟล์งาน หรือ เอกสารที่สำคัญออกมาก่อน และรีบแจ้งผู้ดูแลระบบของหน่วยงานเพื่อทำการเฝ้าระวังและป้องกันไม่ให้เกิดการแพร่กระจาย

ข้อมูลอ้างอิง : The Hacker News , Telegraph , Thaicert

เรียบเรียงโดย : รองศาสตราจารย์ ดร.เอื้อน ปิ่นเงิน

ผู้อำนวยการสถาบันคอมพิวเตอร์