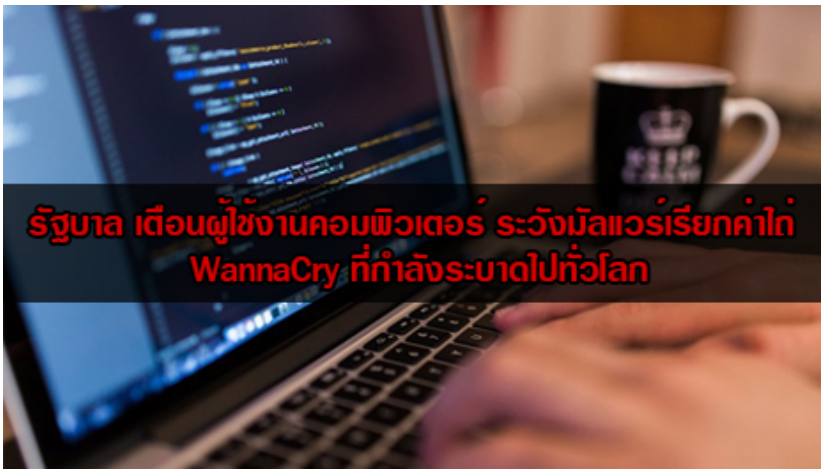
กระทรวงดิจิทัลฯ พร้อมรับมือ-แก้ปัญหามัลแวร์เรียกค่าไถ่ ย้ำผู้ใช้คอมฯ อย่าเปิดอีเมลที่ไม่รู้จักแหล่งที่มา (16/5/2017)



กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มอบไทยเซิร์ตพร้อมรับมือและช่วยแก้ไขปัญหามัลแวร์เรียกค่าไถ่
เร่งเตือนประชาชนผู้ใช้คอมพิวเตอร์ หลังพบมัลแวร์เรียกค่าไถ่ WannaCry ระบาดหนักทั่วโลก
ย้ำอย่าเปิดอีเมล์หรือไฟล์เอกสารที่ไม่รู้จักแหล่งที่มา และหมั่นสำรองข้อมูลสำคัญในฮาร์ดดิสก์อื่น (External Hardisk) อย่างสม่ำเสมอ หากพบว่าติดมัลแวร์ดังกล่าวรีบปิดเครื่องพร้อมแจ้งสายด่วน 1212 ทันที

นาวาอากาศเอก สมศักดิ์ ขาวสุวรรณ์ รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) เปิดเผยว่า
จากกรณีที่มีมัลแวร์เรียกค่าไถ่ ชื่อ \"WannaCry ระบาดไปยังคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการไมโครซอฟต์ทั่วโลก
เมื่อวันที่ 12 พฤษภาคมที่ผ่านมา โดยมัลแวร์ดังกล่าวถูกสร้างขึ้นมาเพื่อก่อความเสียหายแก่ผู้ใช้คอมพิวเตอร์
ซึ่งจะถูกส่งมายังคอมพิวเตอร์ของผู้ใช้โดยไม่มีข้อมูลใด ๆ ของผู้ส่ง เมื่อผู้ใช้เปิดไฟล์ หรือดาวน์โหลด
ตัวมัลแวร์จะทำงานด้วยการบล็อกไฟล์เอกสารต่าง ๆ ในคอมพิวเตอร์ของผู้ใช้ด้วยการเข้ารหัสลับ
ซึ่งผู้ใช้จะไม่สามารถเปิดหรือดาวน์โหลดข้อมูลที่อยู่ในคอมพิวเตอร์ของตัวเองได้เลย
ปัจจุบันมีคอมพิวเตอร์ที่ถูกระบบ WannaCry นี้ เข้าบล็อกข้อมูลแล้วกว่า 1 แสนเครื่องทั่วโลก
โดยเฉพาะในประเทศอังกฤษ โรงพยาบาลกว่า 10 แห่ง ไม่สามารถเปิดบริการได้
เนื่องจากคอมพิวเตอร์ถูกมัลแวร์ดังกล่าวเล่นงาน ตัว WannaCry หรือ มัลแวร์เรียกค่าไถ่นี้
เมื่อคอมพิวเตอร์ของผู้ใช้คนใดกลายเป็นเหยื่อ หากต้องการที่จะปลดล็อกจะต้องจ่ายเงินประมาณ 300 ดอลลาร์
หรือประมาณ 10,500 บาท และจะเพิ่มมูลค่าขึ้นไปเรื่อย ๆ เพื่อเป็นการไถ่ข้อมูลคืนในรูปแบบของ Bit Coin
ไม่เช่นนั้นก็ไม่สามารถเปิดไฟล์เอกสารต่าง ๆ ได้

น.อ.สมศักดิ์ฯ กล่าวต่อไปว่า รัฐบาลมีความเป็นห่วงกรณีดังกล่าว โดยพลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี
ได้สั่งการให้กระทรวงดิจิทัลฯ เร่งติดตามเฝ้าระวังปัญหาที่อาจจะเกิดขึ้นอย่างใกล้ชิด ซึ่ง ดร.พิเชฐ ดุรงคเวโรจน์
รัฐมนตรีว่าการกระทรวงดิจิทัลฯ ได้มอบหมายให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA
ดำเนินการแจ้งเตือนและให้คำแนะนำแก่ผู้ใช้คอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานในทันที
รวมทั้งติดตามเฝ้าระวังและเตรียมพร้อมให้ความช่วยเหลือผู้ใช้คอมพิวเตอร์หรือผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานต่างๆ อย่างทันการณ์ตลอดเวลา
ซึ่งในส่วนของประเทศไทยขณะนี้ยังไม่พบความเสียหายที่ร้ายแรงจากการติดมัลแวร์ดังกล่าวแต่อย่างใด

อย่างไรก็ตาม สิ่งที่ผู้ใช้คอมพิวเตอร์หรือผู้ดูแลระบบของหน่วยงานต้องดำเนินการในเบื้องต้น คือ
การป้องกันไม่ให้มัลแวร์ดังกล่าวเข้ามาอยู่ในคอมพิวเตอร์ของเราด้วยการไม่เปิดไฟล์เอกสารแนบของอีเมล์โดยไม่จำเป็น และควรตรวจสอบแหล่งที่มาของไฟล์ที่ถูกส่งเข้ามาในอีเมล์ หรือช่องทางต่าง ๆ ให้แน่ใจก่อนเปิดอ่าน
ที่สำคัญควรปรับปรุงระบบปฏิบัติการคอมพิวเตอร์ หรือ OS ของระบบวินโดว์ (Windows) ให้เป็นเวอร์ชั่นล่าสุด
รวมทั้งควรสำเนาข้อมูลสำคัญต่าง ๆ ไว้ในฮาร์ดดิสต์อื่น (External Hardisk) อยู่เสมอ เพื่อเป็นการสำรองข้อมูล

สำหรับแนวทางการป้องกันการแพร่ระบาดนั้น

กรณีผู้ใช้งานทั่วไปเมื่อผู้ใช้พบว่าคอมพิวเตอร์ติดมัลแวร์ดังกล่าวแล้ว
ให้ปิดเครื่องและแจ้งผู้ดูแลระบบของหน่วยงาน
หรือแจ้งศูนย์ OCC (Online Complaint Center) โทร. 1212
สำหรับผู้ดูแลระบบคอมพิวเตอร์ให้ปิดบริการ SMBv1 ที่ Windows servers
และปิดการเข้าถึง พอร์ต TCP/UDP 135-139 และ TCP 445 ที่อุปกรณ์ Firewall
โดยสามารถติดต่อ ThaiCERT ETDA โ ทร. 0 2123-1212 ได้ตลอด 24 ชม.

ที่มา : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม