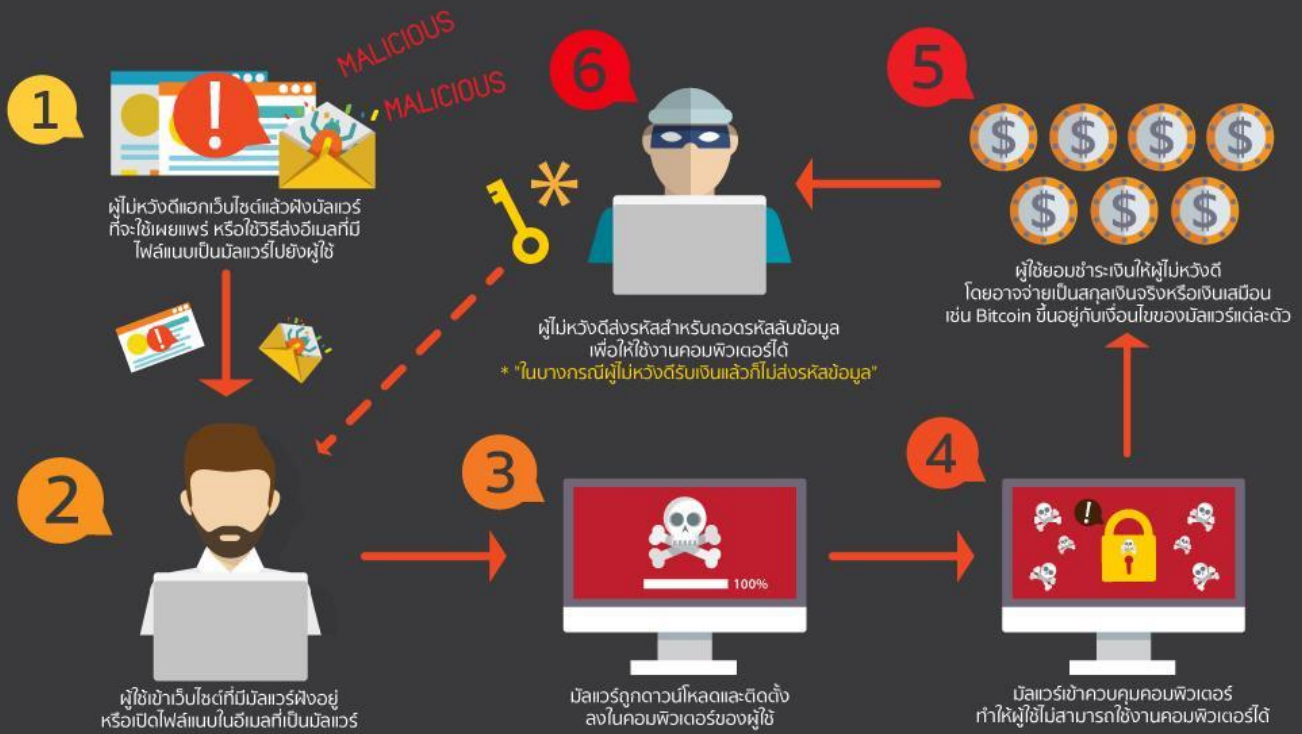


เตือนระวัง!! เปิดอีเมล เจอมัลแวร์เรียกค่าไถ่ระบาด

ThaiCERT แจ้งเตือนและขอแนะนำ วิธีป้องกันความเสียหายจาก Ransomware

รูปแบบการโจมตีของ Ransomware เพื่อยึดข้อมูลในเครื่องคอมพิวเตอร์ของเหยื่อ



ขอแนะนำในการป้องกันความเสียหายจากภัย Ransomware

ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล



สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ



ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ

สร้างความระมัดระวังในการใช้อีเมลและเปิดเว็บไซต์



ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย



ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

ในกรณีที่เกิดเป็นเหยื่อ



ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่



ให้ติดต่อกับเจ้าหน้าที่ IT ของหน่วยงานในทันที

การเรียกค่าไถ่ของมัลแวร์ Ransomware คืออะไร?

นี่ก็เป็นภาพง่ายๆว่า มัลแวร์ Ransomware ได้จับไฟล์ข้อมูลในคอมพิวเตอร์ที่สำคัญ และจับคอมพิวเตอร์ของเราเป็นตัวประกัน แล้วส่งจดหมายทางอีเมลเรียกค่าไถ่ ว่าถ้าคุณอยากได้ไฟล์สำคัญในเครื่องนี้คืน คุณจะต้องจ่ายเงินถ้าไม่จ่ายก็จะเปิดไฟล์ไม่ออก ไม่สามารถใช้ไฟล์นั้นได้ เท่านั้นยังไม่พอ หากคุณต่อเน็ต หรือเสียบ Extranal Harddisk หรือ USB Flash Drive เข้ากับคอมพิวเตอร์ที่ติดไวรัส ละก็ ไฟล์ในหน่วยความจำพกพาของคุณก็จะถูกล็อกเข้ารหัสด้วย

รูปแบบการโจมตี

ส่วนใหญ่จะมาทางอีเมลหลอกลวงที่แนบไฟล์มัลแวร์อยู่ มัลแวร์นี้มุ่งโจมตีคอมพิวเตอร์ระบบปฏิบัติการ Windows , MAC , Android , iOS โดยจะทิ้งไฟล์ไฟล์หนึ่งไว้ในโฟลเดอร์ที่ติดมัลแวร์ ที่มีการเข้ารหัสไว้ อีเมลที่ว่ามันมาในรูปแบบที่หลากหลาย เช่น มาแบบแจ้งเตือนว่า มีของมาส่งถึงคุณ.... เช่น FedEx , DHL ปลอมหน้าจดหมายเหมือนของจริง จนแยกไม่ออก เมื่อคลิกไฟล์แนบของอีเมลนั้น หรือคลิกที่ลิงค์ มันจะดาวน์โหลดไฟล์ exe ที่มีมัลแวร์ติดตั้งทันที บัญชีคุณโดนล็อก !!!!! Accounts Suspended !

วิธีป้องกันไม่ให้เกิดเป็นเหยื่อ

1. ให้สำรองข้อมูลสำคัญ ที่ใช้งานอย่างสม่ำเสมอ ไว้ที่อื่นด้วยเช่น flashdrive , external hard disk , คอมเครื่องอื่น
2. ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus)
3. หากเจอเมลที่เราไม่รู้จัก และส่งอะไรมาไม่รู้ ไม่ควรคลิกเปิดอ่านและควรลบจดหมายทิ้งทันที

หากคุณโดนมัลแวร์ แบบนี้แล้วต้องทำอะไร?

๑. ตัดการเชื่อมต่อกับเครือข่าย ห้ามเสียบ Flash Drive หรือ External Hard disk และห้ามต่อเน็ตเข้ากับคอมพิวเตอร์ที่ติดไวรัส เด็ดขาด เพราะหากเสียบหรือต่อเน็ตจะ เป็นการกระจายไปยังเครื่องอื่น และทำให้เครื่องอื่นในเครือข่าย ได้รับผลกระทบหนักขึ้นด้วย
๒. ให้ติดต่อ เจ้าหน้าที่ IT ทันที (โทร. ๒๓๑๙, ๒๓๔๐)