เตือนภัยมัลแวร์ CTB Locker

เรียกค่าไถ่ผู้ใช้งานในการกู้ไฟล์ที่ถูกเข้ารหัสลับ

เนื่องจากขณะนี้ มีภัยมัลแวร์ CLB Locker ที่พบการแพร่ระบาดหนักทั่วโลกในช่วงนี้ ซึ่งอาจมีผลกระทบกับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพวง **ส่วนมาตรฐานเทคโนโลยีสารสนเทศ *(มส.)*** ขอให้พนักงานใช้อีเมลอย่างระมัดระวัง

การติดมัลแวร์ CTB Locker มีผู้ไม่ประสงค์ดีทำการส่งอีเมลพร้อมแนบไฟล์นามสกุล .zip มายังผู้ใช้งาน เมื่อผู้ใช้งานคลิกเปิดไฟล์ .zip ดังกล่าว จะทำให้เกิดการติดมัลแวร์ทันที โดยมีจุดประสงค์ในการเข้ารหัสลับไฟล์เอกสารประเภทต่างๆ บนเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์ เช่น .pdf, .xls, .ppt, .txt, .wb2. .jpg, .odb, .md. .js, .pl, .doc เป็นต้น

หลังจากติดมัลแวร์ CTB Locker จะพบหน้าต่างแสดงข้อมูลของการเรียกค่าไถ่กับผู้ใช้งานที่เป็นเจ้าของไฟล์ดังกล่าว ในการถอดรหัสลับไฟล์ข้อมูลทั้งหมดที่ถูกเข้ารหัสไว้ เจ้าของไฟล์จะต้องเสียเงินเป็นจำนวนประมาณ 630 ดอลล่าร์สหรัฐ (คิดเป็นเงินไทยประมาณ 20,000 บาท) จ่ายให้กับผู้ไม่ประสงค์ดี จากนั้นผู้ไม่ประสงค์ดีจึงจะส่งซอฟต์แวร์และกุญแจที่ใช้ในการถอดรหัสลับไฟล์กลับมา แต่ยังไม่มีใครสามารถการันตีได้ว่าการจ่ายเงินแล้วจะทำให้สามารถได้ข้อมูลกลับคืนมาได้จริงอย่างที่อ้างไว้หรือไม่

ข้อแนะนำในการแก้ไขและป้องกัน

1. ไม่คลิกลิ้งก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย หากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือหรือไม่ ให้สอบถามจากผู้ส่งโดยตรง
2. แยกเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ออกจากระบบ และไม่เชื่อมต่อ External Drive กับเครื่องดังกล่าว
3. สำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ
4. หากมีความต้องการใช้งานคอมพิวเตอร์นั้นอีกครั้ง ให้ทำการ Format ข้อมูลในเครื่องและติดตั้งระบบปฏิบัติการใหม่
5. ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส รวมถึงอัปเดตโปรแกรมอื่นๆ โดยเฉพาะโปรแรมที่มักมีปัญหาเรื่องช่องโหว่อยู่บ่อยๆ เช่น Java และ Adobe Reader รวมถึงอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ
6. หากมีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิ์ในการเข้าถึงแต่ละส่วน และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์อ่านหรือแก้ไขเฉพาะไฟล์ที่มีความจำเป็นต้องใช้สิทธิ์เหล่านั้น

ส่วนมาตรฐานเทคโนโลยีสารสนเทศ *(มส.)* จึงขอความร่วมมือเพื่อนพนักงานทุกท่านปฏิบัติตามคำสั่ง ทีโอที ที่ รบ.9/2554 เรื่อง การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างเคร่งครัด เพื่อป้องกันชื่อเสียง ภาพพจน์ และผลกระทบที่อาจจะเกิดขึ้นกับการดำเนินงานของ ทีโอที

โดยสามารถเรียกดูรายละเอียดเพิ่มเติมได้ที่เว็บไซต์ security.intra.tot.co.th

หากมีข้อสงสัยหรือต้องการแสดงความคิดเห็นติดต่อได้ที่ โทร. 0 2505 1081

################

3 **พฤษภาคม 2558**