# สถานการณ์การโจมตี

# ลักษณะการติด

ไฟล์แนบในอีเมลล์ (e-mail attachment)



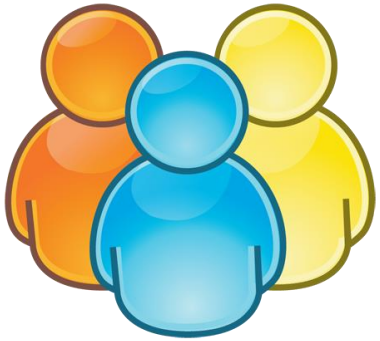
# จุดประสงค์

๑.เข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดที่ใช้งาน

๒.การแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์

# คำแนะนำ/แนวทางป้องกัน

- ผู้ดูแลระบบ(ADMIN)
- ผู้ใช้งาน(USERS)

# คำแนะนำ/แนวทางป้องกัน

๑. การทำสำรองข้อมูล (Backup Data)

๒. หมั่นปรับปรุงระบบปฏิบัติการ เช่น Patch MS Windows และซอฟต์แวร์ใช้งานต่าง ๆ ให้เป็น Version ปัจจุบัน

๓. ติดตั้ง Anti-Virus Computer หรือ Anti-Malware ในเครื่องคอมพิวเตอร์

๔. ระวังการหลอกลวงให้ Click ไฟล์ต่าง ๆ ที่แนบมากับ e-Mail หรือทุกช่องทางจาก Internet

๕. การติด Ransomware แล้ว และมีข้อความขึ้นให้ชำระหรือโอนเงิน เพื่อรับรหัสปลดล็อคไฟล์หรือคอมพิวเตอร์ก็ห้ามอย่างเด็ดขาด เพราะไม่ได้หมายความว่าจะได้รับรหัสที่สามารถปลอดล็อคได้

# ข้อแนะนำในการป้องกันความเสียหายจากภัย Ransomware

**ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล**

สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ

ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ

**สร้างความตระหนักในการใช้อีเมลและเปิดเว็บไซต์**

ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย

ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

**ในกรณีที่ตกเป็นเหยื่อ**

ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่

ให้ติดต่อกับเจ้าหน้าที่ IT ของหน่วยงานในทันที

ThaiCERT

ThaiCERT

thaicert.or.th

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
www.etda.or.th

ICT
Smart Thailand

# คำแนะนำ/แนวทางป้องกัน

๑. ไม่เปิดเอกสารแนบอีเมลล์โดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมลล์ ควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลล์ฉบับนั้นมาจริง

๒. ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบัน เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware

# ระบบป้องกันของ บก.ทท.

๑. ระบบป้องกันไวรัสหรือมัลแวร์คอมพิวเตอร์ (Antimalware) ศทส.สส.ทหาร ให้บริการติดตั้งกับเครื่องคอมพิวเตอร์ของส่วนราชการ บก.ทท. จำนวน ๒,๐๐๐ license

๒. ระบบ Anti-APT ที่ติดตั้งในระบบเครื่องข่ายของ บก.ทท. ซึ่งถ้ามีการแพร่ระบาดทางเครือข่าย ระบบจะทำการกักไว้ในระบบ

๓. การแจ้งเตือนผู้ใช้งาน (cyber awareness)