

# สถานการณ์การโจมตี

## WannaCry Ransomware Attack

Patch for Unsupported Windows (**Apply Now**)



# ลักษณะการติด

ไฟล์แนบในอีเมล (e-mail attachment)



# จุดประสงค์

๑. เข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดที่ใช้งาน
๒. การแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดวส์



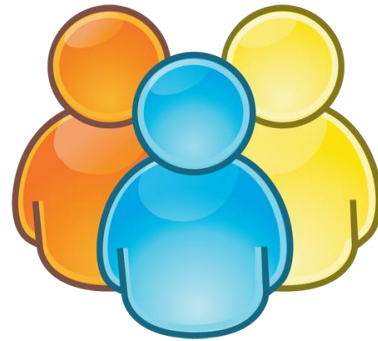
The screenshot shows the Wana Decrypt0r 2.0 ransomware interface. The window title is "Wana Decrypt0r 2.0". The main message reads: "Ooops, your files have been encrypted!". Below this, there is a large padlock icon. The interface is divided into several sections:

- Payment will be raised on:** 1/4/1970 00:00:00. Time Left: 00:00:00:00.
- Your files will be lost on:** 1/8/1970 00:00:00. Time Left: 00:00:00:00.
- How Do I Pay?:** Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday. Once the payment is checked, you can start decrypting your files immediately.
- Contact:** If you need our assistance, send a message by clicking <Contact Us>.
- Bitcoin Address:** Send \$600 worth of bitcoin to this address: [Redacted Address] [Copy]
- Buttons:** Check Payment, Decrypt.

At the bottom left, there are links for "About bitcoin", "How to buy bitcoins?", and "Contact Us".

# 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. ระมัดระวังการหลอกลวงให้ Click ไฟล์ต่าง ๆ ที่แนบมากับ e-Mail หรือทุกช่องทางจาก Internet
๕. การติด Ransomware แล้ว และมีข้อความขึ้นให้ชำระหรือ โอนเงิน เพื่อรับรหัสปลดล็อคไฟล์หรือคอมพิวเตอร์ก็ห้ามอย่างเด็ดขาด เพราะไม่ได้หมายความว่า จะได้รับรหัสที่สามารถปลดล็อคได้

# ข้อเสนอแนะในการป้องกันความเสียหายจากภัย Ransomware

ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล



สำรองข้อมูลสำคัญที่ใช้ทำงานอย่างสม่ำเสมอ



ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ

สร้างความระมัดระวังในการใช้อีเมลและเปิดเว็บไซต์



ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย



ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

ในกรณีที่เกิดเป็นเหยื่อ



ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่



ให้ติดต่อกับเจ้าหน้าที่ IT ของหน่วยงานในทันที

## คำแนะนำ/แนวทางป้องกัน

๑. ไม่เปิดเอกสารแนบอีเมลล์โดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมลล์ ควรตรวจสอบกับผู้ส่งก่อนว่า ได้ส่งอีเมลล์ฉบับนั้นมาจริง
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 ที่ติดตั้งในระบบเครือข่ายของ บก.ทท. ซึ่งถ้ามีการแพร่ระบาดทางเครือข่าย ระบบจะทำการกักไว้ในระบบ
๓. การแจ้งเตือนผู้ใช้งาน (cyber awareness)

