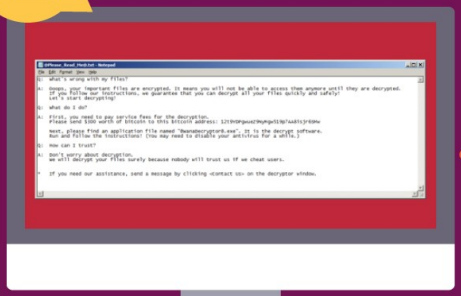
กระทรวงดีอี

เตือนภัยมัลแวร์เรียกค่าไถ่ WannaCry

กระจายผ่านช่องโหว่ของวินโดว์ รีบอัปเดตทันที

เมื่อวันที่ 12 พฤษภาคม 2560 บริษัท Avast ได้เผยแพร่รายงานการพบมัลแวร์เรียกค่าไถ่ชื่อ WannaCry ซึ่งมีจุดประสงค์เพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดที่ใช้งาน รวมถึงสามารถกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์ที่เกี่ยวข้องกับบริการแชร์ไฟล์ผ่านเครือข่าย (SMB) ที่มีการเปิดให้บริการ

1

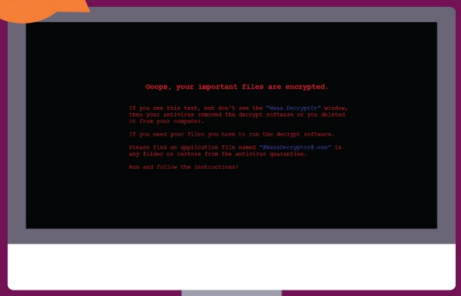


มัลแวร์ถูกดาวน์โหลด
และติดตั้งลงในคอมพิวเตอร์ของผู้ใช้
และแสดงการเรียกค่าไถ่

2

ค่าไถ่ที่ถูกเรียกคือ บิตคอยน์
300 ดอลลาร์ โดยแนะนำ
วิธีการจ่ายค่าไถ่ อธิบายสิ่งที่เกิดขึ้น
และการนับถอยหลัง

3



วอลล์เปเปอร์ของผู้ที่ตกเป็นเหยื่อ

ถึงแม้ทางผู้พัฒนาจะออกเวอร์ชันรุ่นอัปเดตช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แล้วแต่ก็ยังพบว่ามีผู้เสียหายในระดับองค์กรทั่วโลกที่ได้รับผลกระทบจากการโจมตีช่องโหว่ดังกล่าวและฝังมัลแวร์เรียกค่าไถ่ WannaCry เอาไว้

สำหรับประเทศไทยมีการตรวจพบข้อมูลในสื่อสังคมออนไลน์ของผู้ใช้งานท่านหนึ่งที่โพสต์ข้อมูลว่าตนเองโดนมัลแวร์ดังกล่าวเช่นกัน แต่ยังไม่ทราบว่าเป็นความเสียหายระดับใดและกระทบกับหน่วยงานใดโดยปัจจุบัน ไทยเซิร์ต ETDA กำลังประสานเพื่อให้คำแนะนำถึงกรณีดังกล่าว

แนวทางการป้องการการติด Ransomware WannaCry

1. ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น
หากจำเป็นต้องเปิดเอกสารแนบอีเมล
ควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมล
ฉบับนั้นมาจริง

2. ปรับปรุงระบบปฏิบัติการ
Microsoft Windows ให้เป็นปัจจุบัน
เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่ง
เป็นช่องทางให้คอมพิวเตอร์ติด
Ransomware

แนวทางการป้องกันการแพร่กระจาย (หากพบการติด Ransomware แล้ว)

สำหรับผู้ใช้งานทั่วไป

ให้ปิดเครื่องและแจ้งเจ้าหน้าที่
ผู้ดูแลระบบ หรือเจ้าหน้าที่
ไทยเซิร์ต ETDA ที่หมายเลข
02 123 1212 (24x7)

สำหรับผู้ดูแลระบบ

ปิดบริการ SMBv1
ที่ Windows servers

ปิดการเข้าถึงพอร์ต
TCP/UDP 135-139
และ TCP 445
ที่อุปกรณ์ Firewall