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

ThaiCERT ThaiCERT thaicert.or.th

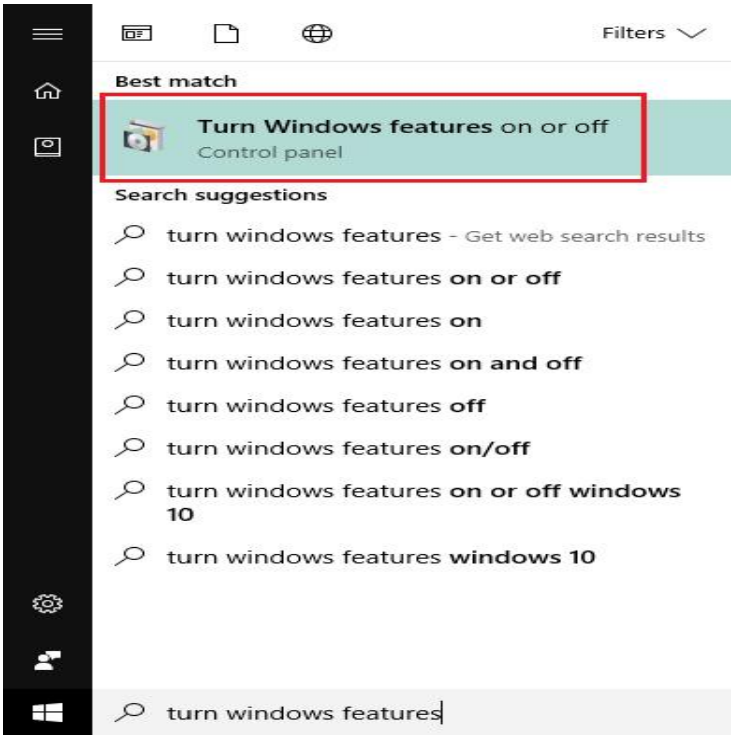
ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA

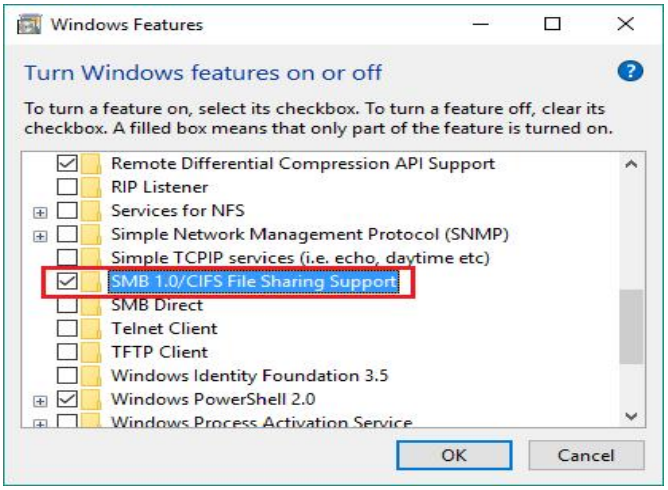
แนวทางการป้องกันมัลแวร์เรียกค่าไถ่ WannaCry

1. สำรองข้อมูลในเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ โดยทำการสำรองข้อมูลในอุปกรณ์ External Harddisk, Handy Drive และอุปกรณ์สำรองอื่นๆ
2. ไม่เปิด E-mail หรือไฟล์บนเอกสารที่มาพร้อมกับ E-mail ที่ไม่รู้จัก
3. ระมัดระวังการ Download โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การ Download การ Upload โปรแกรมต่างๆ ต้องตรวจสอบความถูกต้องและปลอดภัยก่อนนำไปใช้งาน
4. ไม่เข้าเว็บไซต์ที่ไม่มีความน่าเชื่อถือ
5. การอัพเดทระบบปฏิบัติการเพื่ออุดช่องโหว่
6. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทฐานข้อมูลไวรัสให้เป็นปัจจุบัน
7. ปิดการใช้งาน SMBv1 (Server Message Block Version1) ซึ่งเป็นโปรโตรคอลในการแชร์ไฟล์ ปัจจุบัน SMB มี 3 เวอร์ชันด้วยกัน คือ SMBv1, SMBv2 และ SMBv3 โดย SMBv1 เป็นรุ่นเก่ามากออกมาเกือบ 30 ปีแล้ว ซึ่ง WannaCry ก็ใช้ช่องโหว่ของ SMBv1 เป็นช่องทางแพร่ตัวเองเข้าโจมตีคอมพิวเตอร์เครื่องอื่นในเครือข่าย โดยที่เครื่องเป้าหมายไม่ต้องคลิกเปิดไฟล์ ดังนั้น SMBv1 จึงไม่มีความปลอดภัยที่จะใช้งาน ซึ่งมีขั้นตอนการปิดดังนี้

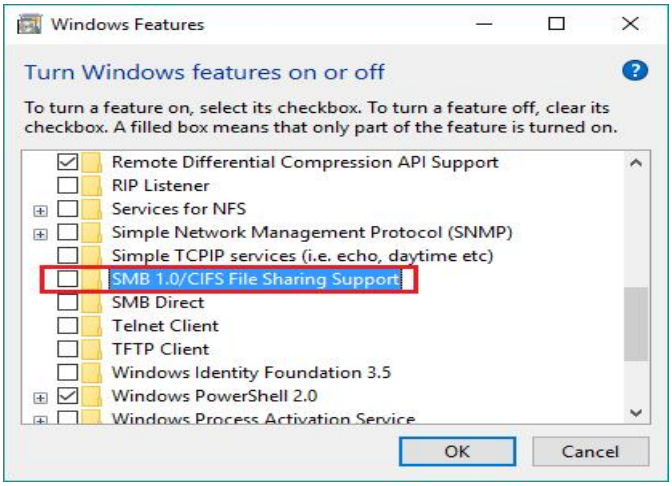
    1. คลิก **Start**
    2. พิมพ์ในช่อง Search ว่า "turn windows features" แล้วคลิกที่ **"Turn Windows features on or off"** ตามภาพ



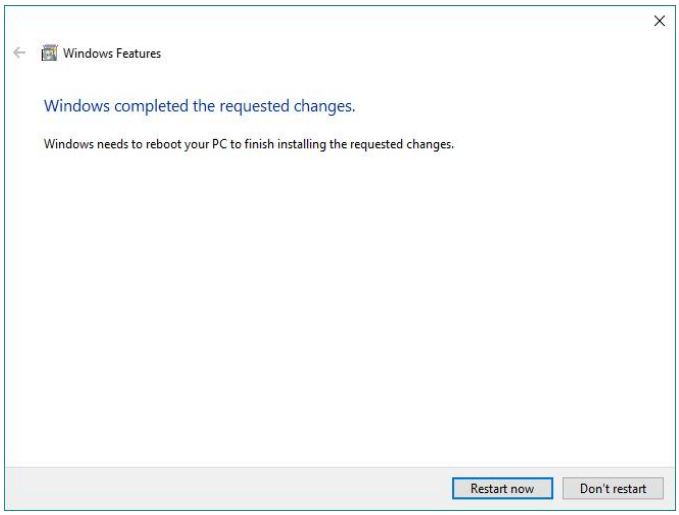
3. หน้าต่าง **Windows Features** จะเปิดขึ้นมา ให้เลื่อนลงไปล่างๆ หาข้อความ **"SMB 1.0/CIFS File Sharing Support"** โดยฟีเจอร์นี้จะถูกเปิดไว้เป็นค่าเริ่มต้น



4. ให้คลิกเครื่องหมายถูกออกจากช่องสี่เหลี่ยม และกด OK

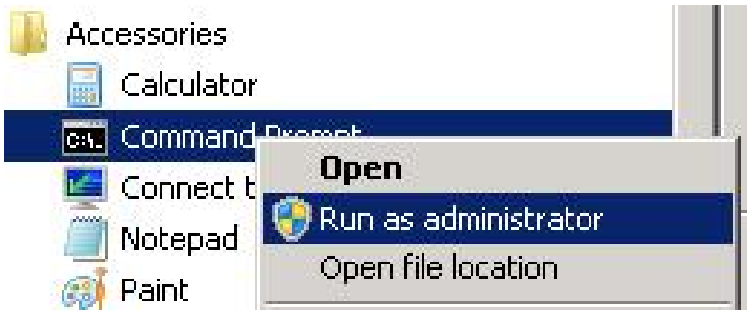


5. ให้ทำการรีสตาร์ทเครื่องคอมพิวเตอร์



ในระบบปฏิบัติการ Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 และ Windows Server 2012 โดยผ่าน Command Prompt ดังนี้

1. เปิด elevated command prompt โดยการคลิกขวาที่ Command Prompt แล้วคลิก Run as administrator



2. พิมพ์คำสั่งด้านล่าง ทีละบรรทัด

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start= disabled
```

3. ให้ทำการรีสตาร์ทเครื่องคอมพิวเตอร์

หากพบเหตุความผิดปกติใดๆ ที่เกี่ยวข้อง สามารถแจ้งกลับมายังกลุ่มระบบเครือข่ายคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ติดต่อนายชูศักดิ์ จันทะเดช นายไชยรัต กุลไพจิตร นายสมัฐการณ์ งามพัฒนพงศ์ชัย และนายณัฐพล งามดี หรือทาง E-mail : netgrp@cad.go.th หมายเลขโทรศัพท์ 0 2281 2714, 0 2628 5240 - 59 ต่อ 2356 และ 2357
