แนวทางการป้องกัน
Wanna Cry มัลแวร์เรียกค่าไถ่คอมพิวเตอร์

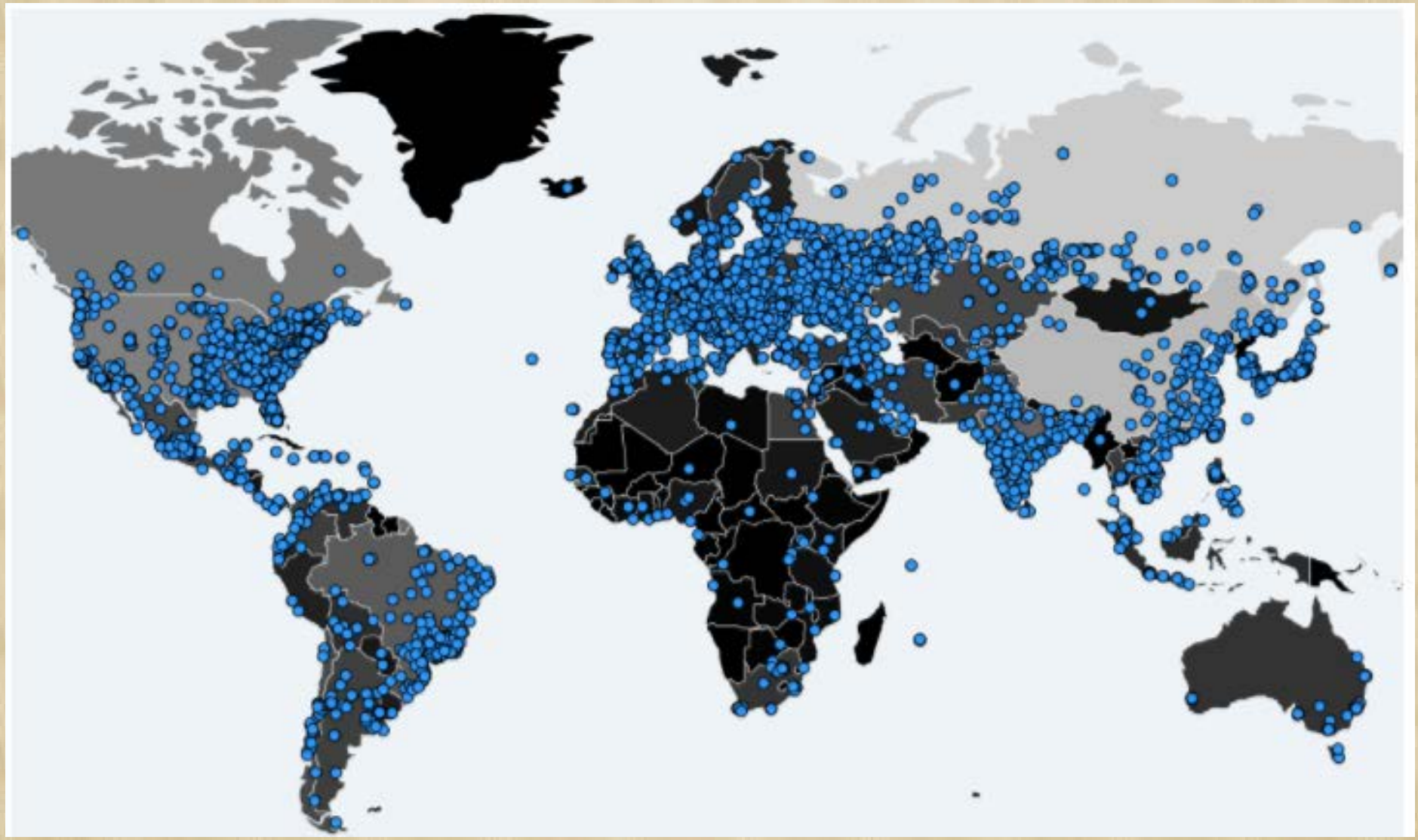
งาน 7 เทคโนโลยีสารสนเทศและการสื่อสาร ฝอ.ภ.จว.อุบลราชธานี

มัลแวร์ Wanna Cry

เมื่อเดือนสิงหาคม 2016 กลุ่มแฮกเกอร์ที่เรียกตัวเองว่า The Shadow Broker สามารถเข้าถึงเครื่องมือระดับสูงที่คาดว่าเป็นของ NSA โดยเรียกร้องเงิน 1 ล้านเหรียญสหรัฐ แต่ไม่มีหน่วยงานไหนยอมจ่ายจึงปล่อยเครื่องมือและช่องโหว่เหล่านี้ทั้งหมดออกสู่สาธารณะในช่วงเมษายน 2017

หนึ่งในช่องโหว่สำคัญที่หลุดออกมาด้วยเรียกว่า EternalBlue ซึ่งเจาะ SMBv1 (Microsoft Server Message Block) ใน Windows ทำให้สามารถควบคุมเครื่องได้ ซึ่ง Microsoft ก็รู้เรื่องนี้ (คาดว่า NSA รีบแจ้งหลังโดนเจาะไป) จึงออกอัพเดทเพื่อปิดช่องโหว่ตั้งแต่เดือนมีนาคมที่ผ่านมา

ประเทศที่ถูกมัลแวร์ Wanna Cry โจมตี



หน้าจอคอมพิวเตอร์เมื่อโดนมัลแวร์เรียกค่าไถ่ WannaCry

ผลกระทบเมื่อถูกโจมตี

ความร้ายกาจของ WannaCry

คือจะเข้ารหัสไฟล์สำคัญทั้งหมดของเครื่อง เช่น

.docx, .pptx, .mpeg, .zip, .backup

แล้วเรียกค่าไถ่เป็นเงิน $300 ผ่านทาง Bitcoin

ซึ่งแน่นอนว่าเหยื่อสามารถกดทดลองกู้ไฟล์คืนได้ถ้าไม่แน่ใจ และมีตัวเลขเวลาบอกว่าไฟล์ทั้งหมดในเครื่องจะถูกลบเมื่อไหร่ถ้าไม่จ่ายเงิน

ข้อแนะนำในการป้องกัน

การป้องกัน

1. ขั้นแรก

อัพเดต Windows ให้ล่าสุดเสมอ เพื่ออุดช่องโหว่ และช่วยลดความเสี่ยงในการถูกโจมตี

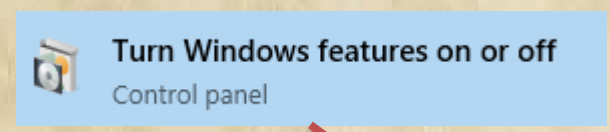
การป้องกัน

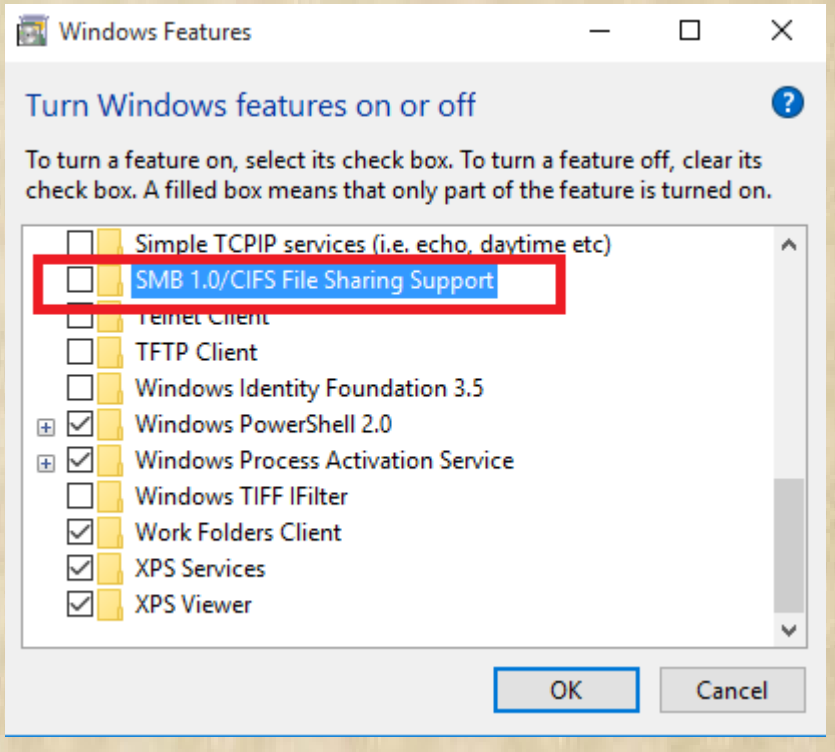
2. ปิดโปรโตคอล Server Message Block (SMB)

SMB คือโปรโตคอลในการรับส่งไฟล์ระหว่างคอมพิวเตอร์ที่อยู่ในเครือข่ายเดียวกัน ซึ่ง SMB นั้นจะมี 3 เวอร์ชั่น คือ SMBv1, SMBv2 และ SMBv3 แต่ SMBv1 นั้นเป็นรุ่นเก่ามาก 30 ปีมาแล้ว และนี่เองไอ้เจ้า WannaCry ได้ใช้ช่องโหว่ของ SMBv1 ในการเข้าโจมตีคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย จึงทำให้ SMBv1 นั้นไม่เหมาะสมที่จะใช้งาน

2.1 ปิด SMB สำหรับ Windows 8.1, Windows 10

- คลิก **Start**
- พิมพ์ในช่อง Search ว่า “turn windows features” แล้วคลิกที่ “Turn Windows features on or off”

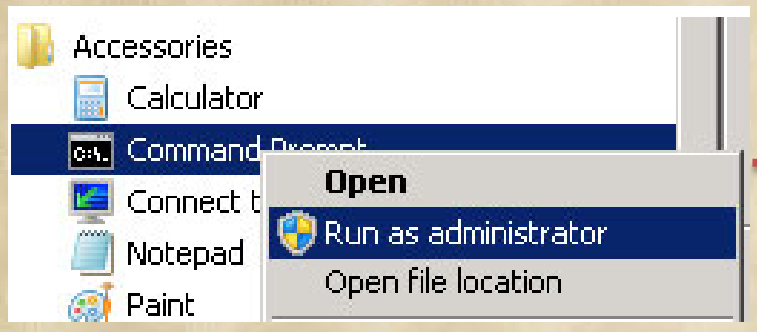


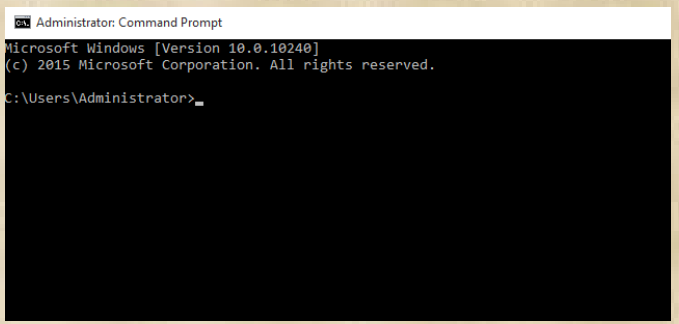


- กด OK แล้วก็ **Restart now**

2.2 ปิด SMB สำหรับ Vista, 7

- ไปที่ Start – All program – Accessories
- คลิกขวาที่ Command Prompt แล้วคลิก Run as administrator





พิมพ์คำสั่งด้านล่างนี้ทีละบรรทัด

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

sc.exe config mrxsmb10 start= disabled
```

- รีสตาร์ทเครื่อง

2.3 อัพเดทแพทช์กรณีพิเศษสำหรับ Windows XP

ดาวน์โหลดไฟล์ติดตั้ง

http://www.catalog.update.microsoft.com/search.aspx?q=4012598

Microsoft®Update Catalog

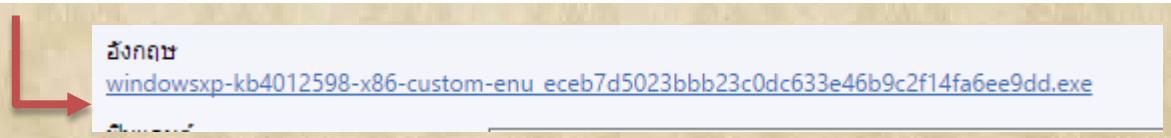
4012598 ค้นหา

คำถามที่ถามบ่อย | วิธีใช้

ผลลัพธ์การค้นหาสำหรับ "4012598"

การปรับปรุง: 1 - 13 จาก 13 (หน้า 1 จาก 1) ก่อนหน้า | ถัดไป

ชื่อเรื่อง	ผลิตภัณฑ์	การจำแนกประเภท	ปรับปรุงล่าสุด	รุ่น	ขนาด	
Security Update for Windows XP SP3 (KB4012598)	Windows XP	Security Updates	13/5/2560	n/a	15.7 MB	ดาวน์โหลด
Security Update for Windows Server 2008 (KB4012598)	Windows Server 2008	Security Updates	12/3/2560	n/a	1.2 MB	ดาวน์โหลด
Security Update for Windows Server 2003 for x64-based Systems (KB4012598)	Windows Server 2003,Windows Server 2003, Datacenter Edition	Security Updates	13/5/2560	n/a	10.3 MB	ดาวน์โหลด
โปรแกรมปรับปรุงความปลอดภัยสำหรับ Windows 8 (KB4012598)	Windows 8	Security Updates	13/5/2560	n/a	872 KB	ดาวน์โหลด
Security Update for Windows XP SP3 for XPe (KB4012598)	Windows XP Embedded	Security Updates	13/5/2560	n/a	15.7 MB	ดาวน์โหลด
Security Update for Windows Server 2003 (KB4012598)	Windows Server 2003,Windows Server 2003, Datacenter Edition	Security Updates	13/5/2560	n/a	12.1 MB	ดาวน์โหลด
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	Windows XP x64 Edition	Security Updates	13/5/2560	n/a	1.9 MB	ดาวน์โหลด
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598)	Windows Server 2008	Security Updates	12/3/2560	n/a	1.2 MB	ดาวน์โหลด
โปรแกรมปรับปรุงความปลอดภัยสำหรับ Windows Vista (KB4012598)	Windows Vista	Security Updates	12/3/2560	n/a	1.2 MB	ดาวน์โหลด
Security Update for Windows Server 2008 for x64-based Systems (KB4012598)	Windows Server 2008	Security Updates	12/3/2560	n/a	1.3 MB	ดาวน์โหลด
โปรแกรมปรับปรุงความปลอดภัยสำหรับ WES09 และ POSReady 2009 (KB4012598)	Windows XP Embedded	Security Updates	12/3/2560	n/a	15.7 MB	ดาวน์โหลด
โปรแกรมปรับปรุงความปลอดภัยสำหรับ Windows 8 สำหรับระบบที่ใช้ x64 (KB4012598)	Windows 8	Security Updates	13/5/2560	n/a	984 KB	ดาวน์โหลด
โปรแกรมปรับปรุงความปลอดภัยสำหรับ Windows Vista สำหรับระบบที่ใช้ x64 (KB4012598)	Windows Vista	Security Updates	12/3/2560	n/a	1.3 MB	ดาวน์โหลด



- ติดตั้งไฟล์แพทช์

การป้องกัน

3. ลงโปรแกรมป้องกัน WannaCry Block

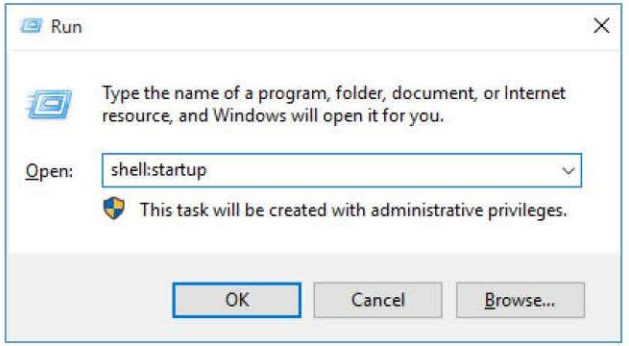
โปรแกรม WannaCry Block พัฒนาโดยห้องปฏิบัติการวิจัยไอยราคลัสเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี ใช้ป้องกันไม่ให้แรนซัมแวร์ WCry ทำงานได้ รวมถึงปิดช่องทางการเผยแพร่ในเครื่องข่ายด้วย ดาวน์โหลดที่ลิงค์นี้

https://github.com/chanwit/wannacry_blocker/releases/download/v5/block_wannacry_v5.zip

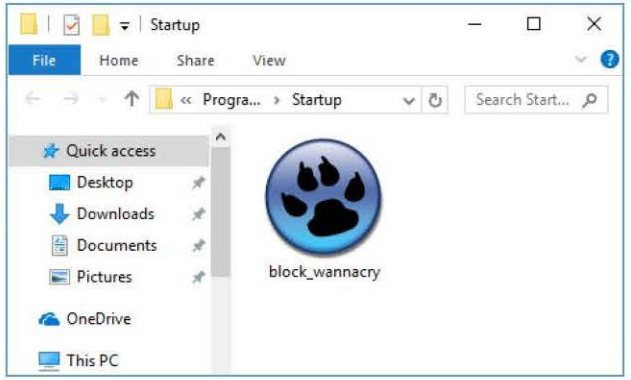
การป้องกัน

1.กดปุ่ม Win+R ที่คีย์บอร์ด

2.พิมพ์ shell:startup



3.นำโปรแกรมมาวางที่โฟลเดอร์นี้



เมื่อดาวน์โหลดโปรแกรมแล้วให้แตกไฟล์แล้วนำไปวางไว้ที่โฟลเดอร์ Startup

ข้อแนะนำในการแก้ไขหากตกเป็นเหยื่อ

ข้อแนะนำในการแก้ไขหากตกเป็นเหยื่อ

1. หากพบว่าเครื่องคอมพิวเตอร์ตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่ WannaCry ให้ตัดการเชื่อมต่อเครือข่าย (ถอดสาย LAN, ปิด Wi-Fi) และปิดเครื่องทันที

2. ใช้เครื่องคอมพิวเตอร์ที่ไม่ได้ติดมัลแวร์ ดาวน์โหลดไฟล์อัพเดตฐานข้อมูล (Definition) ล่าสุดของโปรแกรมแอนติไวรัสที่ติดตั้งในเครื่อง เพื่อนำมาอัปเดตแบบ offline หากใช้งาน Windows Defender สามารถดาวน์โหลดฐานข้อมูลล่าสุดได้จากเว็บไซต์ Microsoft https://www.microsoft.com/en-us/security/portal/definitions/adl.aspx

3. รีสตาร์ทเครื่องเข้า Safe Mode

4. อัพเดตฐานข้อมูลแอนติไวรัส และสั่งสแกนเพื่อลบมัลแวร์