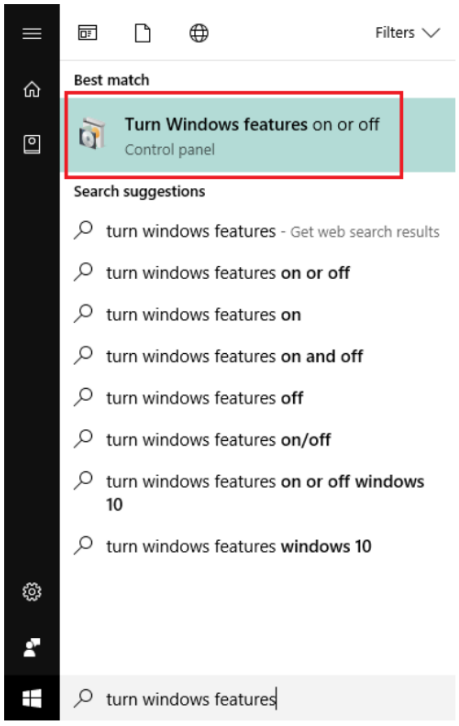
วิธีปิด SMBv1 เพื่อป้องกันตัวเองจากมัลแวร์เรียกค่าไถ่ WannaCry

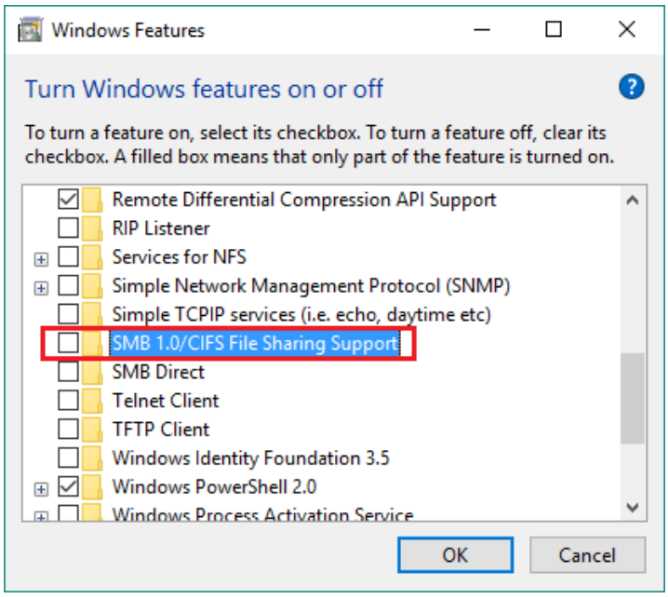
ขณะนี้มัลแวร์เรียกค่าไถ่ WannaCry / WannaCrypt กำลังระบาดหนักทั่วโลก มีคอมพิวเตอร์โดน โจมตีไปแล้วกว่า 200,000 เครื่องใน 99 ประเทศภายในเวลาเพียง 2 วันเท่านั้น มีวิธีป้องกันตัวเองจากมัลแวร์ดังกล่าวอยู่ 2 อย่าง คือการอัพเดตวินโดวส์เพื่ออุดช่องโหว่ และอีกอย่างคือการปิดโปรโตคอล Server Message Block (SMB) ที่เป็นโปรโตคอลสำหรับการรับส่งไฟล์ ระหว่างคอมพิวเตอร์ที่อยู่ในเครือข่ายเดียวกัน ปัจจุบันโปรโตคอล SMB มี 3 เวอร์ชันด้วยกัน คือ SMBv1, SMBv2 และ SMBv3 โดย SMBv1 เป็น รุ่นเก่ามาก ออกมาเกือบ 30 ปีแล้ว ซึ่ง WannaCry ก็ใช้ช่องโหว่ของ SMBv1 เป็นช่องทาง แพร่ตัวเองเข้าโจมตีคอมพิวเตอร์เครื่องอื่นในเครือข่าย โดยที่เครื่องเป้าหมายไม่ต้องคลิกเปิดไฟล์ (เปิดคอมต่อเน็ตอยู่ดีๆ ก็ติดเลย) ดังนั้น SMBv1 จึงไม่เหมาะสมที่จะใช้งานในยุคนี้แล้ว และควรปิดทิ้งไป เมื่อขึ้นชื่อว่าเป็นการรับส่งข้อมูลหากัน จึงต้องมีฝั่งนึงเป็น Server และอีกฝั่งเป็น Client โดย สำหรับผู้ใช้ทั่วไป จะถือว่าตัวเองเป็น Client ซึ่งการปิดแบบ Client ก็เพียงพอแล้วต่อการป้องกัน ตนเองไม่ให้รับมัลแวร์เข้ามา

การปิด SMBv1 ฝั่ง Client โชคดีที่ขั้นตอนการปิด SMBv1 ใน Windows 8.1, Windows 10, Windows Server 2012 R2 และ Windows Server 2016 นั้นง่ายมาก ไม่ต้องมีความรู้ทางเทคนิคเลยก็ทำได้ ใช้เวลาไม่ถึง 5 นาทีก็เสร็จแล้ว ดังนี้

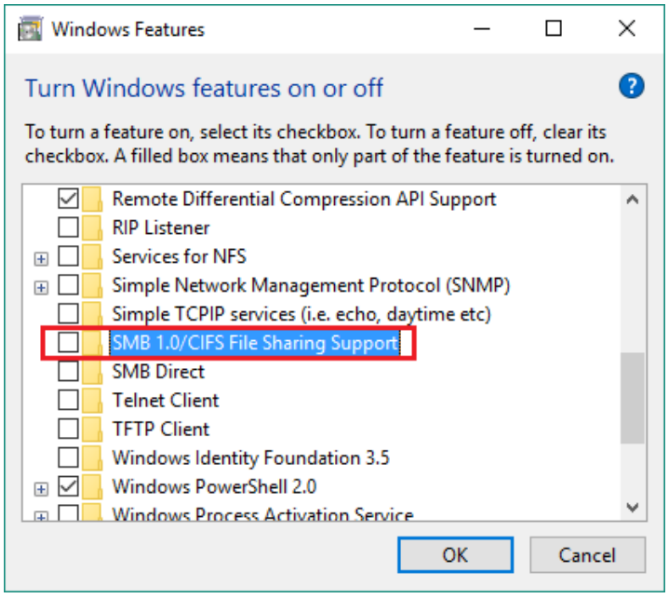
1. คลิก Start
2. พิมพ์ในช่อง Search ว่า "turn windows features" แล้วคลิกที่ "Turn Windows features on or off" ตามภาพ



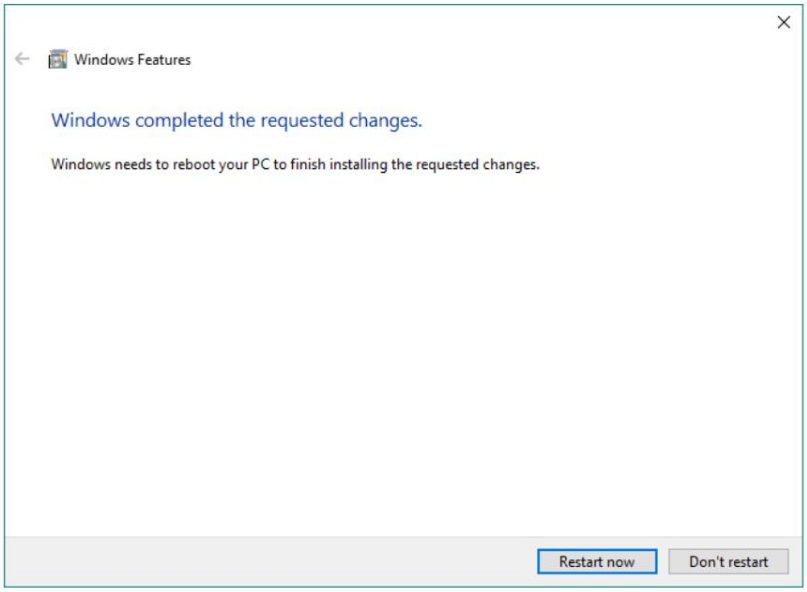
3. หน้าต่าง Windows Features จะเปิดขึ้นมา ให้เลื่อนลงไปล่างๆ หาข้อความ "SMB 1.0/CIFS File Sharing Support" โดยฟีเจอร์นี้จะถูกเปิดไว้เป็นค่าเริ่มต้น



4. ให้นำติ๊กถูกออกจากช่องสี่เหลี่ยม และกด OK

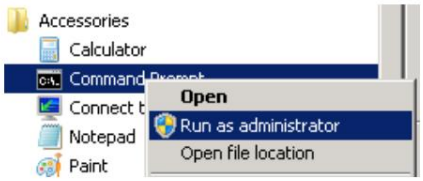


5. สุดท้ายให้รีสตาร์ทเครื่อง 1 รอบ ก็เป็นอันเสร็จสิ้นเพียงเท่านี้มัลแวร์ WannaCry ก็ไม่สามารถแพร่มาได้



อย่างไรก็ตาม การปิด SMBv1 ฝั่ง Client ในระบบปฏิบัติการรุ่นเก่าอย่าง Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 และ Windows Server 2012 มีความยุ่งยากอยู่บ้าง เพราะต้องรันคำสั่งผ่าน Command Prompt ดังนี้

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



2. พิมพ์คำสั่งด้านล่าง ทีละบรรทัด

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

   sc.exe config mrxsmb10 start= disabled

3. รีสตาร์ทเครื่อง

สุดท้ายขอแนะนำให้ข้าราชการทุกท่านอัพเดตระบบปฏิบัติการ รวมถึงซอฟต์แวร์ต่างๆ ให้เป็นเวอร์ชั่น ล่าสุดอยู่เสมอ ขอให้มีความตระหนักระหว่างการใช้งานให้มาก เพราะการโจมตีไซเบอร์สมัยนี้โหดร้ายกว่าแต่ก่อนมาก