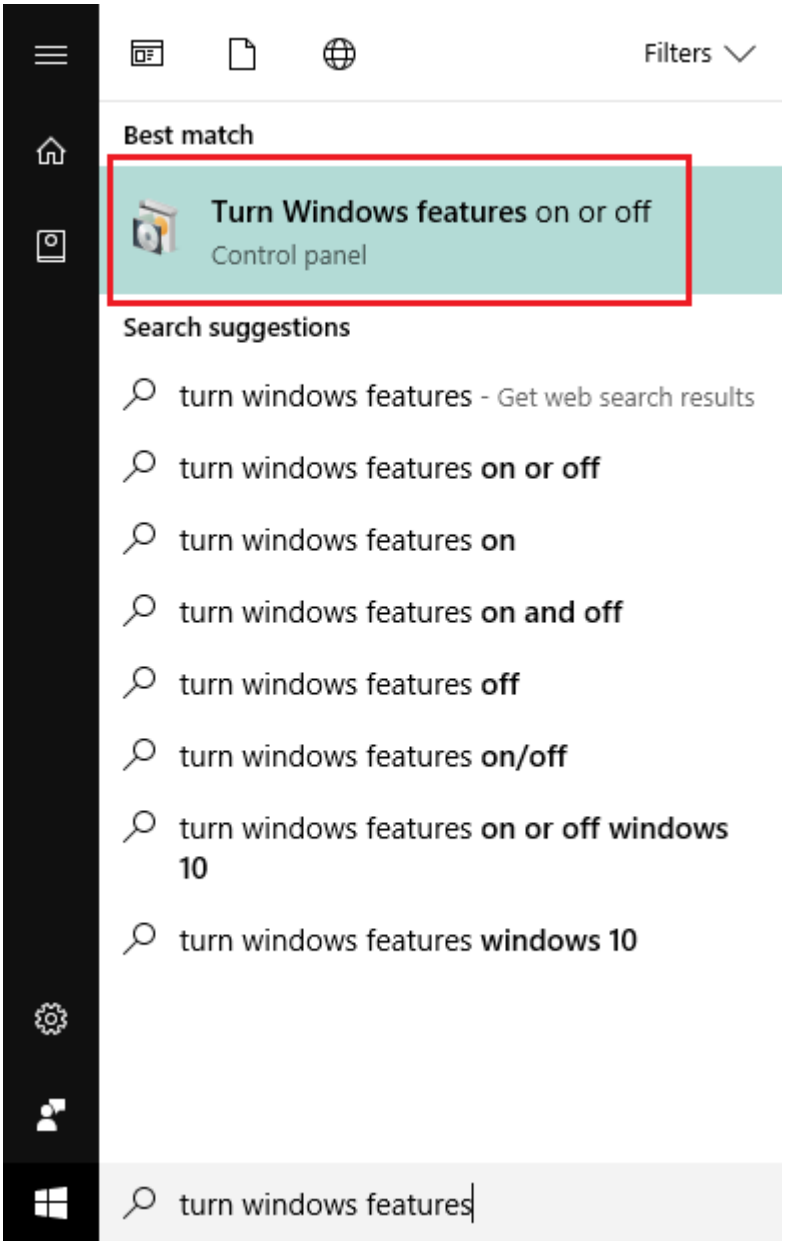
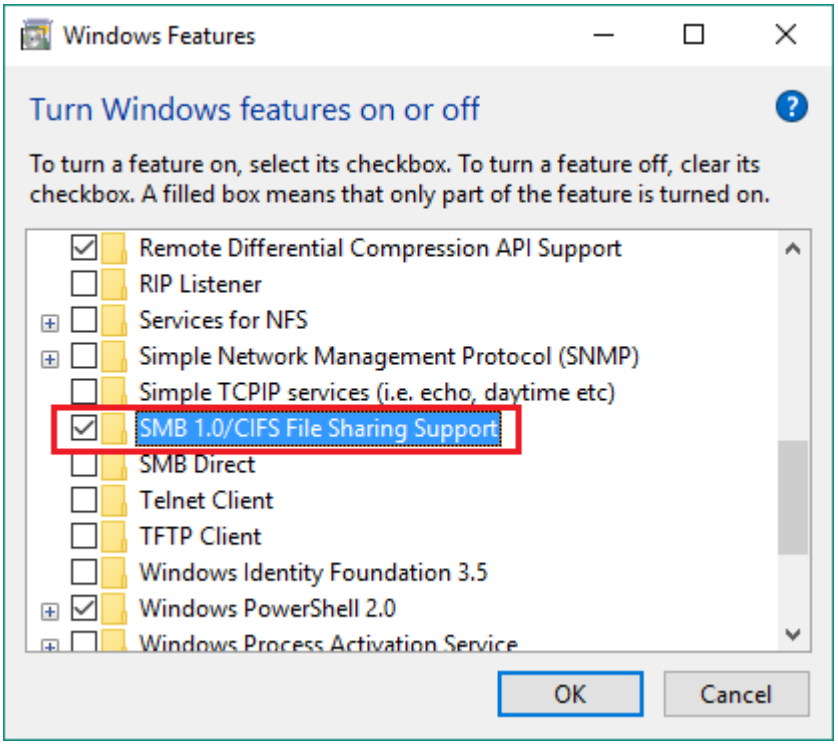
การปิด SMBv1(Server Message Block (SMB)) **ฝั่ง Client**

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

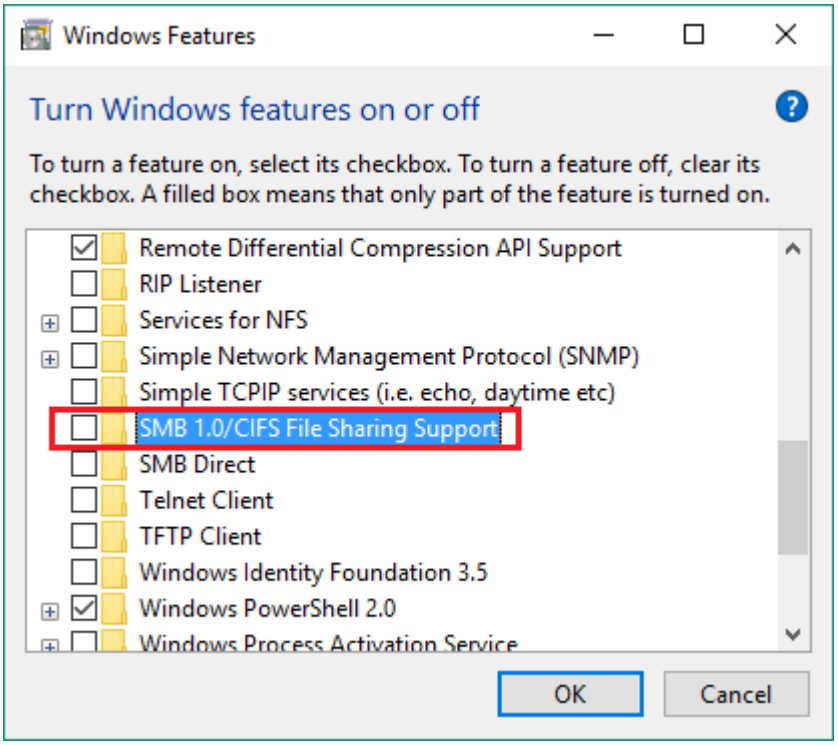
1. คลิก **Start**
2. พิมพ์ในช่อง Search ว่า "turn windows features" แล้วคลิกที่ **"Turn Windows features on or off"** ตามภาพ



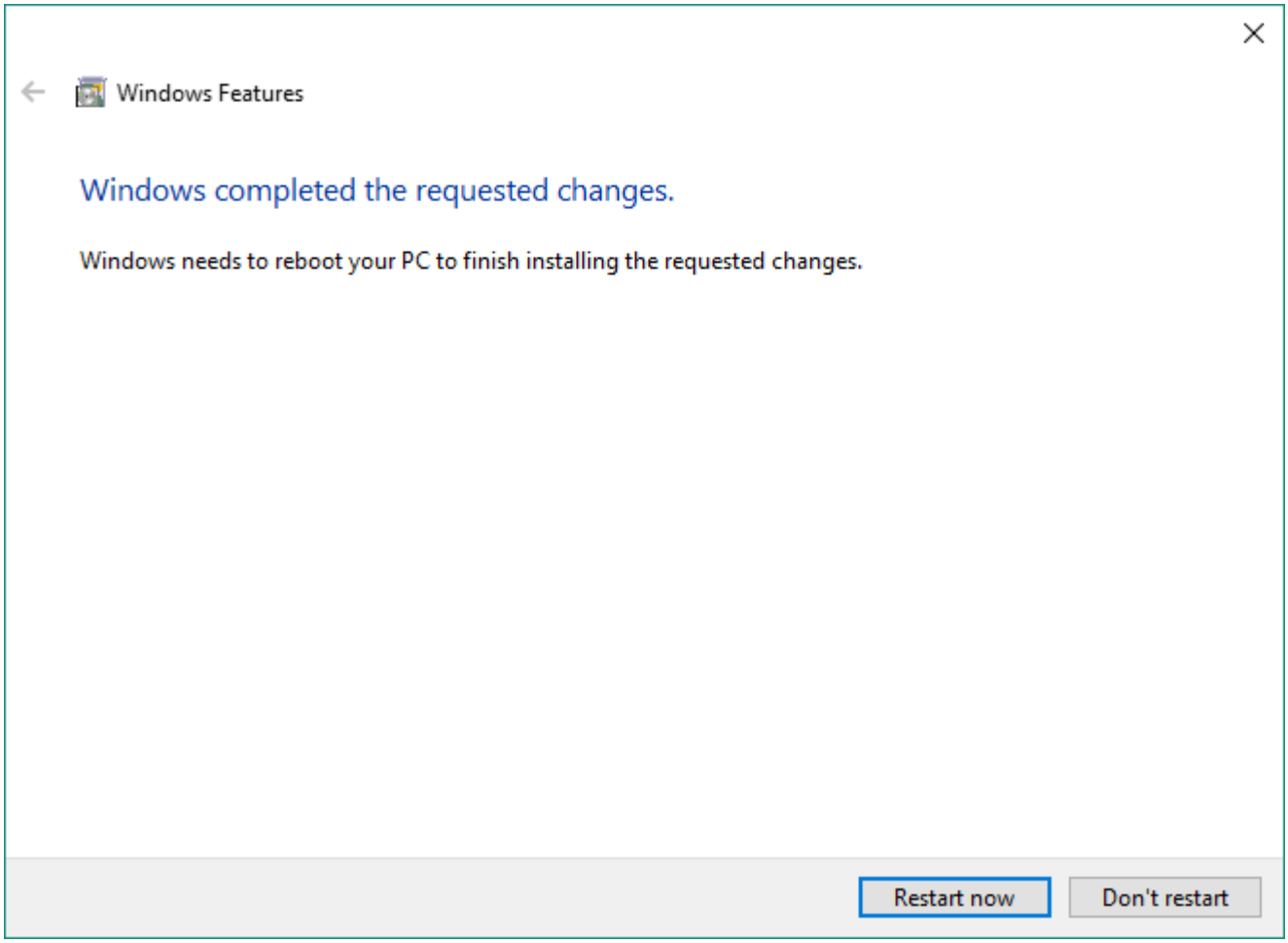
3. หน้าต่าง **Windows Features** จะเปิดขึ้นมา ให้เลื่อนลงไปล่างๆ หาข้อความ **"SMB 1.0/CIFS File Sharing Support"** โดยฟีเจอร์นี้จะถูกเปิดไว้เป็นค่าเริ่มต้น



4. ให้**นำติ๊กถูกออกจากช่องสี่เหลี่ยม** และกด OK

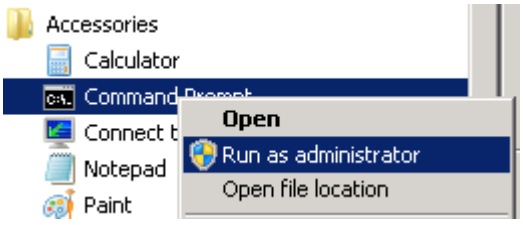


5. สุดท้าย ให้รีสตาร์ทเครื่อง 1 รอบ ก็เป็นอันเสร็จสิ้น เพียงเท่านี้มัลแวร์ WannaCry ก็ไม่สามารถแพร่มาหาเราได้แล้ว



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 แล้วคลิก Run as administrator



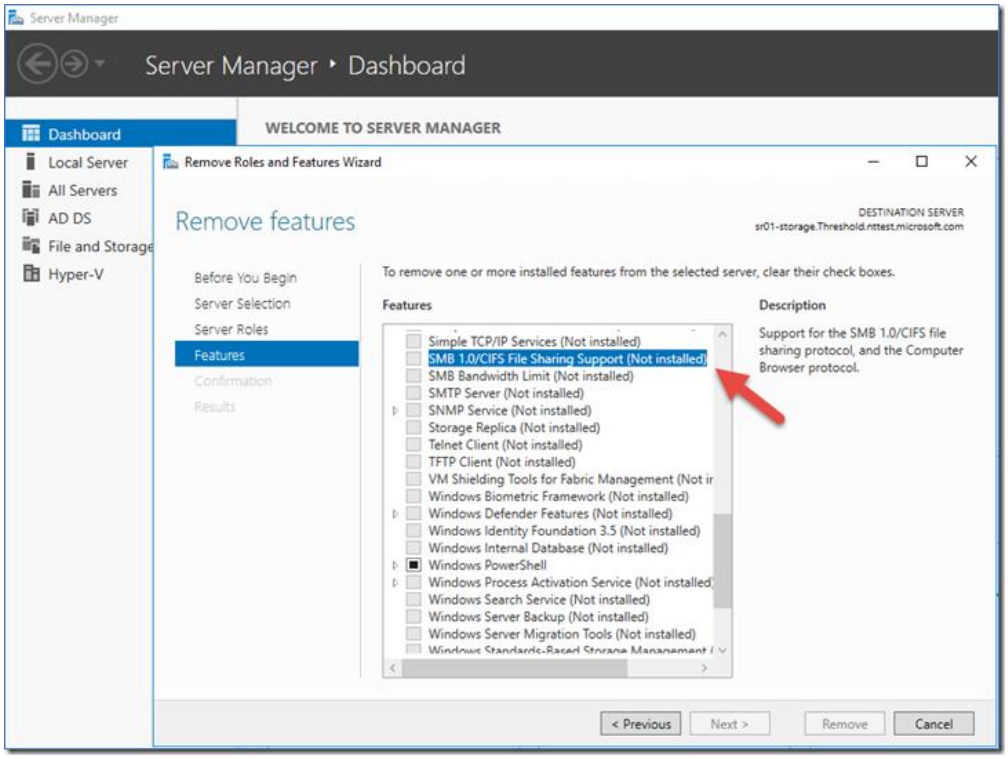
2. พิมพ์คำสั่งด้านล่าง ทีละบรรทัด

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

3. รีสตาร์ทเครื่อง

การปิด SMBv1 ฝั่ง Server

สำหรับฝั่ง Server ที่ใช้ระบบปฏิบัติการ Windows Server 2012 R2 และ Windows Server 2016 ก็ให้เปิด Server Manager และไปที่ Dashboard จากนั้นก็นำติ๊กถูกออกตามภาพ



ส่วนการปิด SMBv1 ฝั่งเซิฟเวอร์ในระบบปฏิบัติการรุ่นเก่า อย่าง Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2, Windows Vista และ Windows Server 2008 มีความซับซ้อนมาก จึงจะไม่นำมาสอนในบทความนี้ ขอให้ผู้ดูแลระบบเข้าไปทำตามวิธีที่ไมโครซอฟท์สอนไว้จากลิงค์อ้างอิงท้ายบทความนะครับ

สุดท้าย เราขอแนะนำให้ทุกท่านอัพเดตระบบปฏิบัติการ รวมถึงซอฟต์แวร์ต่างๆ ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ และใช้ซอฟต์แวร์ลิขสิทธิ์กันเถิดครับ อย่าง Windows 10 แบบ OEM ในปัจจุบันก็ราคาเพียง 3,990 บาทเท่านั้น สามารถใช้งานได้อย่างสบายใจ (และภูมิใจ) พร้อมรับแพตช์ล่าสุดตลอดเวลา ขอให้มี awareness ระหว่างการใช้งานให้มาก เพราะการโจมตีไซเบอร์สมัยนี้มันโหดร้ายกว่าแต่ก่อนเยอะครับ

ที่มา : https://www.blognone.com/node/92410

การแก้ไขระยะยาวคือการอัปเดต Patch ให้ปลอดภัยจาก Microsoft โดยตรง

- Vista, 7 SP1, 8.1, 10 v1607 หรือเก่ากว่า
- Server 2008 SP2, Server 2008 R2 SP1, Server 2012, Server 2012 R2, Server 2016

Microsoft Security Bulletin MS17-010 - Critical

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

- XP SP2, XP SP3, Windows 8.0
- Server 2003 SP2
Customer Guidance for WannaCrypt attacks
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

WannaCry เป็นเพียงตัวแรก ดังนั้นปิดช่องโหว่ **MS17-010 ที่บ้าน ที่ทำงาน** และ**ร้านโปรด**ของคุณเสียแต่วันนี้นะครับ

ข้อแนะนำในการป้องกัน

1. ติดตั้งแพตช์แก้ไขช่องโหว่ SMBv1 จาก Microsoft โดย Windows Vista, Windows Server 2008 ถึง Windows 10 และ Windows Server 2016 ดาวน์โหลดอัปเดตได้จาก https://technet.microsoft.com/en-us/library/security/ms17-010.aspx ส่วน Windows XP และ Windows Server 2003 ดาวน์โหลดอัปเดตได้จาก https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
2. เนื่องจากมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ SMBv1 ซึ่งถูกใช้ใน Windows เวอร์ชันเก่า เช่น Windows XP, Windows Server 2003 หรือระบบเซิร์ฟเวอร์บางรุ่น หากใช้งาน Windows เวอร์ชันใหม่และไม่มีความจำเป็นต้องใช้ SMBv1 ผู้ดูแลระบบอาจพิจารณาปิดการใช้งาน SMBv1 โดยดูวิธีการปิดได้จาก https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
3. ผู้ดูแลระบบควรติดตามและป้องกันการเชื่อมต่อพอร์ต SMB (TCP 137, 139 และ 445 UDP 137 และ 138) จากเครือข่ายภายนอก อย่างไรก็ตาม การบล็อกพอร์ต SMB อาจมีผลกระทบกับบางระบบที่จำเป็นต้องใช้งานพอร์ตเหล่านี้ เช่น file sharing, domain, printer ผู้ดูแลระบบควรตรวจสอบก่อนบล็อกพอร์ตเพื่อป้องกันไม่ให้เกิดปัญหา [6]
4. ตั้งค่า Firewall เพื่อบล็อกการเชื่อมต่อกับไอพีแอดเดรสปลายทางตามตารางที่ 1 เนื่องจากเป็นไอพีที่ถูกใช้ในการแพร่กระจายและควบคุมมัลแวร์
5. อัปเดตระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดอยู่เสมอ หากเป็นได้ได้ควรหยุดใช้งานระบบปฏิบัติการ Windows XP, Windows Server 2003 และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ
6. ติดตั้งแอนติไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ ปัจจุบันแอนติไวรัสส่วนใหญ่ (รวมถึง Windows Defender ของ Microsoft) สามารถตรวจจับมัลแวร์ WannaCry สายพันธุ์ที่กำลังมีการแพร่ระบาดได้แล้ว