ด่วนที่สุด

ที่ รง ๐๒๐๘.๑/ ว ๕๖๗

สำนักงานปลัดกระทรวงแรงงาน
ถนนมิตรไมตรี ดินแดง
กรุงเทพฯ ๑๐๔๐๐

๑๖ พฤษภาคม ๒๕๖๐

เรื่อง การป้องกันการเรียกค่าไถ่จากมัลแวร์ WannaCry

เรียน แรงงานจังหวัดทุกจังหวัด

สิ่งที่ส่งมาด้วย ๑. คู่มือการปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นระบบปัจจุบันและการปิดบริการ SMBv1
๒. การ update signature Antivirus

ตามที่เว็บไซต์ สพทอ. (ETDA) แจ้งข่าวกระทรวงดิจิทัล (DE) เรื่อง มัลแวร์เรียกค่าไถ่ WannaCry แจ้งว่าเมื่อวันที่ ๑๒ พฤษภาคม ๒๕๖๐ บริษัท Avast ได้เผยแพร่รายงานการพบมัลแวร์เรียกค่าไถ่ ซึ่งมีจุดประสงค์เพื่อเข้ารหัสลับข้อมูลไฟล์เอกสาร และไฟล์สำคัญทั้งหมดที่ใช้งาน รวมตัวสามารถกระจายตัวเองจากเครื่องคอมพิวเตอร์จากเครื่องหนึ่งไปยังเครื่องอื่นๆ ในเครือข่ายผ่านช่องทางใหม่ของวินโดว์ที่บริการ โดยการแชร์ไฟล์ผ่านเครือข่าย (SMB) ที่มีการเปิดบริการที่ผ่านมาเกิดปัญหากับหน่วยงานองค์กรเอกชนในประเทศรัสเซียและประเทศอังกฤษประมาณ ๒๐๐ ราย มีการยับยั้งการแพร่ของมัลแวร์ได้ชั่วคราวจากชาวอังกฤษ และคาดว่าจะระบาดในช่วงหลังวันที่ ๑๕ พฤษภาคม ๒๕๖๐ อีก นั้น

สำนักงานปลัดกระทรวงแรงงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาปัญหา และช่องทางการแก้ไขปัญหามัลแวร์เรียกค่าไถ่ WannaCry จึงเห็นควรให้ทุกจังหวัดดำเนินการ ดังนี้

๑) ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นระบบปัจจุบันเพื่อป้องกันช่องโหว่ของระบบ โดยเฉพาะปิดบริการ SMBv1 ที่เป็นช่องทางการเชื่อมต่อ (วิธีการดำเนินการตามเอกสาร ๑)

๒) ตรวจสอบ Antivirus NOD32 ที่เครื่องคอมพิวเตอร์มีการ update signature เป็นปัจจุบันหรือไม่ (เอกสาร ๒)

๓) ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นควรตรวจสอบกับผู้ส่งอีเมลว่าเป็นฉบับจริง หรือไม่คลิกลิงค์จากเว็บไซต์ที่ไม่น่าเชื่อถือ

๔) เพื่อป้องกันข้อมูลสูญหาย ให้ผู้ใช้งานจัดเก็บข้อมูลงานส่วนตัวในอุปกรณ์จัดเก็บภายนอก

โดยสอบถามข้อมูลได้ที่นายพงษ์พัฒน์ ศรัณยานุรักษ์ นักวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทร ๐๒-๒๓๒-๑๐๓๕ และหากพบปัญหาดังกล่าวให้รายงานผลกลับมาที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

จึงเรียนมาเพื่อพิจารณา

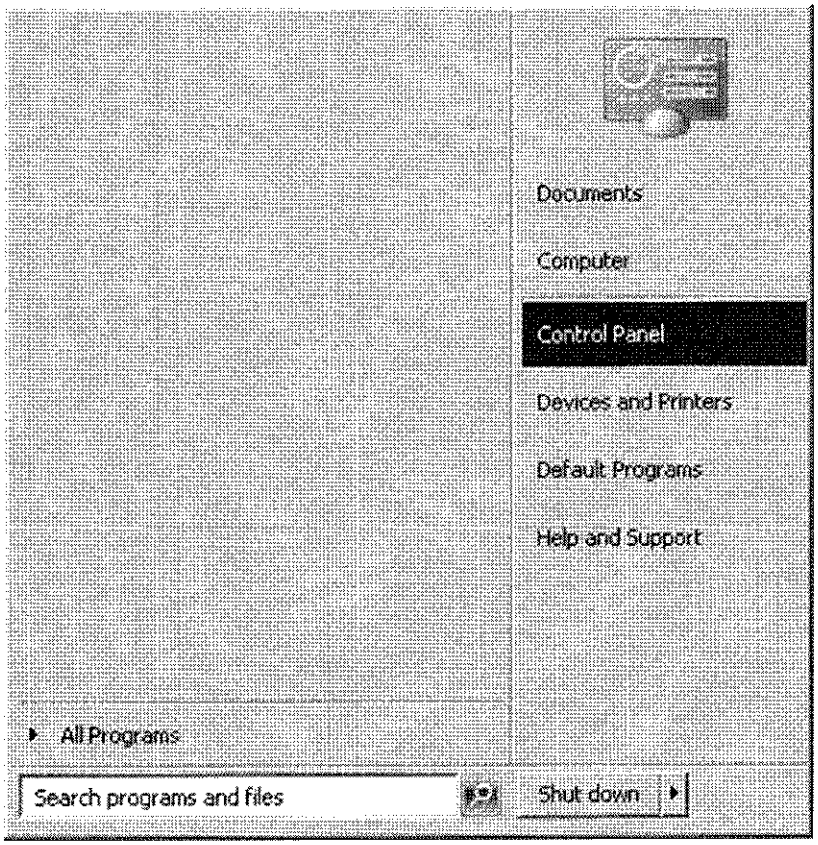
ขอแสดงความนับถือ

(นายสิงหเดช ชูอำนาจ)
รองปลัดกระทรวงแรงงาน ปฏิบัติราชการแทน
ปลัดกระทรวงแรงงาน

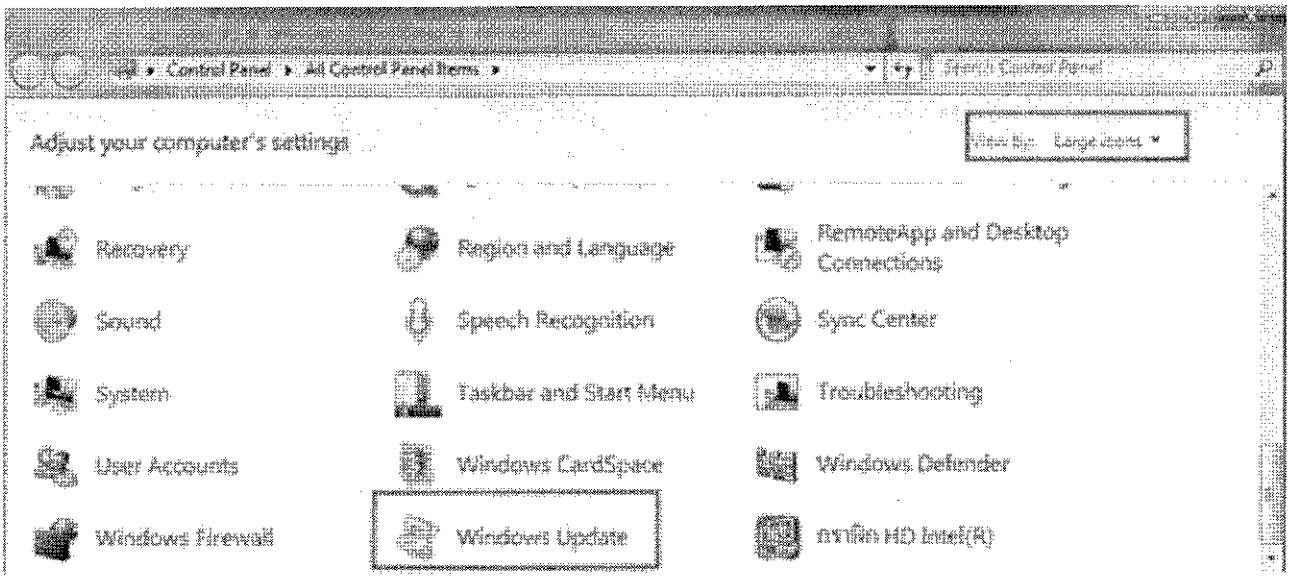
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๒๓๒ ๑๐๓๕
โทรสาร ๐ ๒๒๔๘ ๔๑๔๑

วิธีการอัพเดท Windows (windows update)

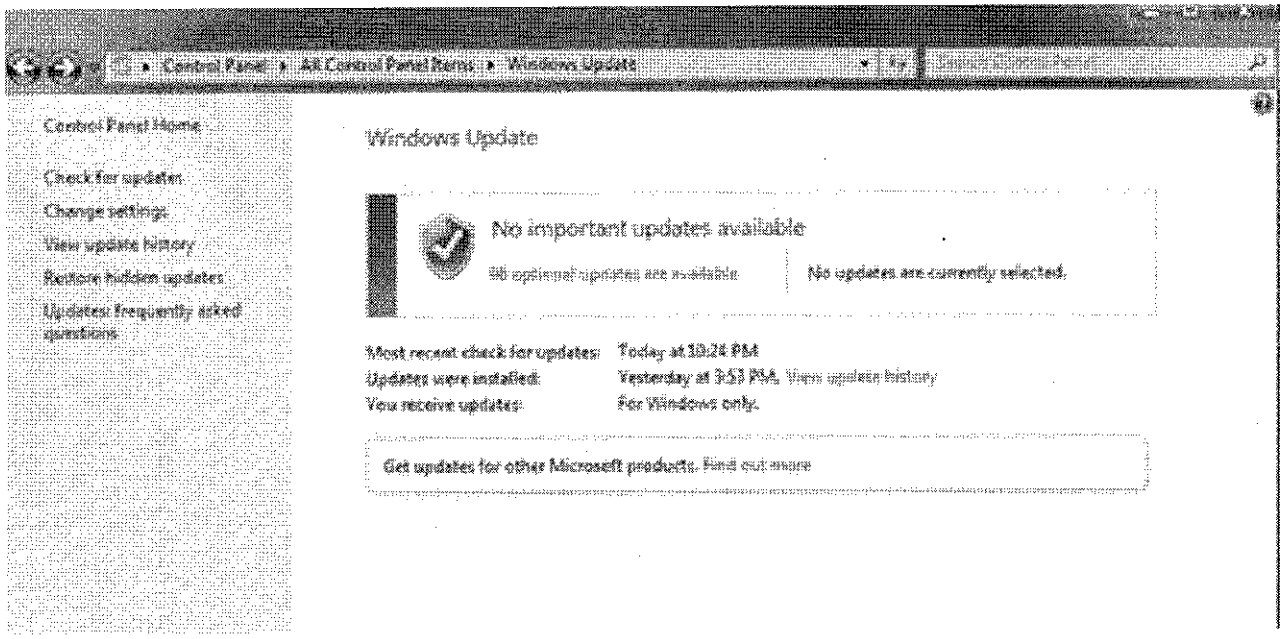
1. ไปที่ Start  > เลือก Control Panel



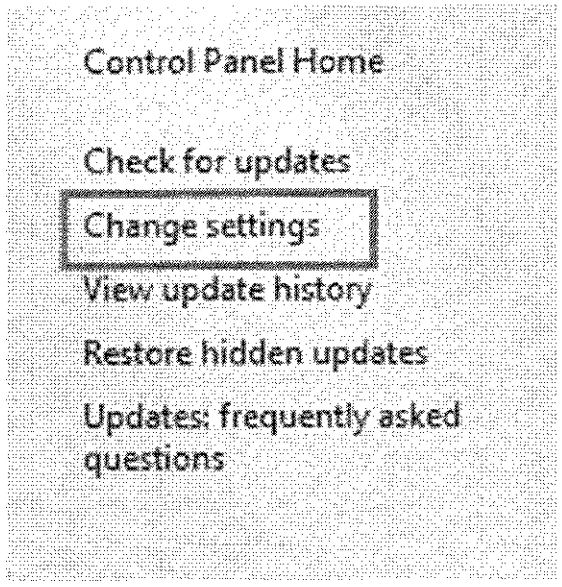
2. เลือก View by : Catagory และทำการเลือก Windows Update



3. จากนั้นเราจะเห็นหน้าต่างของ Windwos Updates

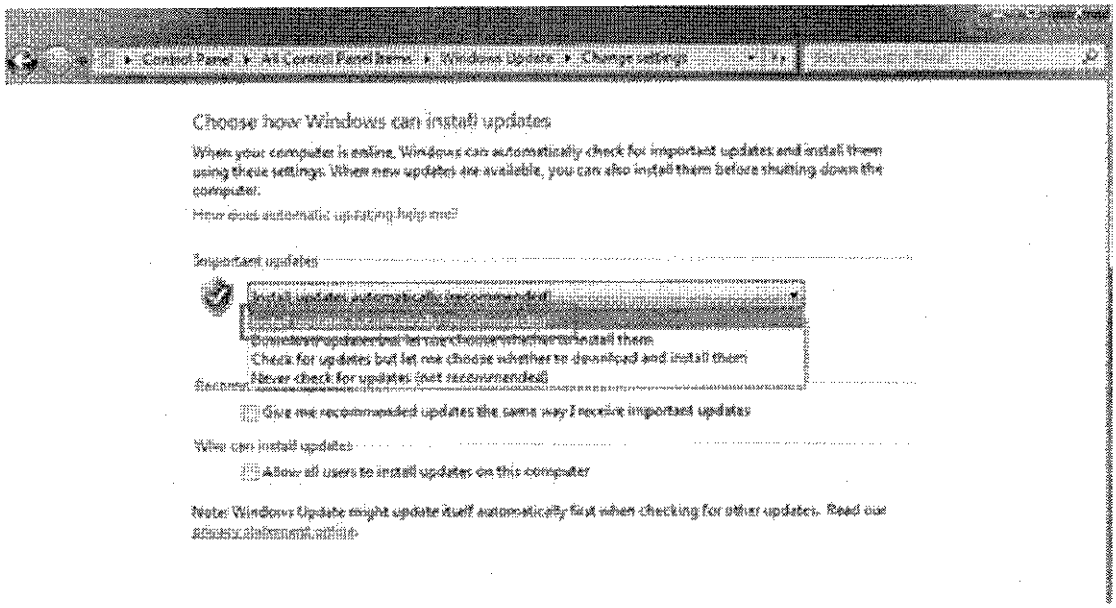


4. ทำการคลิก Change Settings

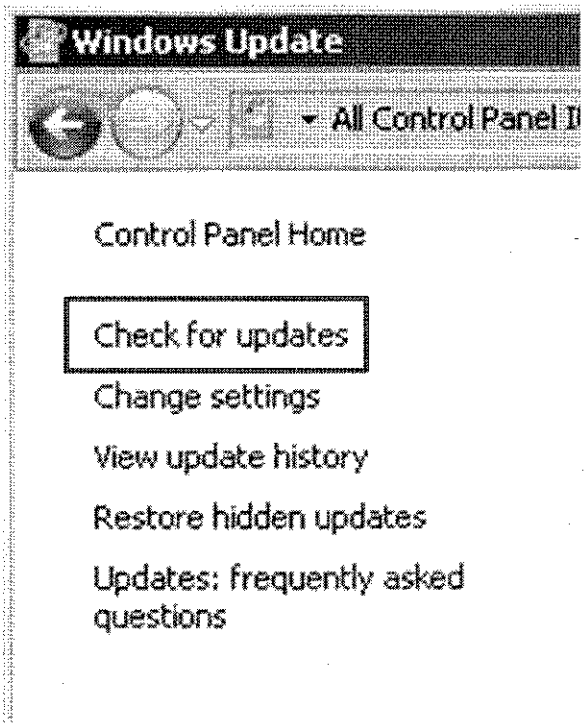


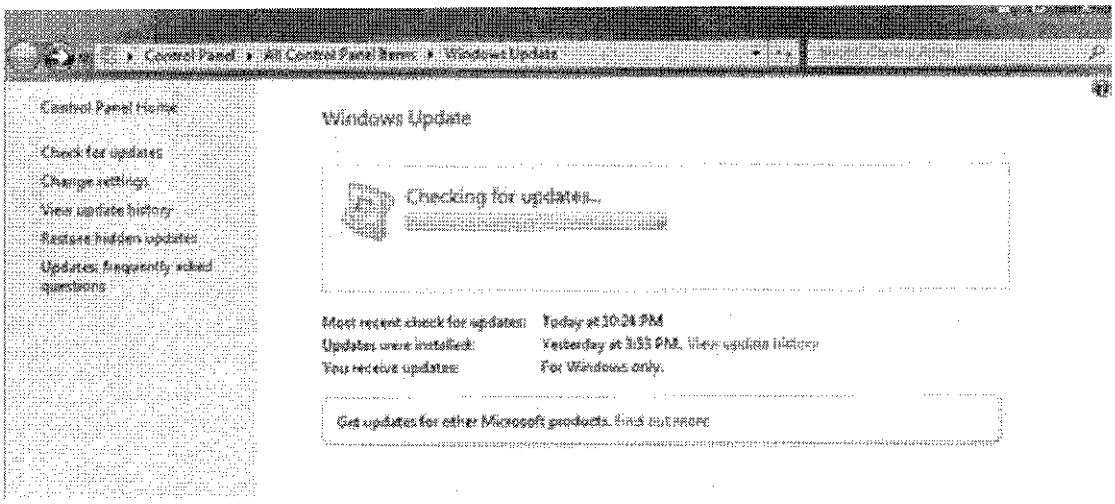
5. จากนั้นเลือก

ถ้าเป็น Windows 7 ของแท้ แนะนำให้เลือก Install Update automatic และเลือกเวลาในการ Update



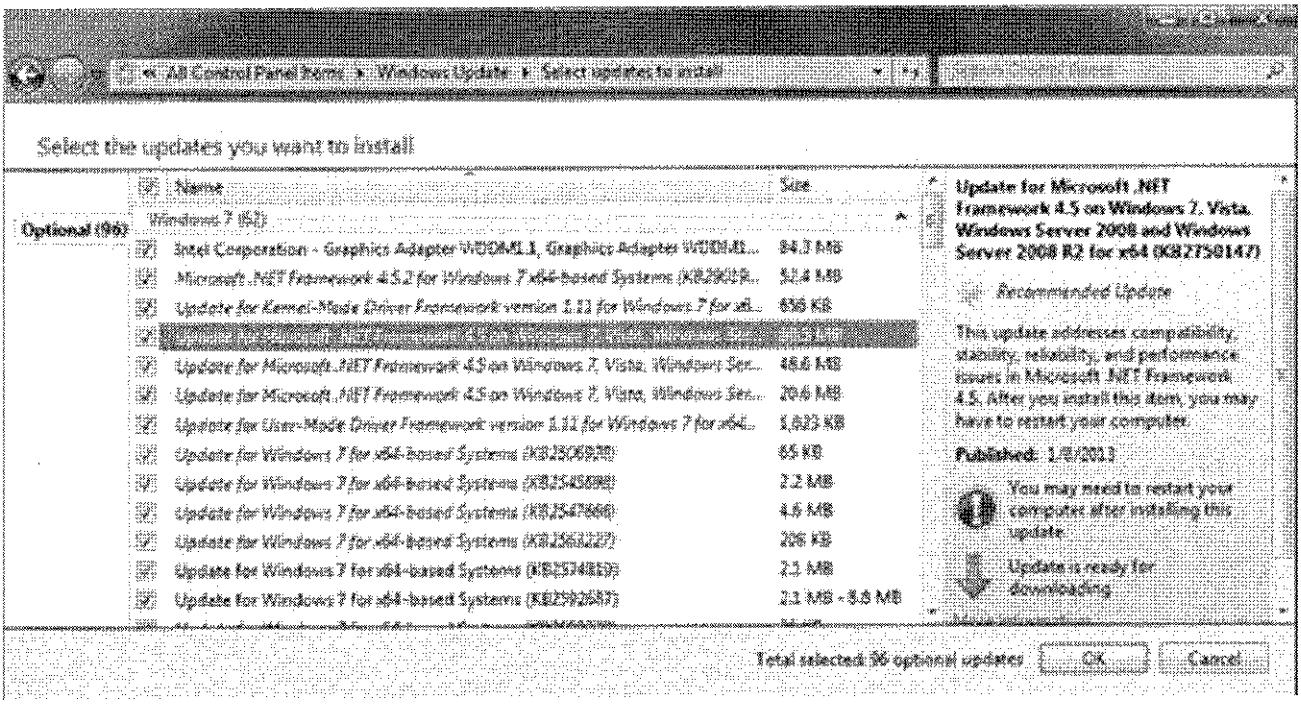
จากนั้นทำการคลิก Check for update





เมื่อทำการตรวจสอบการอัพเดต Windows เรียบร้อย ให้เราทำการกด Optional update are avilable

และเราสามารถเลือก Patch ต่างๆเพิ่มเติมได้ และทำการกด OK โดยให้เราเลือกหมดทุกตัวเลยก็ได้สำหรับ Windows (แต่ถ้าเป็นพวกการอัพเดท Software จะเลือกหรือไม่เลือกก็ได้แล้วแต่ครับ แต่ก็จะแนะนำให้เลือก)

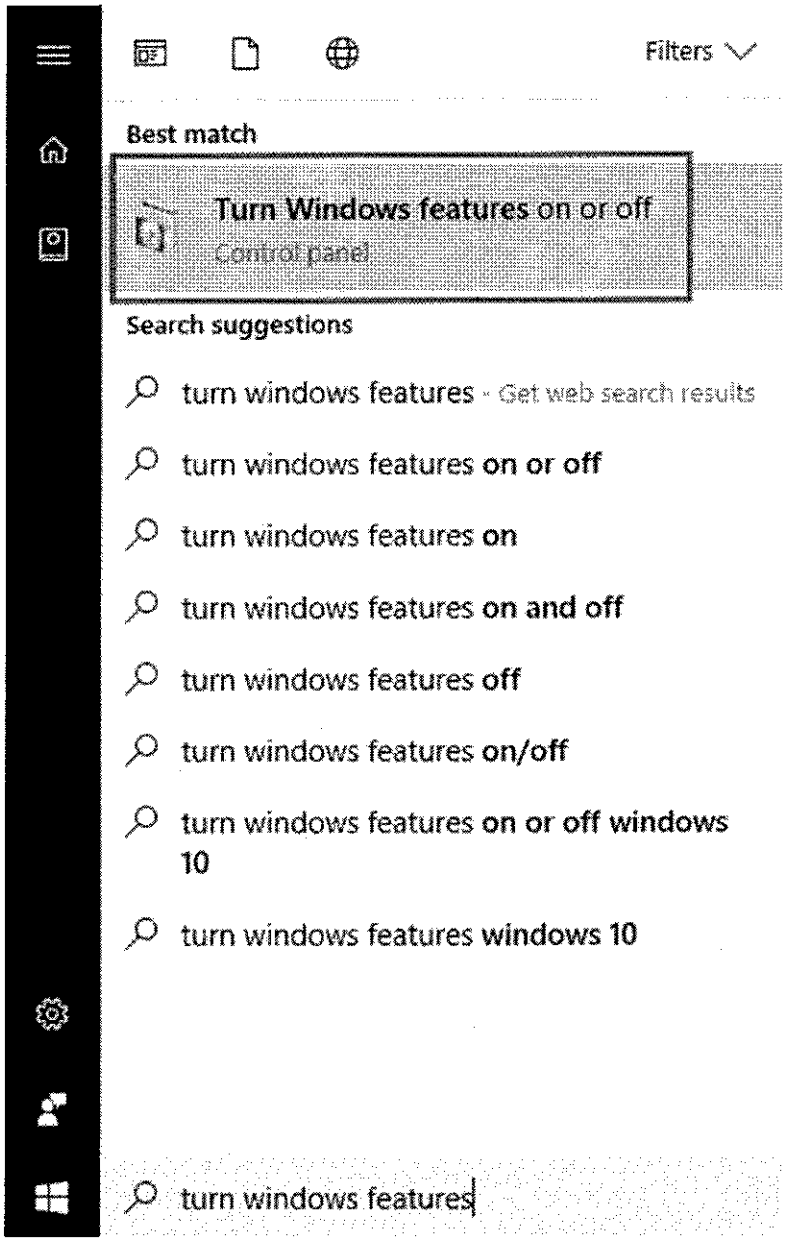


โดยในการ Update Windows 7 หรือจะเป็น Windows 8 / Windows 10 ก็จะเป็นการเพิ่ม Security ของ Windows ให้ดียิ่งขึ้น กัน Hacker เข้ามาทำการล่วงข้อมูลสำคัญๆของเรา โดยสำหรับใครที่ใช้ Windows แท้ ก็แนะนำว่าให้ทำการเลือกเปิด Windows Update ด้วย

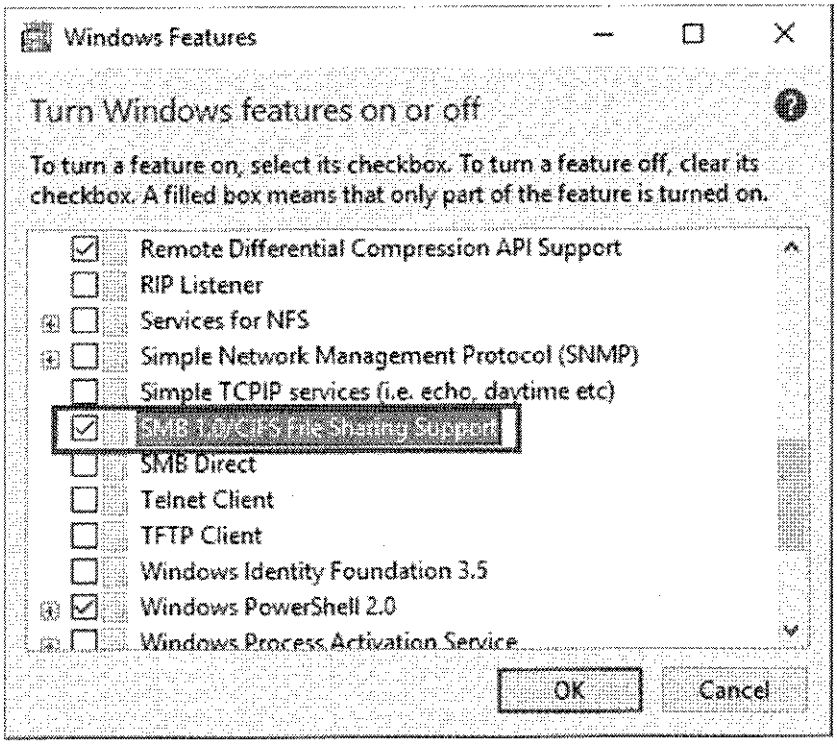
วิธีปิด SMBv1 เพื่อป้องกันตัวเองจากมัลแวร์เรียกค่าไถ่ WannaCry สำหรับระบบปฏิบัติการ Windows XP , Windows Vista และ Windows 7 Windows 8.1และ Windows 10

สำหรับระบบปฏิบัติการ Windows 8.1 และ Windows 10

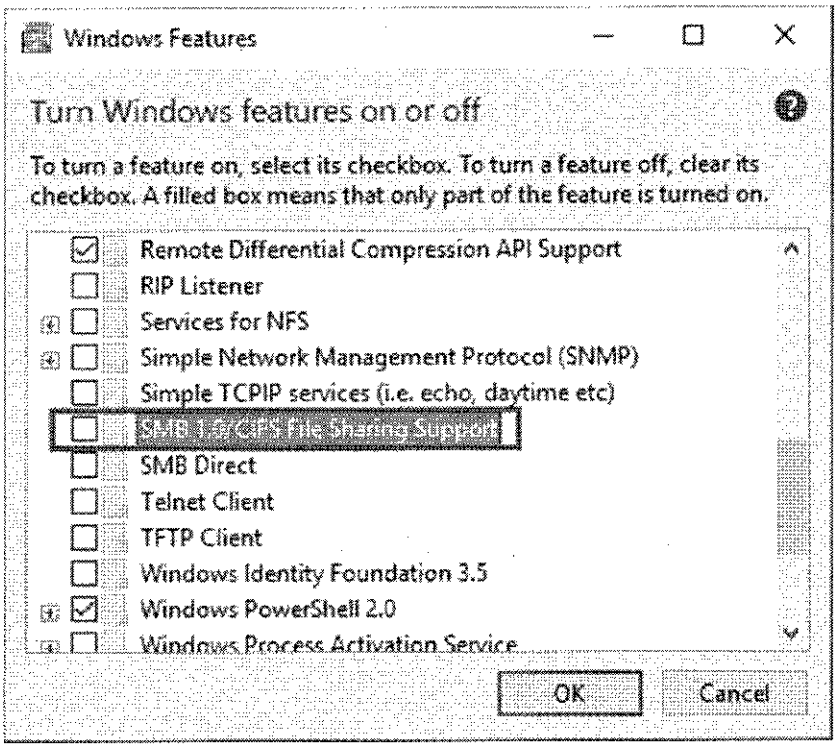
1. คลิก Start
2. พิมพ์ในช่อง Search ว่า "turn windows features" แล้วคลิกที่ "Turn Windows features on or off" ตามภาพ



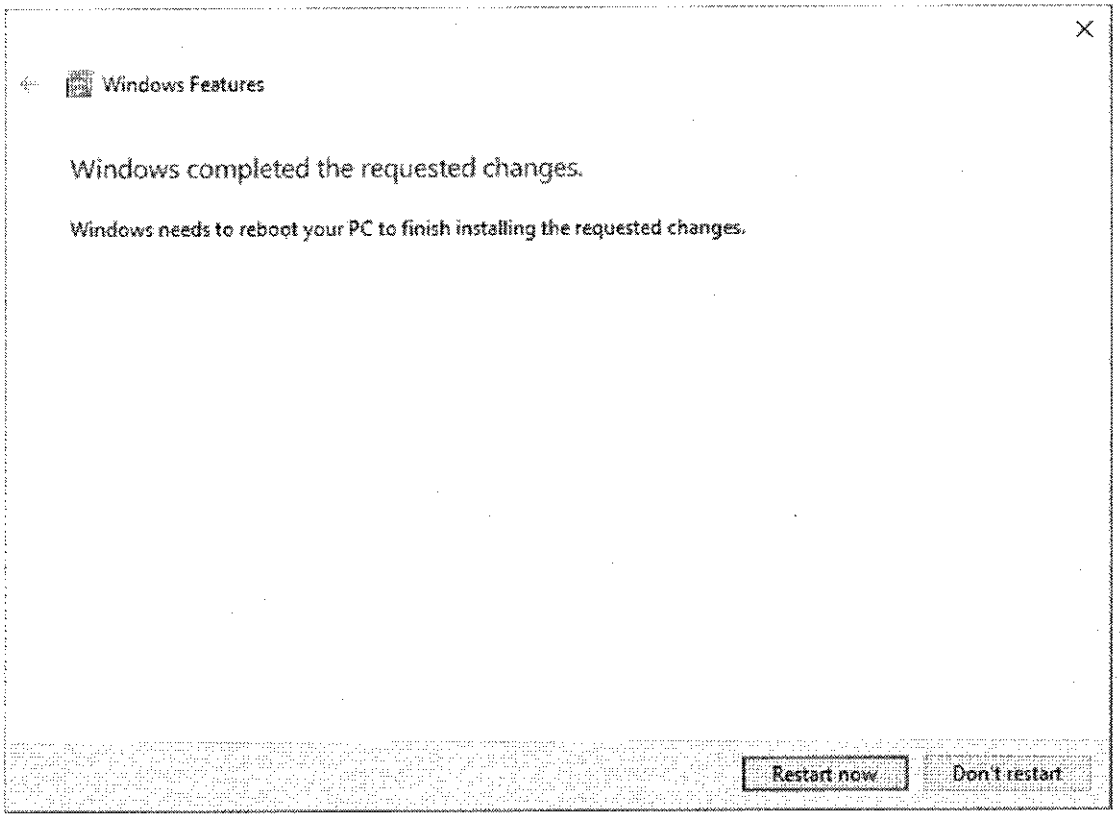
3. หน้าต่าง Windows Features จะเปิดขึ้นมา ให้เลื่อนลงไปล่างๆ หาข้อความ "SMB 1.0/CIFS File Sharing Support" โดยฟีเจอร์นี้จะถูกเปิดไว้เป็นค่าเริ่มต้น



4. ให้นำติ๊กถูกออกจากช่องสี่เหลี่ยม และกด OK



5. สุดท้าย ให้รีสตาร์ทเครื่อง 1 รอบ ก็เป็นอันเสร็จสิ้น เพียงเท่านี้มัลแวร์ WannaCry ก็ไม่สามารถแพร่มาหาเราได้แล้ว



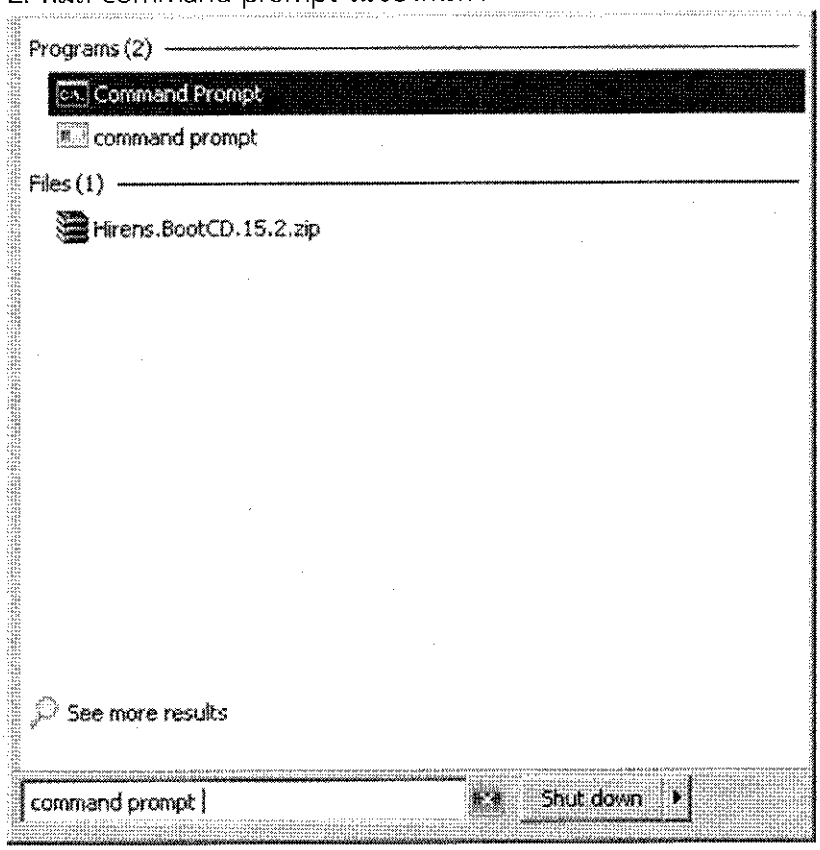
วิธีปิด SMBv1 เพื่อป้องกันตัวเองจากมัลแวร์เรียกค่าไถ่ WannaCry

สำหรับระบบปฏิบัติการ Windows XP , Windows Vista และ Windows 7

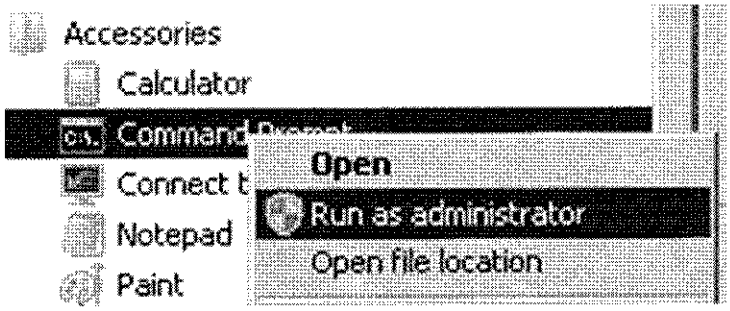
1. กดปุ่ม Start (รูป 

)

2. พิมส์ command prompt ในช่องค้นหา



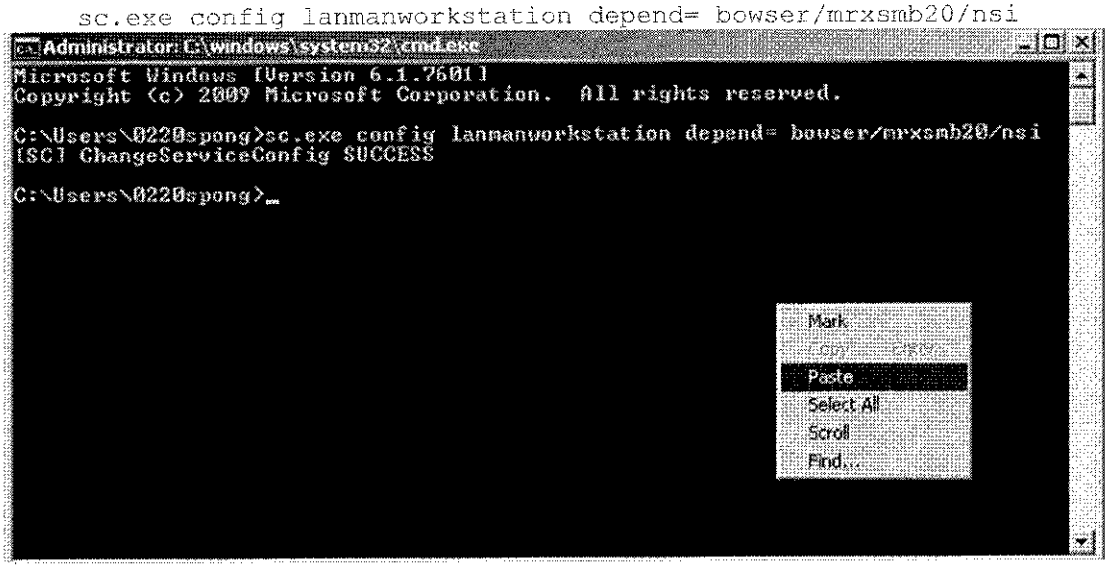
3. คลิกขวาที่ Command Prompt แล้วคลิก Run as administrator



4. พิมพ์คำสั่งด้านล่าง ทีละบรรทัด

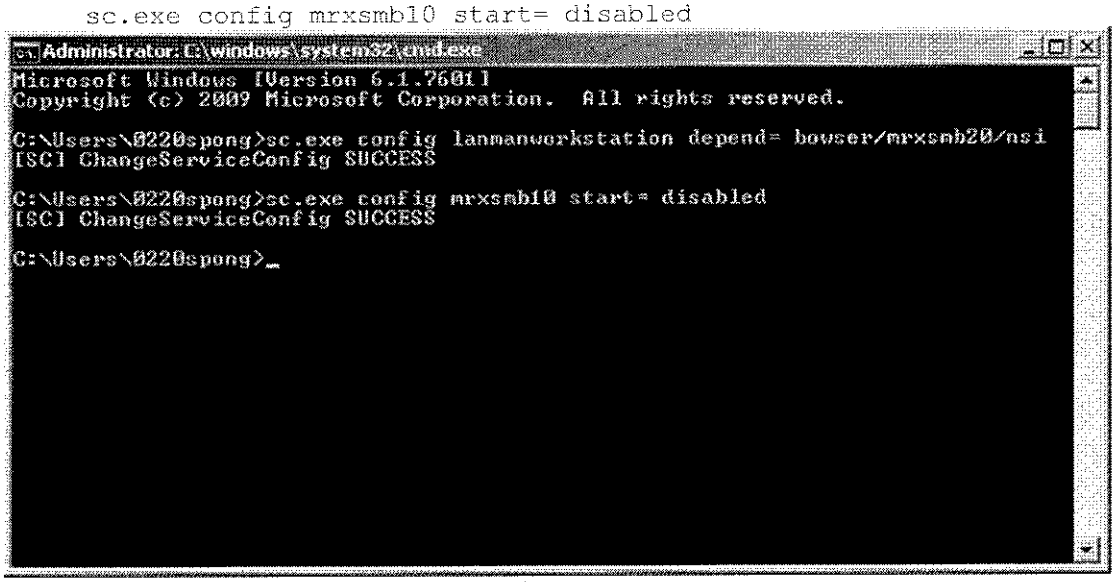
4.1 copy คำสั่ง ด้านล่าง แล้วคลิกขวาที่ Command Prompt เลือก Paste แล้ว กด Enter

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



4.2 copy คำสั่ง ด้านล่าง แล้วคลิกขวาที่ Command Prompt เลือก Paste แล้ว กด Enter

```
sc.exe config mrxsmb10 start= disabled
```

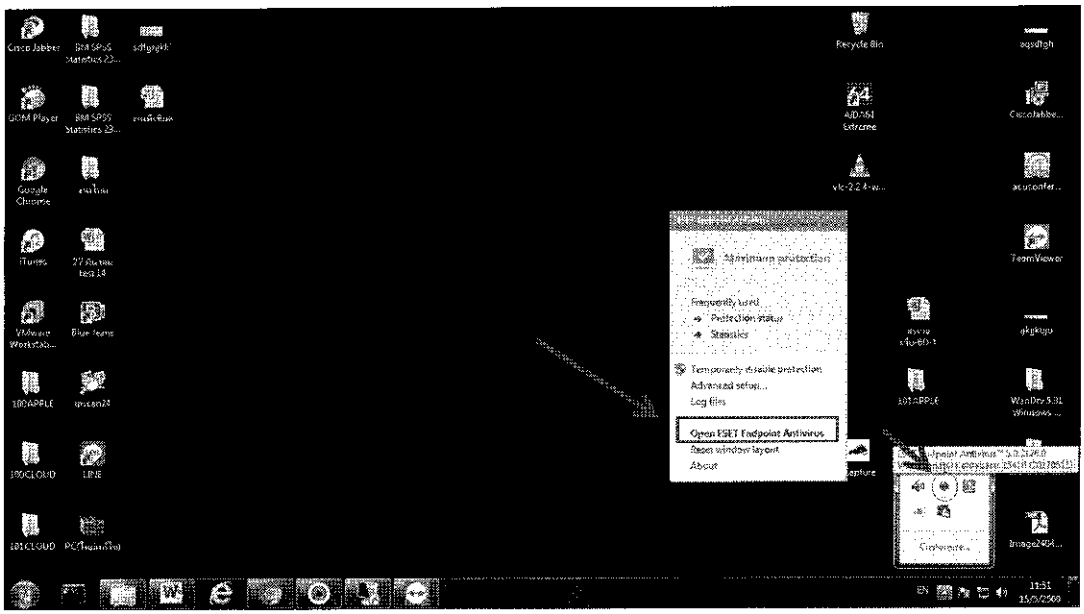


3. รีสตาร์ทเครื่อง

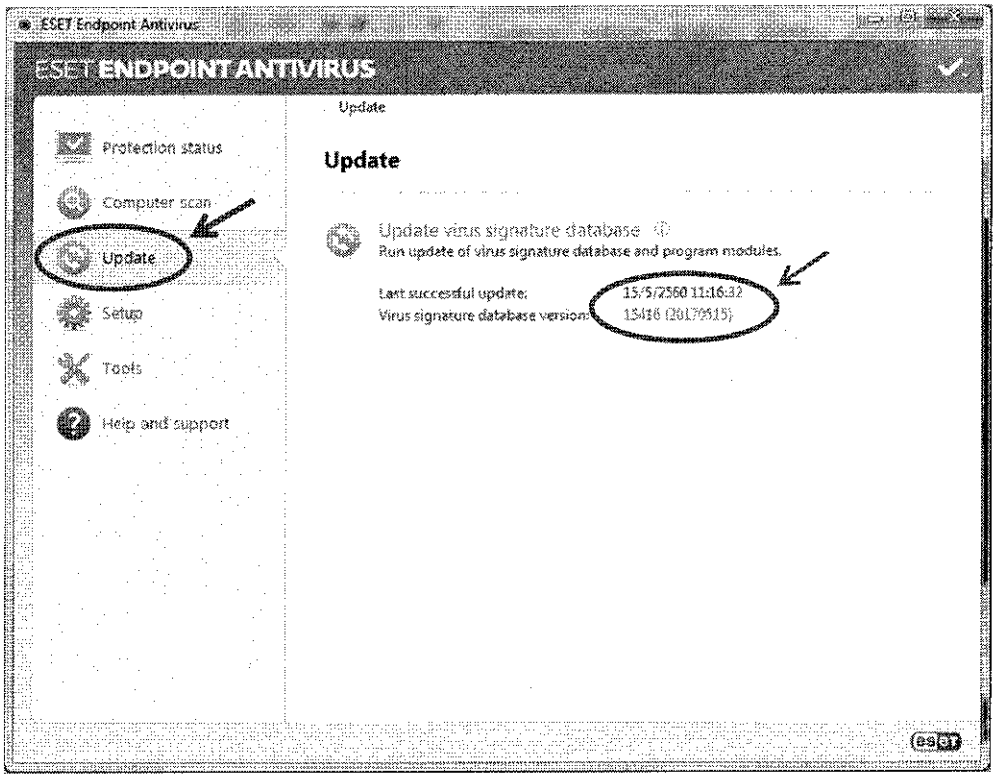
เอกสาร ๒

คู่มือการ Check Update Anti-Virus Note 32

1.เลือก ที่ ไอคอน ด้านล่าง ขวาของจอ แล้วคลิก **Open ESET ENDPOINT ANTIVIRUS**



2.คลิก Update แล้วดูการอัพเดทล่าสุด ถ้าอัพเดท จะเป็นวันเวลาล่าสุดที่คลิกเข้าไปดู



3.หากพบว่าAnti-Virusไม่ update ตามข้อสอง ให้คลิกที่ Update virus signature database เพื่อทำการ Update