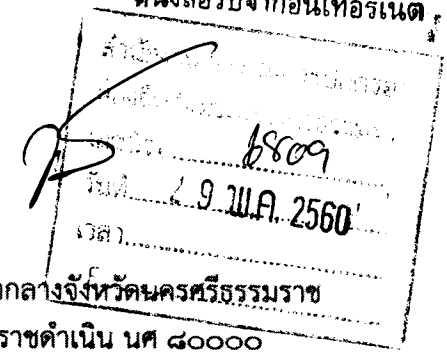
หนังสือรับจากอินเทอร์เน็ต



ด่วนที่สุด

ที่ นศ ๐๐๑๗.๒/ว ๓๒๕๐

ศาลากลางจังหวัดนครศรีธรรมราช
ถนนราชดำเนิน นศ ๘๐๐๐๐

๒๔ พฤษภาคม ๒๕๖๐

เรื่อง การป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดว์

เรียน หัวหน้าส่วนราชการทุกส่วนราชการ หัวหน้าหน่วยงานรัฐวิสาหกิจ นายอำเภอทุกอำเภอ นายกองค์การบริหารส่วนจังหวัดนครศรีธรรมราช นายกเทศบาลนครนครศรีธรรมราช นายกเทศมนตรีเมืองทุ่งสง เมืองปากพนัง เมืองปากพูน นายกเทศมนตรีตำบลและนายกองค์การบริหารส่วนตำบลทุกแห่ง

สิ่งที่ส่งมาด้วย แนวทางการป้องกันการติด Ransomware

ตามที่มีข่าวสารกระจายในวงกว้างถึงภัยจากการติดมัลแวร์เรียกค่าไถ่ (Ransomware) สายพันธุ์ชื่อ wannaCry โดยมัลแวร์ดังกล่าว มีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมด รวมถึงมีความสามารถในการกระจายตัวเองจากคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์ที่เกี่ยวข้องกับการบริหารแชร์ไฟล์ผ่านเครือข่าย (Server Message Block : SMB) ที่มีการเปิดให้บริการ นำมาเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้นั้น

เพื่อเป็นการป้องกันและเฝ้าระวังภัยมัลแวร์ดังกล่าว สำนักงานปลัดกระทรวงมหาดไทยได้จัดทำแนวทางในการป้องกัน ดังนี้

๑. แนวทางการป้องกันการติด Ransomware สำหรับผู้ดูแลระบบ

(๑) ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบันเสมอ เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware หากเป็นไปได้ควรหยุดใช้งานระบบปฏิบัติการ WindowsXP, Windows Server๒๐๐๓ และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ

(๒) กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือระบบที่สำคัญและไม่สามารถ Patch ได้ในทันที ควรทำการ Disable SMBv๑ หากไม่ได้ทำการใช้งาน

(๓) ปิด Port Remote การเข้าถึงผ่าน RDP(Remote Destop Protocol) และ SMB จาก Internet ของระบบที่มีความเสี่ยง

(๔) ติดตั้งแอนตี้ไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ

๒. แนวทางการป้องกันการติด Ransomware สำหรับผู้ใช้งาน

(๑) ไม่เปิดเอกสารแนบอีเมล์โดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมล์ควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมล์ฉบับนั้นมาจริง

(๒) เครื่องคอมพิวเตอร์ควร update Patch เดียวกัน เพื่อลดโอกาสที่ผู้ใช้งานจะนำ Mailware เข้ามาระบาด

/๓. ควรสำรองข้อมูล...

(๓) ควรสำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่าย (รายละเอียดตามสิ่งที่ส่งมาด้วย)

จึงเรียนมาเพื่อพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายชรเกียรติ รักพานิชมณี)
รองผู้ว่าราชการจังหวัด ปฏิบัติราชการแทน
ผู้ว่าราชการจังหวัดนครศรีธรรมราช

เรียน ท้องถิ่นจังหวัดนครศรีธรรมราช

เห็นควรประชาสัมพันธ์

ให้ ขก. กนว. สกจ. นศ ทราบ

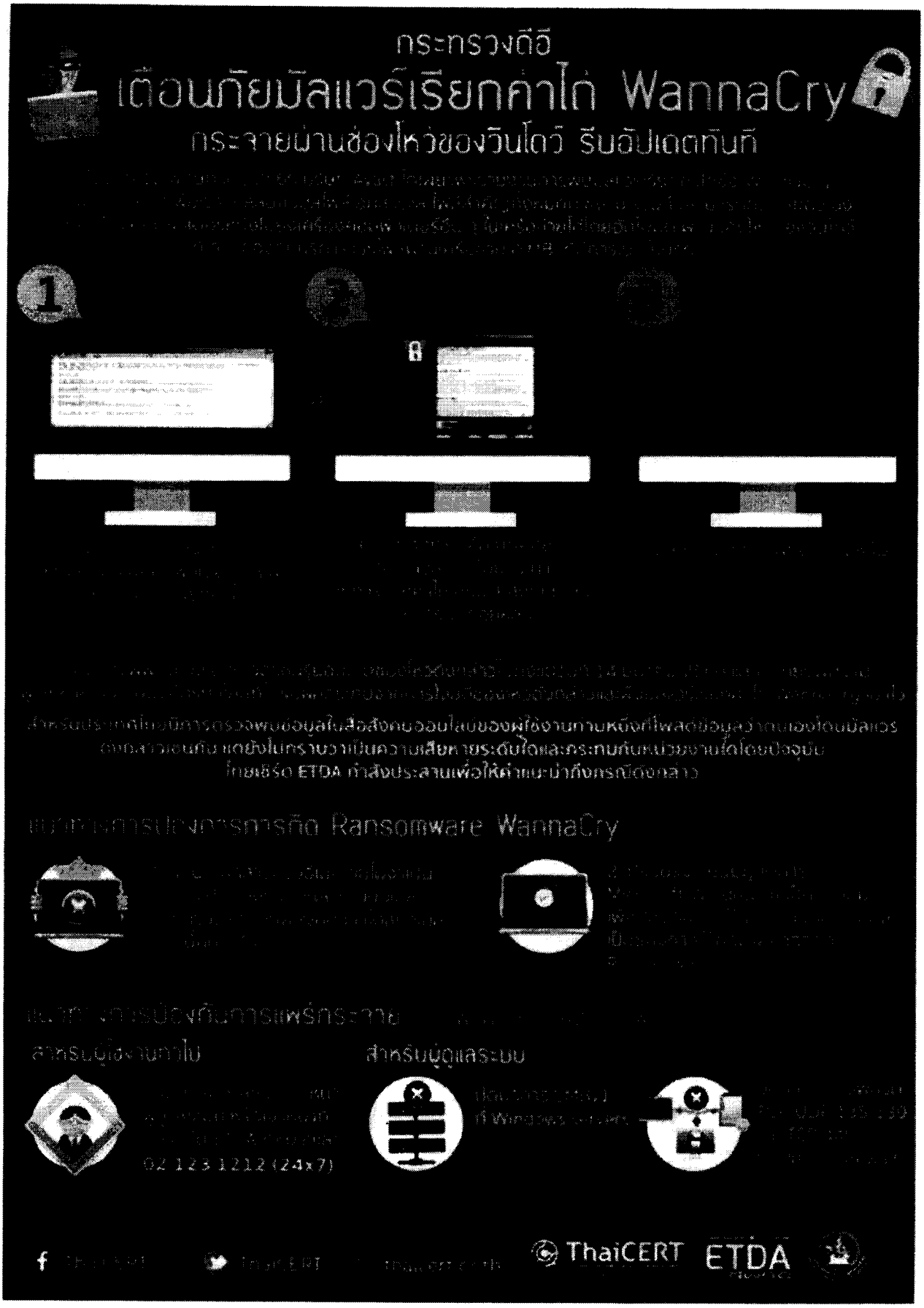
จึงเรียนมาเพื่อโปรดทราบและพิจารณา

ศิริชาติ ปิลกะนันธ์
๒๗ น.ค. ๒๕๖๐

(นายสุพจน์ จิตร์เพ็ชร์)
หัวหน้าฝ่ายบริหารทั่วไป
๒๗ พ.ค. ๖๐

(นายวิญญ์ สิทธิเชนทร์)
ท้องถิ่นจังหวัดนครศรีธรรมราช

สำนักงานจังหวัดนครศรีธรรมราช
กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
โทร. /โทรสาร ๐-๕๔๗๑-๖๓๘๗


กระทรวงดีอี
เตือนภัยมัลแวร์เรียกค่าไถ่ WannaCry
กระจายผ่านช่องโหว่ของวินโดว์ รีบอัปเดตทันที
ThaiCERT
ETDA

อันตราย: Ransomware WannaCry

ที่จะมาเข้ารหัสไฟล์ในเครื่องคอมพิวเตอร์เพื่อเรียกค่าไถ่



เช้าวันนี้ ก่อนทำงานกับคอมพิวเตอร์ ให้ปฏิบัติดังนี้

1. ถอดสาย LAN ออกจากเครื่องคอมพิวเตอร์ก่อน

   กรณีใช้ Wi-Fi ให้ปิดการใช้งาน Wi-Fi ของเครื่องคอมพิวเตอร์
   หรือ ปิดอุปกรณ์กระจายสัญญาณ Access Point ในที่ทำงาน
2. ทำการ Backup ข้อมูลสำคัญลงใน External Disk Drive
3. **ถอด**อุปกรณ์ External Disk Drive ออกจากคอมพิวเตอร์ เมื่อ Backup เสร็จ
4. ปิดการทำงานของบริการ SMB 1.0 (ที่เป็นช่องโหว่) โดยทำตามขั้นตอนตามภาพ
5. Restart คอมพิวเตอร์
6. เสียบสาย LAN หรือเปิด Wi-Fi ใช้ตามปกติ

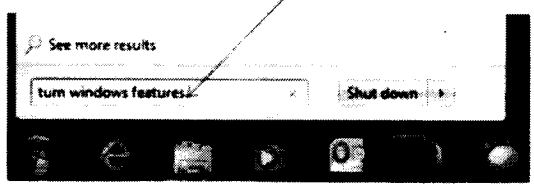
S.Natthawut

ขั้นตอนการปิดบริการ SMB 1.0 (ที่เป็นช่องโหว่)



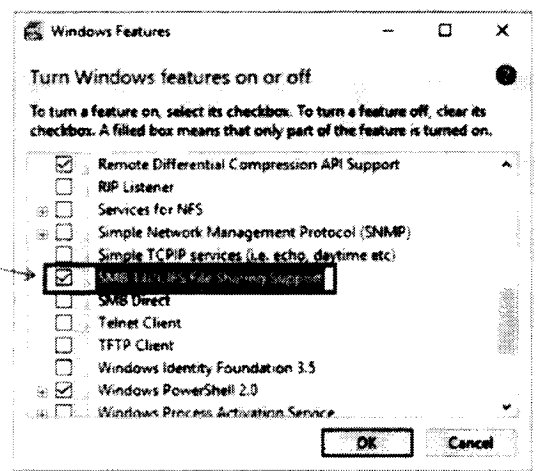
วิธีที่ 1: Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016

1. พิมพ์ "turn windows features" ลงในช่อง Search **แล้วกด Enter**



2. ติ๊กเครื่องหมาย**ออก**จากช่อง

เอาเครื่องหมายออก



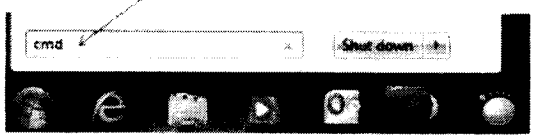
3. กด OK
4. Restart คอมพิวเตอร์

ขั้นตอนการปิดบริการ SMB 1.0 (ที่เป็นช่องโหว่)



วิธีที่ 2: Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012

1. พิมพ์ "cmd" ลงในช่อง Search **แล้วกด Enter**

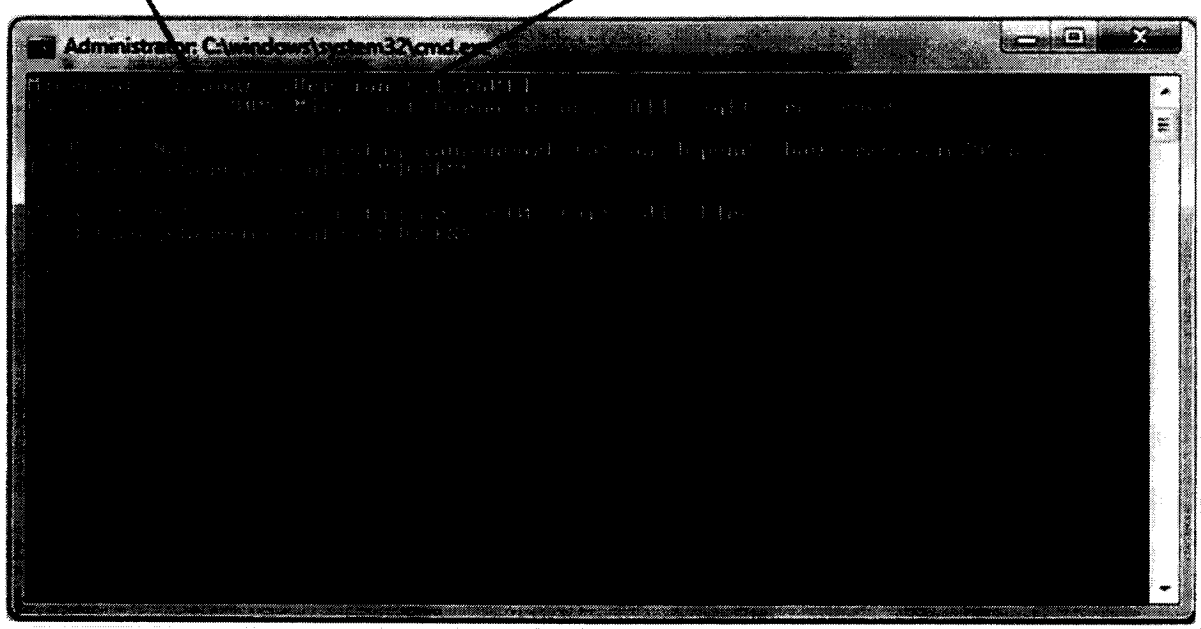


2. พิมพ์คำสั่งตามภาพถัดไป
3. Restart คอมพิวเตอร์

1. พิมพ์ "sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi" แล้วกด Enter

2. พิมพ์ "sc.exe config mrxsmb10 start= disabled" แล้วกด Enter

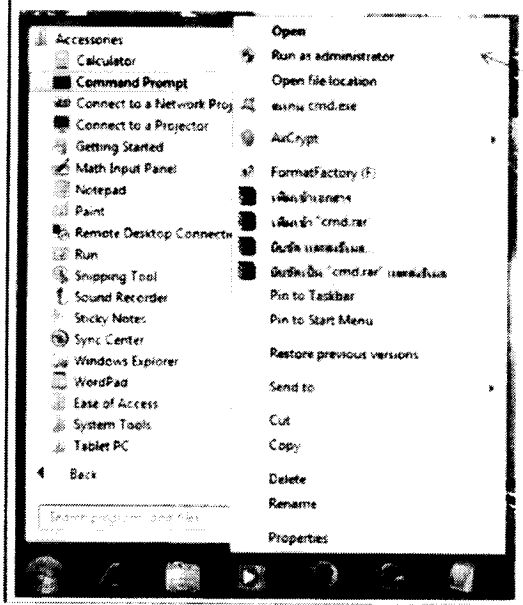
Disabled
มีตัว d ด้วย



ขั้นตอนการปิดบริการ SMB 1.0 (ที่เป็นช่องโหว่)



วิธีที่ 2: Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012



กรณีที่ผู้ใช้ไม่เป็น Admin

1. เลือก "All Programs/Accessories/Command Prompt" Click ขวา เลือกไปที่ "Run as administrator"
2. พิมพ์คำสั่งตามภาพถัดไป
3. Restart คอมพิวเตอร์

1. พิมพ์ "sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi" แล้วกด Enter

2. พิมพ์ "sc.exe config mrxsmb10 start= disabled" แล้วกด Enter

Disabled มีตัว d ด้วย

