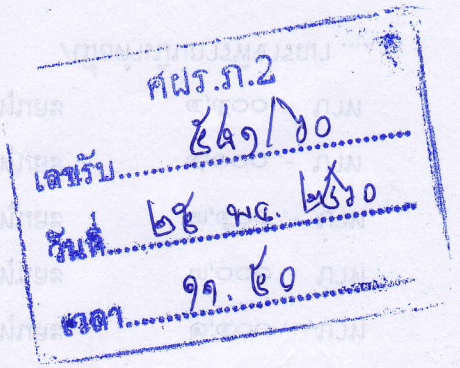
ด่วนที่สุด



สำเนาถูกต้อง
ที่ ๐๐๑๗.๑๙๒/๓๙๓๐
เรียน ผบช.ภ.๒
รอง ผบช.ภ.๒
เพื่อโปรดทราบ
ผบก. ในสังกัด ภ.๒

เพื่อทราบและดำเนินการตามหนังสือ ตร. ด่วนที่สุด ที่ ๐๐๓๓.๓๓/๑๖๙๔ ลง ๑๘ พ.ค.๖๐ เรื่อง มาตรการป้องกันคอมพิวเตอร์จากแรนซัมแวร์ WannaCry ซึ่งแรนซัมแวร์ดังกล่าวกำลังระบาดไปทั่วโลก เพื่อให้การป้องกันเป็นไปอย่างมีประสิทธิภาพและทันต่อเหตุการณ์ไม่เกิดความเสียหายต่อทางราชการ จึงให้ทุกหน่วยเร่งดำเนินการตามมาตรการฯ รายละเอียดปรากฏตามสำเนาเอกสารที่แนบมาพร้อมนี้ จำนวน ๖ แผ่น

พล.ต.ต.
(อังกูร พูลเจริญ)
รอง ผบช.ฯ ปรท.ผบช.ภ.๒
๒๕ พ.ค.๖๐

ด่วนที่สุด

ส่วนราชการ ตร.

ที่ ๐๐๓๓.๓๓/๑๖๙๔

บันทึกข้อความ

โทร. ๐ ๒๒๐๕ ๒๖๒๘

วันที่ 18 พฤษภาคม ๒๕๖๐

ศูนย์สื่อสาร ก.๒
เลขที่รับ 157
วันที่ 22 พ.ค 60
เวลา 11.54

ตำรวจภูธรภาค ๒
เลขที่รับ 4275
วันที่ 22 พ.ค. 2560
เวลา 15.05

เรื่อง มาตรการป้องกันคอมพิวเตอร์จากแรนซัมแวร์ WannaCry

เรียน จตช., รอง ผบ.ตร. หรือตำแหน่งเทียบเท่า
ผู้ช่วย ผบ.ตร. หรือตำแหน่งเทียบเท่า
- เพื่อโปรดทราบ
ผบช. หรือตำแหน่งเทียบเท่า
ผบก.ในสังกัด สง.ผบ.ตร.

จากเหตุการณ์กรณีมีแรนซัมแวร์เรียกค่าไถ่ ชื่อ WannaCry (หรือในชื่ออื่น WCry, WanaCryptor, WannaCrypt, Wana Decryptor) ระบาดไปทั่วโลก มากกว่า ๑๐๐ ประเทศ ทั้งในโรงพยาบาล องค์กรด้านคมนาคม และองค์กรหรือหน่วยงานอื่นๆ ในหลายประเทศ เช่น สหรัฐอเมริกา อังกฤษ เยอรมัน สเปน จีน ไต้หวัน ฯลฯ มัลแวร์ตัวนี้ สร้างขึ้นโดยกลุ่มแฮ็คเกอร์ Shadow Brokers ฉกฉวยช่องโหว่ของระบบปฏิบัติการ Windows ของ Microsoft ที่มีชื่อเรียกว่า ระบบ SMBv1 (Server Message Block) แรนซัมแวร์ชนิดนี้จะเข้ารหัสไฟล์ของผู้ใช้คอมพิวเตอร์ ทำให้ไม่สามารถเปิดไฟล์ได้ หากต้องการเปิดใช้งานไฟล์จะต้องจ่ายค่าไถ่ผ่านทาง Bitcoin และสามารถกระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นในเครือข่ายเดียวกัน แม้ผู้ใช้จะไม่ได้โหลดหรือเปิดแรนซัมแวร์ตัวนี้เลย สร้างความเดือดร้อนให้ผู้ใช้คอมพิวเตอร์ทั่วโลกรวมทั้งประเทศไทย

เพื่อให้การป้องกันแรนซัมแวร์ WannaCry ดังกล่าว เป็นไปอย่างมีประสิทธิภาพและทันต่อสถานการณ์ จึงให้ทุกหน่วยเร่งดำเนินการตามมาตรการดังนี้

๑. อัปเดตระบบปฏิบัติ Windows ให้เป็นปัจจุบัน โดยติดตั้งแพตช์แก้ไขช่องโหว่ SMBv1 จาก Microsoft โดย Windows Vista, Windows Server 2008 ถึง Windows 10 และ Windows Server 2016 ดาวน์โหลดอัปเดตได้จากhttps://technet.microsoft.com/en-us/library/security/ms17-010.aspx ส่วน Windows XP และWindows Server 2003 ดาวน์โหลดอัปเดตได้จาก https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

๒. กรณีไม่สามารถอัปเดตระบบปฏิบัติ Windows ให้ปิดการใช้งาน SMBv1 ซึ่งเป็นช่องโหว่ของระบบปฏิบัติการ Windows ที่ทำให้แรนซัมแวร์ WannaCry เข้าถึงระบบคอมพิวเตอร์ได้ วิธีการปิด SMBv1 รายละเอียดขั้นตอนการปฏิบัติ ตามเอกสารแนบ ๑

๓. ตั้งค่า Firewall เพื่อบล็อกการเชื่อมต่อกับไอพีแอดเดรสปลายทางตามตารางเอกสารแนบ ๒ เนื่องจากเป็นไอพีที่ถูกใช้ในการแพร่กระจายและควบคุมมัลแวร์

๔. ติดตั้งแอนติไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ ปัจจุบันแอนติไวรัสส่วนใหญ่ (รวมถึง Windows Defender ของ Microsoft) สามารถตรวจจับและกำจัด มัลแวร์ WannaCry สายพันธุ์ที่กำลังมีการแพร่ระบาดได้แล้ว

๕. หากเครื่องคอมพิวเตอร์ได้ติด แรนซัมแวร์ WannaCry แล้ว ให้ปฏิบัติตาม เอกสารแนบ ๓

หากมีข้อสงสัยหรือต้องการรายละเอียดเพิ่มเติมให้ประสาน พ.ต.อ.พิษณุ สิทธิพูรย์ ผกก.กลุ่มงานอินเทอร์เน็ต บก.สสท. หมายเลขโทรศัพท์ ๐๖ ๑๙๓๙ ๒๙๔๕ หรือว่าที่ ร.ต.อ.เทียนชัย เข็มงาม รอง สว. กลุ่มงานอินเทอร์เน็ต บก.สสท. หมายเลขโทรศัพท์ ๐๘ ๕๐๔๗ ๓๓๖๖ หรือ ๐ ๒๒๐๕ ๒๖๒๘

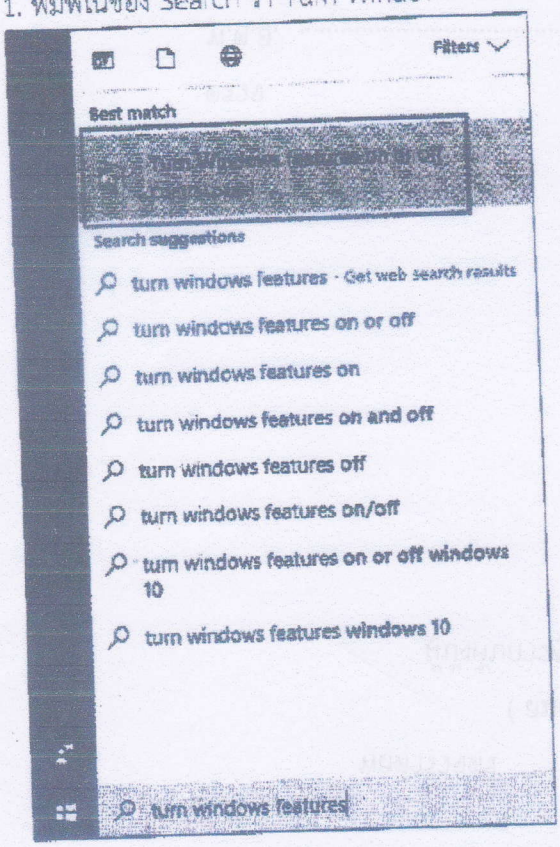
จึงแจ้งมาเพื่อทราบ และดำเนินการในส่วนที่เกี่ยวข้องต่อไป

พล.ต.ท.
(ชนิตศักดิ์ ธีระสวัสดิ์)
ผู้ช่วย ผบ.ตร.ปรท.ผบ.ตร

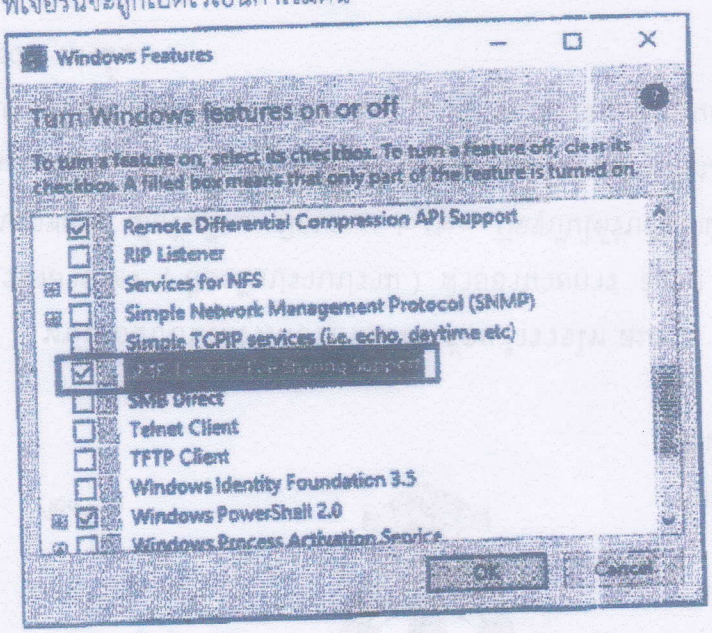
การปิด SMBv1

ขั้นตอนการปิด SMBv1 ใน Windows 8.1, Windows 10, Windows Server 2012 R2 และ Windows Server 2016 ดังนี้

1. พิมพ์ในช่อง Search ว่า Turn Windows features on or off ตามภาพ

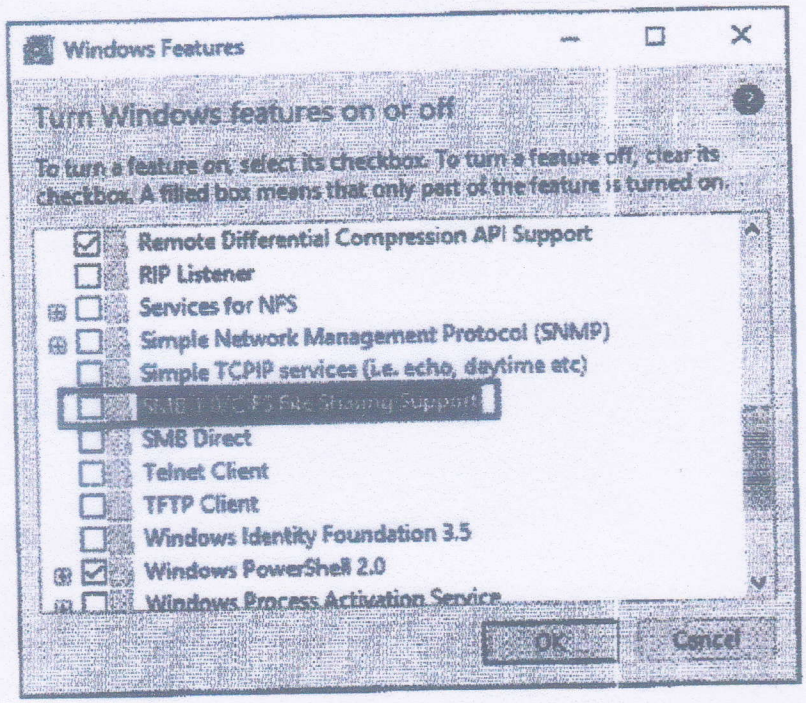


2. หน้าต่าง Windows Features จะเปิดขึ้นมา ให้หาข้อความ "SMB 1.0/CIFS File Sharing Support" โดย ฟีเจอร์นี้จะถูกเปิดไว้เป็นค่าเริ่มต้น



3

ให้นำติ๊กถูกออกจากช่องสี่เหลี่ยม และกด OK

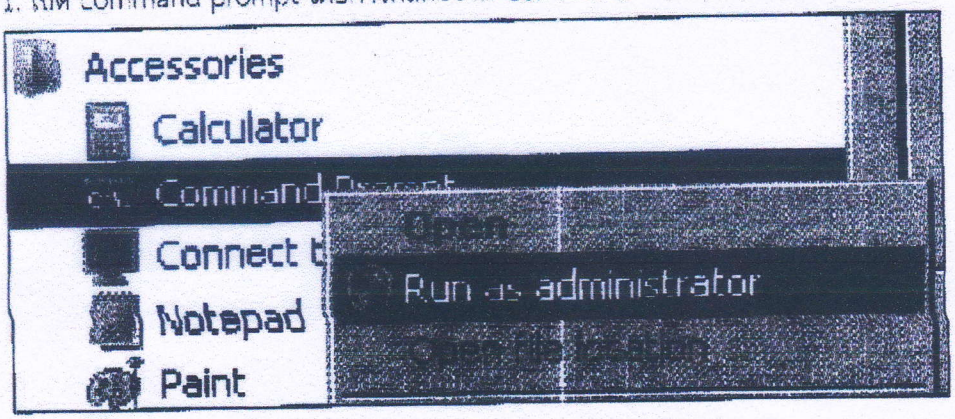


จากนั้น ให้ทำการ รีสตาร์ทเครื่อง 1 ครั้ง

4

ขั้นตอนการปิด SMBv1 ใน Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 และ Windows Server 2012 ดังนี้

1. เปิด 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 1 ครั้ง

เอกสาร ๒

5

การตั้งค่า Firewall เพื่อบล็อกการเชื่อมต่อกับไอพีแอดเดรสปลายทาง เนื่องจากเป็นไอพีที่ถูกใช้ในการแพร่กระจายและควบคุมมัลแวร์

ไอพีแอดเดรสปลายทาง	พอร์ตปลายทาง	ประเทศ
213.61.66.116	9003/TCP	Germany
171.25.193.9	80/TCP	Sweden
163.172.35.247	443/TCP	United Kingdom
128.31.0.39	9101/TCP	United States
185.97.32.18	9001/TCP	Sweden
178.62.173.203	9001/TCP	European Union
136.243.176.148	443/TCP	Germany
217.172.190.251	443/TCP	Germany
94.23.173.93	443/TCP	France
50.7.151.47	443/TCP	United States
83.162.202.182	9001/TCP	Netherlands
163.172.185.132	443/TCP	United Kingdom
163.172.153.12	9001/TCP	United Kingdom
62.138.7.231	9001/TCP	Germany

๖

เอกสาร ๓

6

ข้อแนะนำในการแก้ไขหากตกเป็นเหยื่อ

1. หากพบว่าเครื่องคอมพิวเตอร์ตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่ WannaCry ให้ตัดการเชื่อมต่อเครือข่าย (ถอดสาย LAN, ปิด WI-FI) และปิดเครื่องทันที

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

3. หากเป็นได้ได้ควรหยุดใช้งานระบบปฏิบัติการ Windows XP, Windows Server 2003 และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ

4. หมั่นตรวจสอบข้อมูลจากเว็บไซต์ NoMoreRansom.org รอจนกระทั่งมีการพัฒนาโปรแกรมสำหรับถอดรหัสข้อมูลออกมา แล้วนำไปใช้ถอดรหัสข้อมูลที่ถูกเรียกค่าไถ่ เพื่อกู้คืนข้อมูลกลับคืนมา

5. ติดตั้งระบบปฏิบัติการลงในฮาร์ดดิสก์ลูกใหม่และใช้ทำงานต่อไป