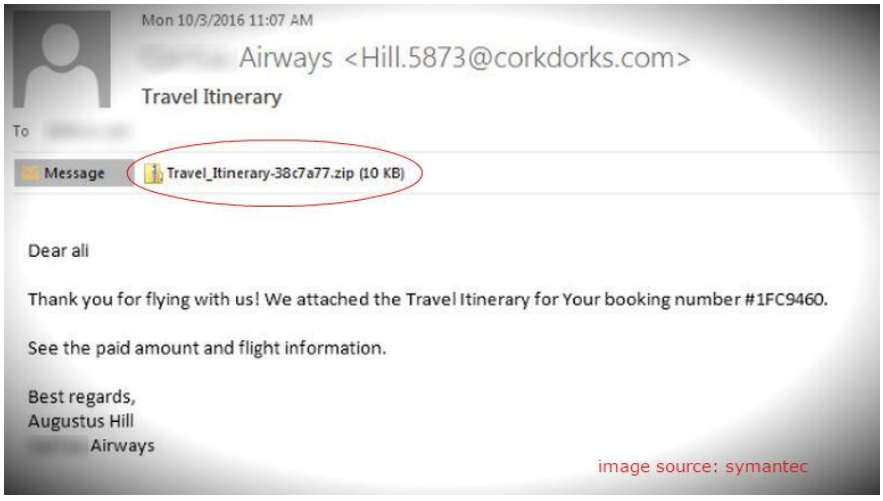
แนวทางการป้องกันการติด Wanacrypt Ransomware

แสดงภาพ Wanacrypt Ransomware

1. ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมล ควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลฉบับนั้นมาจริง

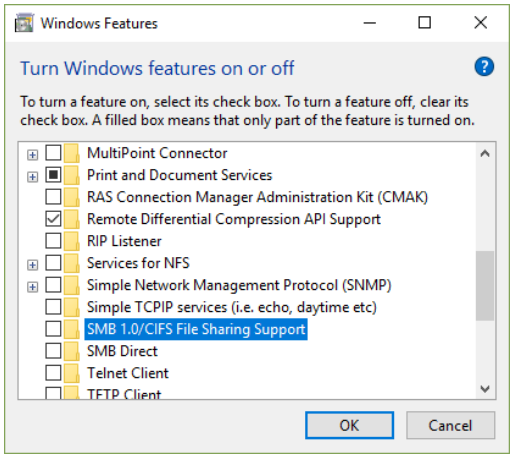


แสดงอีเมลพร้อมไฟล์แนบที่อาจจะมี Wanacrypt แผงมา

2. ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบัน เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware โดยสามารถดาวน์โหลดรายการอัปเดตแพทช์ MS17-010 ของ Microsoft Windows รุ่นอื่นๆ ได้ที่นี่

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ และ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

3. ปิดบริการ SMBv1 ทั้ง Microsoft Windows

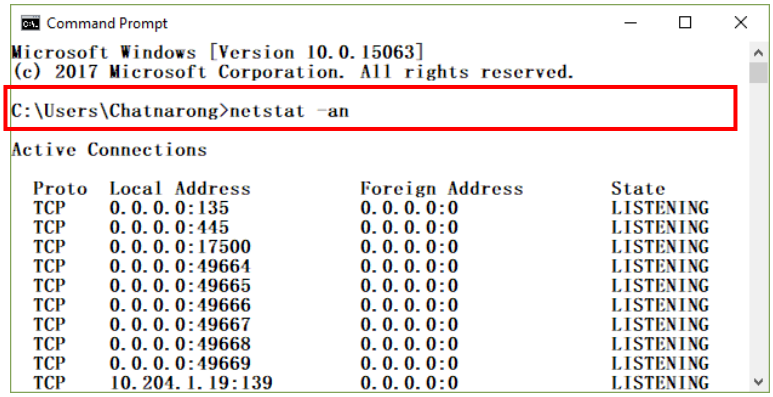


แสดงการปิดบริการ SMBv1 บน Windows 10

วิธีการปิด SMBv1 บนระบบปฏิบัติการ Windows รุ่นอื่นๆ เข้าไปดูได้ที่ https://support.microsoft.com/th-th/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

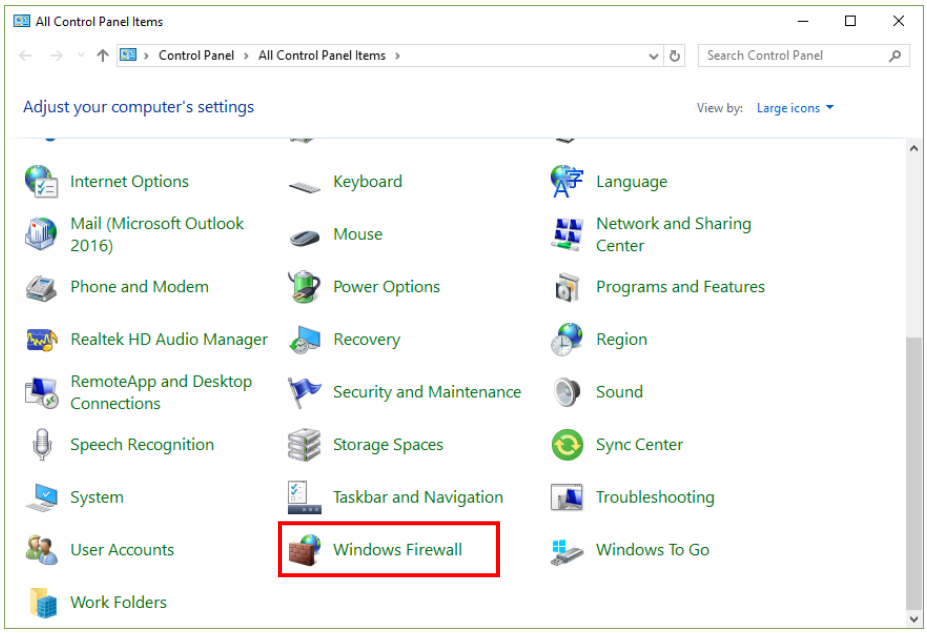
4. ปิด Port 135, 138, 139, 445 ซึ่งเป็น Port ที่ Wanacrypt Ransomware ใช้เป็นช่องทางในการโจมตี

4.1 เปิด Command Prompt แล้วพิมพ์คำสั่ง netstat –an



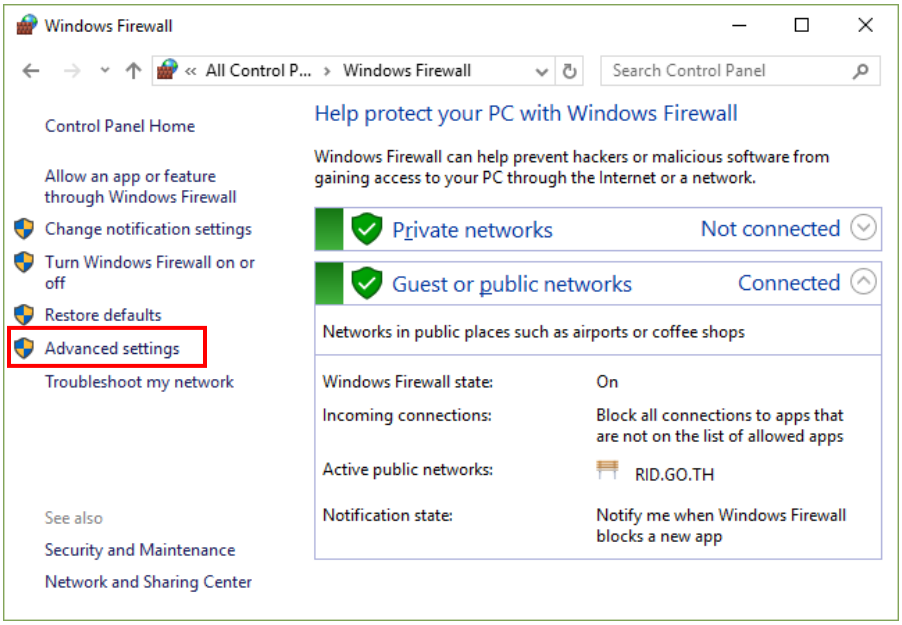
แสดงการใช้คำสั่ง netstat -an เพื่อตรวจสอบว่าระบบปฏิบัติการได้เปิด Port 135, 138, 139 และ 445 หรือไม่

4.3 เปิด Control Panel แล้วคลิก Windows Firewall



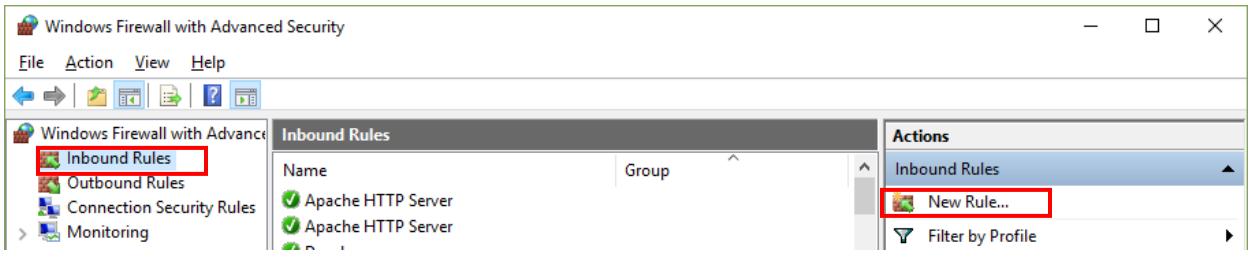
แสดงหน้าต่าง Control Panel

4.3 คลิก Advance Setting



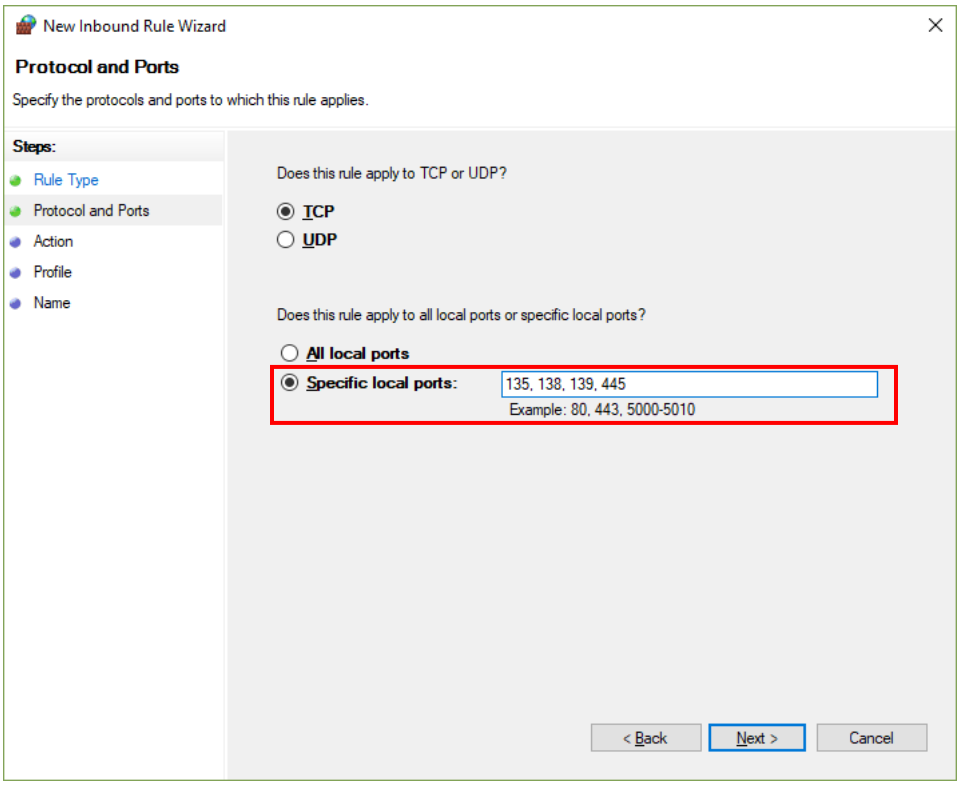
แสดงหน้าต่าง Windows Firewall

4.4 คลิก Inbound Rule แล้วคลิก New Rule... ที่แถบ Action



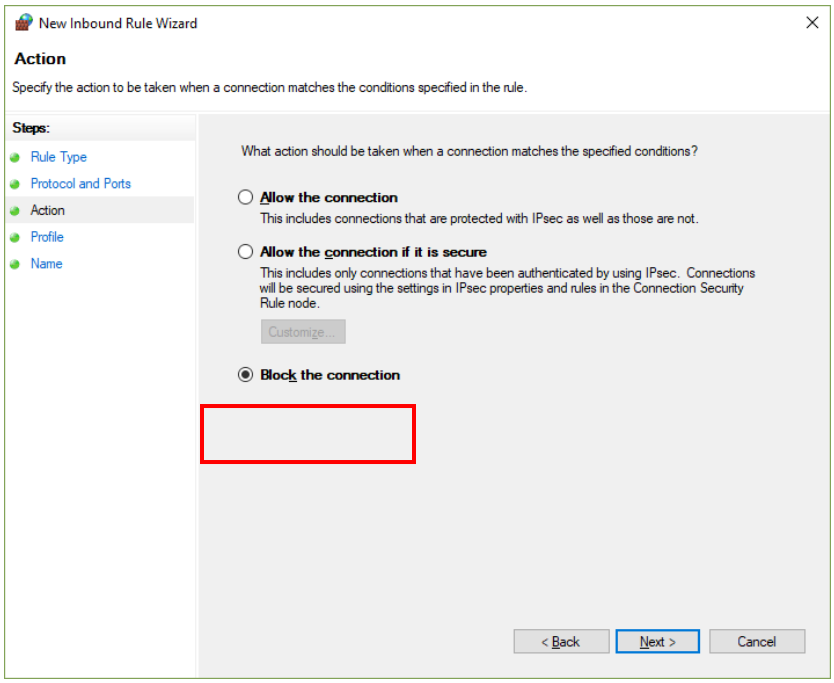
แสดงหน้าต่าง Windows Firewall with Advance Security

4.5 คลิก Protocol and Ports แล้วคลิกเลือกหัวข้อ Specific local ports: พิมพ์หมายเลข Port 135, 138, 139 และ 445 จากนั้นคลิก Next



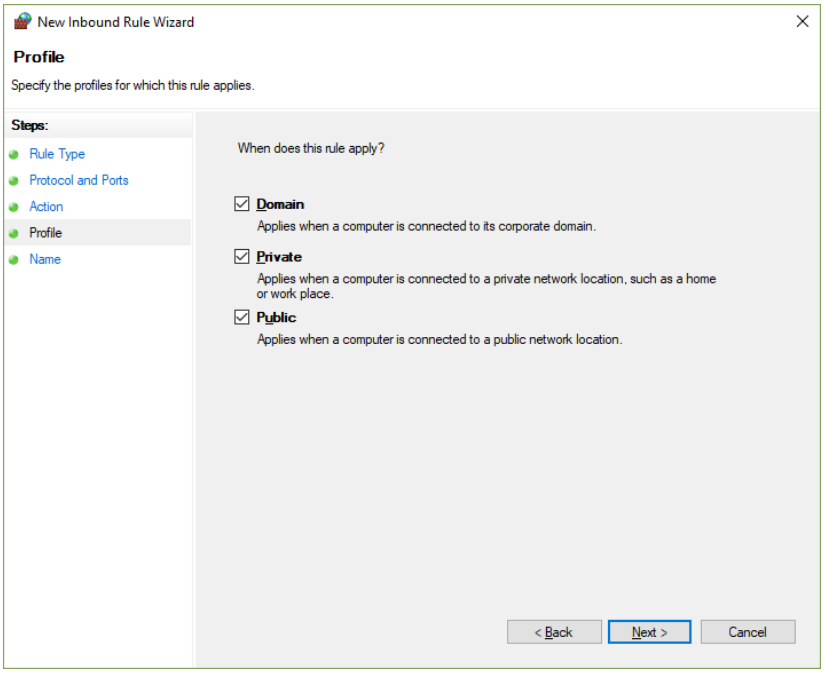
แสดงหน้าต่าง New Inbound Rule Wizard ขั้นตอน Protocol and Ports

4.6 คลิก Block the connection



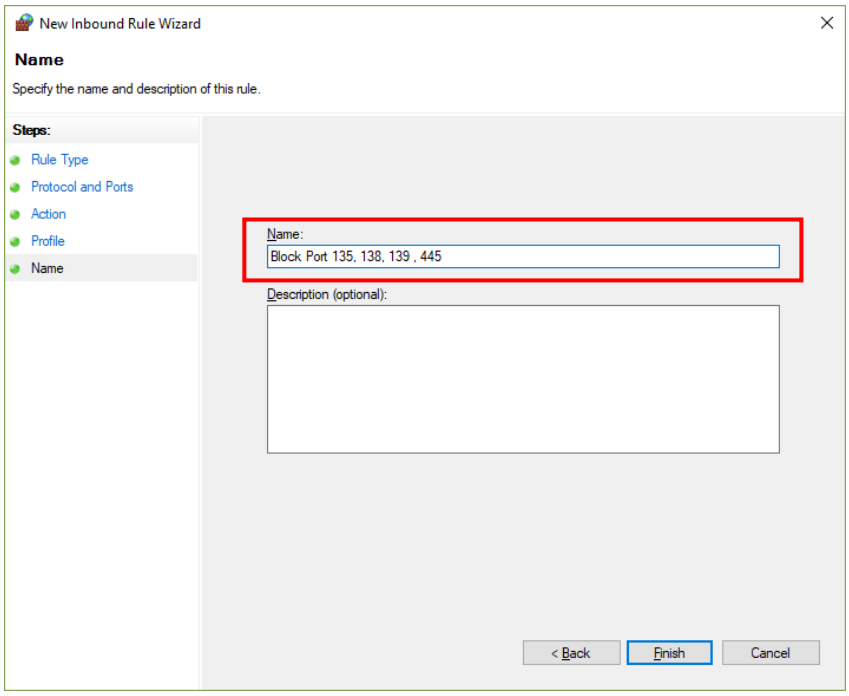
แสดงหน้าต่าง New Inbound Rule Wizard ขั้นตอน Action

4.7 คลิกเลือก Check box ทั้ง 3 ข้อ แล้วคลิก Next



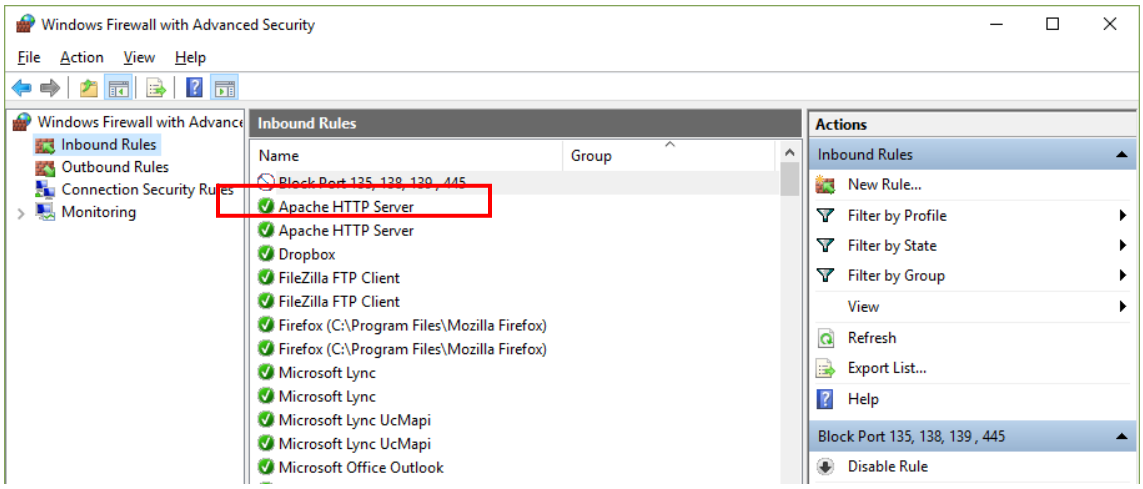
แสดงหน้าต่าง New Inbound Rule Wizard ขั้นตอน Profile

4.7 ใช่ชื่อกฎตามที่ต้องการ ในที่นี้ใส่เป็น Block Ports 135, 138, 139, 445 จากนั้นคลิก Finish



แสดงหน้าต่าง New Inbound Rule Wizard ขั้นตอน Name

4.8 กลับมาที่หน้าต่าง Windows Firewall with Advanced Security จะเห็นว่ามีกฎใหม่ที่เราสร้างขึ้นมา



แสดงหน้าต่าง Windows Firewall with Advanced Security ที่มีรายการกฎของ Firewall

เอกสารอ้างอิง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (Online). https://www.etda.or.th/content/wannacry-ransomware-outbreak.html [2017, May 13].

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (Online). https://www.thaicert.or.th/alerts/user/2017/al2017us001.html [2017, May 13].

Bessie Shaw (Online). http://www.drivethelife.com/windows-drivers/fix-prevent-wannacry-ransomware-windows-10-8-7-vista-xp.html [2017, May 18].

TechTalkThai (Online). https://www.techtalkthai.com/wana-decrypt0r-2-0-technical-note/ [2017, May 13].

TechTalkThai (Online). https://www.techtalkthai.com/disabling-smbv1-guide-for-windows-from-microsoft/ [2017, May 14].