แนวทางการป้องกันไวรัสเรียกค่าไถ่ WannaCry

สำหรับผู้ใช้งานเครือข่ายคอมพิวเตอร์ในหน่วยงานสาธารณสุขทุกระดับ โดย งานเทคโนโลยีสารสนเทศ สสจ.บุรีรัมย์

อาการแสดงเมื่อติดไวรัส WannaCry (วอนนาคราย)

WannaCry ทำงานโดยจะเข้าไปล็อกไฟล์ข้อมูล ทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ได้และเรียกร้องเงินค่าไถ่ 300 ดอลลาร์สหรัฐฯ ในสกุลเงินดิจิทัลบิทคอยน์ (Bitcion) เพื่อแลกกับคีย์ปลดล็อกรหัสไฟล์ โดยแสดงเป็นป้อบอั้บ ดังภาพ ทั้งยังมีความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์ที่เกี่ยวข้องกับบริการแชร์ไฟล์ผ่านเครือข่าย (SMB) ที่มีการเปิดให้บริการ

*** ขณะนี้ ยังไม่มีวิธีแก้ไข ***

การป้องกัน สำหรับผู้ใช้ (User)

1. ห้ามเปิดอีเมล์จากผู้ส่งที่ไม่รู้จัก
2. ห้ามเปิดไฟล์แนบจากอีเมล์, เฟสบุ๊ค, ไลน์ หรือจากสื่อโซเชียลต่างๆ ที่ไม่จำเป็นในงาน ไม่ว่าจะมาจากผู้ส่งใดก็ตาม
3. ห้ามดาวน์โหลดซอฟแวร์หรือไฟล์ต่างๆ ที่ไม่จำเป็นในงาน จากอินเตอร์เน็ต
4. ห้ามใช้โปรแกรมช่วยดาวน์โหลดต่างๆ
5. ห้ามใช้โปรแกรมดาวน์โหลด bittorrent
6. สำรองข้อมูลสำคัญจากเครื่องคอมฯ ไปเก็บยังแหล่งเก็บข้อมูลอื่น เช่น handy drive , external drive หรือ Cloud
7. ติดต่อผู้ดูแลระบบของหน่วยงาน ให้ทำการปรับปรุง windows, ติดตั้งซอฟต์แวร์ป้องกัน WannaCry ชั่วคราว ของมหาวิทยาลัยเทคโนโลยีสุรนารี และตรวจสอบการทำงาน/อับเดตซอฟแวร์สแกนไวรัสของเครื่องคอมฯ ให้เป็นปัจจุบัน
8. หากพบอาการติดไวรัส จะแสดงป้อบอั้บดังภาพ ให้รีบถอดสายแลนออกจากเครื่อง หรือปิดไวเลส แล้วรีบแจ้งผู้ดูแลระบบทันที

สำหรับผู้ดูแลระบบ (Admin)

1. การจัดการที่เครื่องลูกข่าย windows / windows server

1.1 สำหรับ windows 7 , 10 และ server 2007 ขึ้นไป ให้ทำการอับเดต OS ให้เป็นปัจจุบัน

1.2 สำหรับ Windows XP, Windows 8 และ Windows Server 2003 ให้ดาวน์โหลดไฟล์ Patch มาติดตั้ง จากเวบไซต์นี้ https://www.techtalkthai.com/microsoft-releases-patches-to-protect-from-wannacrypt-ransomware-for-windows-xp-8-and-windows-server-2003/

1.3 ติดตั้งซอฟต์แวร์ป้องกัน WannaCry ชั่วคราว ของมหาวิทยาลัยเทคโนโลยีสุรนารี ที่ https://github.com/chanwit/wannacry_blocker/releases/download/v4/block_wannacry.zip และศึกษารายละเอียดเกี่ยวกับซอฟแวร์นี้ที่ https://www.facebook.com/SUTAiyaraCluster/posts/1166096956833650

1.4 ตรวจสอบการทำงานและอับเดตซอฟแวร์สแกนไวรัสของเครื่องคอมฯ ให้เป็นปัจจุบัน แต่ขณะนี้พบว่ามีเพียงซอฟแวร์สแกนไวรัสที่มีความสามารถสแกนเครือข่ายและไฟร์วอลเท่านั้น จึงจะสามารถป้องกัน WannaCry ได้ (มี firewall and network protection module) เช่น ESET NOD32 Antivirus V6 จะป้องกันไม่ได้ แต่ ESET Endpoint Security v6 ป้องกันได้ เป็นต้น

1.5 สำหรับเครื่อง windows 10 ที่เปิดใช้งาน Windows Defender (ป้องกันได้) ให้อับเดตให้เป็นปัจจุบัน

1.6 งดการแชร์ไฟล์ผ่านเครือข่าย โดยยกเลิกการแชร์ไฟล์หรือโฟลเดอร์ที่เครื่องลูกข่ายทั้งหมด

1.7 พิจารณายกเลิกบริการ SMB Server และปิดบริการ SMB ของเครื่อง windows server

1.8 พิจารณายกเลิกบริการ NAS (Network Attached Storage) หากจำเป็นต้องใช้ ให้เลือก NAS ที่มีระบบสแกนไวรัสในตัวเอง

1.9 สำรองข้อมูลสำคัญจากเครื่อง ไปเก็บยังแหล่งเก็บข้อมูลอื่นที่ไม่ใช่คอมพิวเตอร์

1.10 หากพบเครื่องติด WannaCry ให้ถอดเครื่องออกจากเครือข่ายทันที และรอติดตามข่าวสาร *เนื่องจากยังไม่มีวิธีแก้ไข*

2. การจัดการที่ Router / Firewall

2.1 ปิดกั้น IP และ port ตามเวบไซต์นี้ https://www.thaicert.or.th/alerts/user/2017/al2017us001.html

2.2 ปิดกั้นพอร์ต SMB (TCP 137, 139 และ 445 , UDP 137 และ 138) จากเครือข่ายภายนอก

2.3 อนุญาตเฉพาะ port ใช้งาน เช่น TCP/3306 และ port สำหรับ sync data ของแต่ละหน่วยงาน เป็นต้น

2.4 พิจารณาปิดกั้นการใช้งานอินเตอร์เน็ตของเครื่องลูกข่าย/แม่ข่าย ให้เชื่อมต่อได้เพียง server ภายในเท่านั้น หรืออนุญาตเฉพาะบางปลายทาง หรือบางเครื่อง เช่น อนุญาตเฉพาะเครื่องที่ต้องใช้ตรวจสอบสิทธิ์ หรือ refer online ออกอินเตอร์เน็ตได้เฉพาะปลายทางนั้นๆ เท่านั้น, อนุญาตเฉพาะการ sync มา สสจ. เท่านั้น เป็นต้น

2.5 ติดตามข้อมูลข่าวสาร WannaCry ทางสื่อต่างๆ และทาง https://www.facebook.com/groups/308103775874306/

สำหรับผู้ดูแลด้านเทคโนโลยีสารสนเทศ

1. เสนอข้อมูลต่อผู้บริหารองค์กร ให้เห็นถึงความจำเป็นในการจำกัดการใช้งานเครือข่ายอินเตอร์เน็ทร่วมกันภายในองค์กร เพื่อความปลอดภัย ป้องกันภาวะคุกคามทางไซเบอร์และเป็นไปตาม พรบ.คอมพิวเตอร์ ปี 2560 โดยเสนอให้กำหนดเป็นนโยบายองค์กรให้ชัดเจน เช่น การปิดกั้นการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม/ปลอดภัย, ปิดกั้นเกมส์ออนไลน์, ปิดกั้นการดาวน์โหลดไฟล์จากแหล่งที่ไม่ปลอดภัย ด้วยวิธี Peer to Peer เช่น bittorrent , กำหนดนโยบายการใช้ social media ต่างๆ ให้ชัดเจน รวมถึงการห้ามใช้ USB drive ในการคัดลอกไฟล์จากเครื่องสู่เครื่อง ให้ใช้การส่งทางอีเมล์ หรือบริการฝากไฟล์บน Cloud แบบฟรีที่มีการสแกนไวรัสแทน เป็นต้น

2. เสนอให้องค์กรจัดหาระบบป้องกันไวรัสที่มีลิขสิทธิ์ถูกต้อง เพื่อให้สามารถอับเดตและรับบริการต่างๆ จากเจ้าของผลิตภัณฑ์ได้