(3)

ด่วนที่สุด

ที่ สน ๐๐๑๗.๒/ ว ๑๐๖๐๓

ศาลากลางจังหวัดสกลนคร
ถนนศูนย์ราชการ สน ๔๗๐๐๐

๑๕ พฤษภาคม ๒๕๖๐

เรื่อง การติดตามและเฝ้าระวังการแพร่กระจายของมัลแวร์เรียกค่าไถ่ หรือ Ransomware WannaCry

เรียน หัวหน้าส่วนราชการสังกัดบริหารราชการส่วนกลาง, หัวหน้าส่วนราชการสังกัดบริหารราชการส่วนภูมิภาค, นายกองค์การบริหารส่วนจังหวัดสกลนคร, นายกเทศมนตรีนครสกลนคร และนายอำเภอทุกอำเภอ

สืบเนื่องจากพฤติกรรมการโจมตีของ Ransomware WannaCry ซึ่งจะระบาดผ่านช่องโหว่ของระบบปฏิบัติการวินโดว์ที่ไม่อัพเดตหรือไม่ปรับระบบ โดยมัลแวร์ดังกล่าวมีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเป็นเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้ โดยมัลแวร์ชนิดนี้ยังสามารถกระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่ายโดยอัตโนมัติ ซึ่งอาจก่อให้เกิดผลเสียหายอย่างรุนแรงต่อข้อมูลหรือระบบงานที่มีความสำคัญ ในการนี้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้มีแนวทางการป้องกันการติด Ransomware WannaCry ดังนี้

๑. ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมลควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลฉบับนั้นมาจริง

๒. ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบันเพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware

๓. หากพบการติด Ransomware แล้ว ให้ดำเนินการดังนี้

๓.๑ สำหรับผู้ใช้งานทั่วไป ให้ปิดเครื่องและแจ้งเจ้าหน้าที่ผู้ดูแลระบบ หรือเจ้าหน้าที่ไทยเซิร์ต ETDA ที่หมายเลข ๐๒-๑๒๓ ๑๒๑๒

๓.๒ สำหรับผู้ดูแลระบบ ให้ปิดบริการ SMBv1 ที่ Windows Servers และปิดการเข้าถึงพอร์ต TCP/UDP 135-139 และ TCP 445 ที่อุปกรณ์ Firewall

เพื่อให้การติดตามและเฝ้าระวังการระบาดของมัลแวร์ Ransomware WannaCry ไม่ให้เกิดความเสียหายต่อข้อมูลและระบบปฏิบัติงานที่สำคัญ จึงให้ส่วนราชการปฏิบัติตามแนวทางการป้องกันการติดมัลแวร์ Ransomware WannaCry ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมโดยเคร่งครัดต่อไป ทั้งนี้ให้อำเภอแจ้งองค์กรปกครองส่วนท้องถิ่นในพื้นที่ถือปฏิบัติ และประชาสัมพันธ์ให้ประชาชนทั่วไปทราบด้วย

จึงเรียนมาเพื่อทราบและดำเนินการ

ขอแสดงความนับถือ

(นายวิทยา จันทร์ฉลอง)
ผู้ว่าราชการจังหวัดสกลนคร

(ผู้ช่วยศาสตราจารย์ชาคริต ชาญชิตปรีชา)
รักษาราชการแทนรองอธิการบดีฝ่ายบริหาร

สำนักงานจังหวัดสกลนคร
กลุ่มงานยุทธศาสตร์และข้อมูลฯ
โทร./โทรสาร ๐-๔๒๗๑-๑๐๖๕

"ปวงข้าพระพุทธเจ้า ขอน้อมเกล้า น้อมกระหม่อม รำลึกในพระมหากรุณาธิคุณหาที่สุดมิได้"

(ผู้ช่วยศาสตราจารย์ปรีชา ธรรมวินทร)
รักษาราชการแทนอธิการบดีมหาวิทยาลัยราชภัฏสกลนคร

กระทรวงดีอี
เตือนภัยมัลแวร์เรียกค่าไถ่ WannaCry
กระจายผ่านช่องโหว่ของวินโดว์ รีบอัปเดตทันที

เมื่อวันที่ 12 พฤษภาคม 2560 บริษัท Avast ได้เผยแพร่รายงานการพบมัลแวร์เรียกค่าไถ่ชื่อ WannaCry ซึ่งมีจุดประสงค์เพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดที่ใช้งาน รวมถึงสามารถกระจายตัวของจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ของวินโดว์ที่เกี่ยวข้องกับบริการแชร์ไฟล์ผ่านเครือข่าย (SMB) ที่มีการเปิดให้บริการ

1 มัลแวร์ถูกดาวน์โหลดและติดตั้งลงในคอมพิวเตอร์ของผู้ใช้และแสดงการเรียกค่าไถ่

2 ค่าไถ่ที่ถูกเรียกคือ บิตคอยน์ 300 ดอลลาร์ โดยแนะนำวิธีการจ่ายค่าไถ่ อธิบายสิ่งที่เกิดขึ้นและการนับถอยหลัง

3 วอลล์เปเปอร์ของผู้ถูกเป็นเหยื่อ

ถึงแม้ทางผู้พัฒนาจะออกเวอร์ชันรุ่นอัปเดตช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แล้วแต่ก็ยังพบว่ามีผู้เสียหายในระดับองค์กรทั่วโลกที่ได้รับผลกระทบจากการโจมตีช่องโหว่ดังกล่าวและฝังมัลแวร์เรียกค่าไถ่ WannaCry เอาไว้

สำหรับประเทศไทยมีการตรวจพบข้อมูลในสื่อสังคมออนไลน์ของผู้ใช้งานท่านหนึ่งที่โพสต์ข้อมูลว่าตนเองโดนมัลแวร์ดังกล่าวเช่นกัน แต่ยังไม่ทราบว่าเป็นความเสียหายระดับใดและกระทบกับหน่วยงานใดโดยปัจจุบัน ไทยเซิร์ต ETDA กำลังประสานเพื่อให้คำแนะนำกรณีดังกล่าว

แนวทางการป้องการการติด Ransomware WannaCry

1. ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น หากจำเป็นต้องเปิดเอกสารแนบอีเมล ควรตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมลฉบับนั้นมาจริง

2. ปรับปรุงระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบัน เพื่อป้องกันการใช้ช่องโหว่ของระบบซึ่งเป็นช่องทางให้คอมพิวเตอร์ติด Ransomware

แนวทางการป้องกันการแพร่กระจาย (หากพบการติด Ransomware แล้ว)

สำหรับผู้ใช้งานทั่วไป

ให้ปิดเครื่องและแจ้งเจ้าหน้าที่ผู้ดูแลระบบ หรือเจ้าหน้าที่ไทยเซิร์ต ETDA ที่หมายเลข **02 123 1212 (24x7)**

สำหรับผู้ดูแลระบบ

ปิดบริการ SMBv1 ที่ Windows servers

ปิดการเข้าถึงพอร์ต TCP/UDP 135-139 และ TCP 445 ที่อุปกรณ์ Firewall

ThaiCERT ThaiCERT thaicert.or.th ThaiCERT ETDA