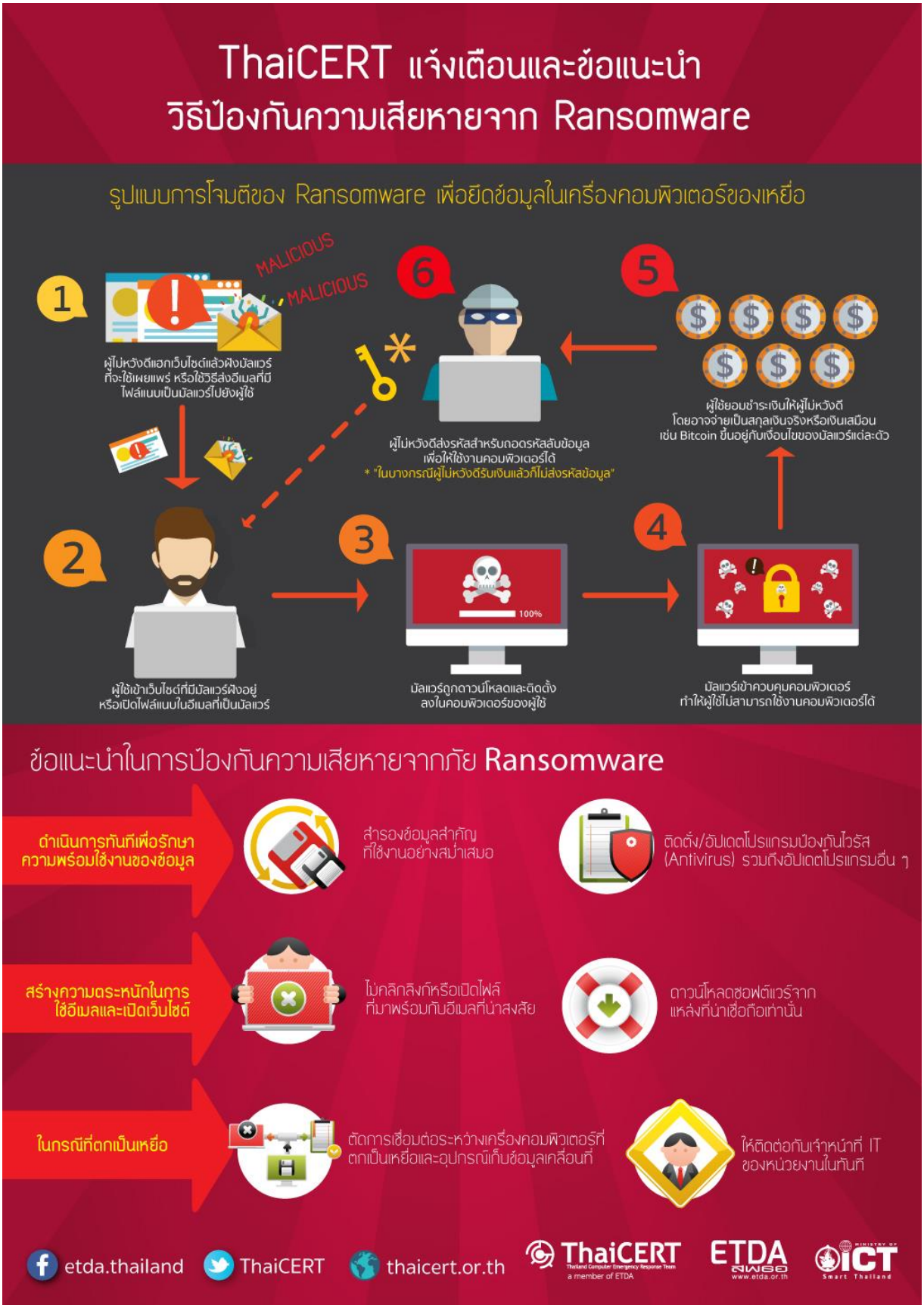

[1] https://www.etda.or.th/content/found-ransom-malware-outbreaks.html เผยแพร่ 07.05.2015 (4 ปีที่ผ่านมา) | แก้ไขล่าสุด 09.07.2019

แผนผังการแก้ไขปัญหาเมื่อเจอ Ransomware

1. พบ Ransomware หรือปัญหาที่ไม่สามารถแก้ไขได้หรือกระทบต่อองค์รวม

↓

2. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับ
ระบบเครือข่ายคอมพิวเตอร์ขององค์กรและเครือข่ายอินเทอร์เน็ตทันที

↓

3. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับอุปกรณ์เก็บข้อมูลเคลื่อนที่
(Portable Storage) หรือระบบเก็บข้อมูลบนเครือข่าย (Network Storage) ทุกประเภท

↓

4. หลังตัดการเชื่อมต่อข้างต้น ให้ติดต่อกับเจ้าหน้าที่ IT และผู้ดูแลระบบ
ของกรมสนับสนุนบริการสุขภาพ ทันที

↓

กรอกแบบฟอร์มแจ้งปัญหา F-QS16 : รายงานการสอบสวน อุบัติการณ์/เหตุการณ์ผิดปกติ
ส่งผ่าน e-Mail : isms@hss.mail.go.th หรือ Electronic Form ที่กำหนด

↓

ทีม IT กรมสนับสนุนบริการสุขภาพ ดำเนินการแก้ไขปัญหา / เสนอผลการแก้ไขปัญหา
ต่อ QMR (ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ) และ CSO (ผู้บริหารระดับสูง
ด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ) ทราบ ตามลำดับ

↓

ประชุมทบทวนแนวทางการแก้ปัญหา ดำเนินการกำหนดเป็นมาตรฐานหรือกฎระเบียบ
การปฏิบัติที่เป็นระบบ ให้ QMR ดำเนินการประกาศแจ้งต่อไป
และบันทึกในฐานข้อมูล CMDB

ต้องการคำแนะนำหรือความช่วยเหลือ สามารถแจ้งปัญหาเพื่อขอคำปรึกษาได้ที่ไทยเซิร์ต
ทาง e-Mail : report@thaicert.or.th หรือ โทรศัพท์ 0 2123 1212

ข้อแนะนำในการป้องกันมัลแวร์เรียกค่าไถ่ (RansomWare) สำหรับผู้ใช้งาน[2]

เตือนระวังเปิดอีเมล เจอมัลแวร์เรียกค่าไถ่ระบาด ภัยท้าทายความมั่นคงโลกไซเบอร์

สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) โดย ThaiCERT (ไทยเซิร์ต) เตือนภัยผู้ใช้อีเมล ระวังเปิดไฟล์แนบในอีเมล เจอแรนซัมแวร์ล็อกไฟล์ทันควัน ก่อนเรียกค่าไถ่สุดโหด เสียหายไปถึงบริษัทและองค์กรต่าง ๆ

“ไทยเซิร์ต” ออกประกาศแจ้งเตือนให้ระวังภัย รวมถึงแนะนำวิธีการป้องกันความเสียหายจากมัลแวร์หรือโปรแกรมประสงค์ร้าย ที่เรียกว่า แรนซัมแวร์ (Ransomware) หรือการเรียกค่าไถ่ข้อมูลด้วยมัลแวร์ และแนวทางแก้ไขหากตกเป็นเหยื่อมัลแวร์ตัวนี้ สืบเนื่องจากกรณีล่าสุดที่ สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กรมสอบสวนคดีพิเศษ (ดีเอสไอ) มีหนังสือแจ้งเตือนแก่เจ้าหน้าที่ภายในดีเอสไอ เรื่อง "แจ้งเตือนการเปิดอ่านจดหมายอิเล็กทรอนิกส์” ซึ่งมีมัลแวร์/ไวรัสส่งผ่านจดหมายอิเล็กทรอนิกส์ การเปิดไฟล์แนบจะทำให้ติดมัลแวร์ประเภทแรนซัมแวร์นี้ทันที

เมื่อเปิดไฟล์แนบ แรนซัมแวร์จะโจมตีด้วยวิธีการเข้ารหัสลับ (Encryption) ไฟล์เอกสารต่าง ๆ บนเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์ ซึ่งไฟล์ของเครื่องเหยื่อจะยังอยู่ แต่ไม่สามารถเปิดอ่านข้อมูลได้ จนกว่าจะจ่ายเงินเป็นสกุลเงินบิทคอยน์ (Bitcoin) เพื่อเป็นค่าใช้จ่ายในการส่งรหัสสำหรับถอดรหัสลับข้อมูล (Decryption) กลับมา หากแต่ในความเป็นจริง มีหลายกรณีที่พบว่าการจ่ายเงินค่าไถ่ไปแล้ว เหยื่อกลับไม่ได้ข้อมูลคืนมาอย่างที่อ้างไว้ ซึ่งส่งผลเสียหายทั้งในระดับบุคคล บริษัท หรือองค์กร โดยเฉพาะการสูญเสียข้อมูลสำคัญของบริษัทหรือองค์กร การตระหนักถึงอันตรายและการป้องกันแรมซัมแวร์จึงเป็นมาตรการที่มีประสิทธิภาพในการลดผลกระทบมากกว่าการแก้ไข

ทั้งนี้ไทยเซิร์ตขอแนะนำวิธีการป้องกันด้วยตัวเอง เพื่อไม่ให้ตกเป็นเหยื่อภัยคุกคามดังกล่าว คือ

1. สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ

2. อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงโปรแกรมอื่น ๆ โดยเฉพาะโปรแกรมที่มักมีปัญหาเรื่องช่องโหว่อยู่บ่อย ๆ เช่น Java และ PDF Reader

3. ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย หากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือหรือไม่เคยรู้จักมาก่อน

4. ดาวน์โหลดซอฟต์แวร์ที่น่าเชื่อถือเท่านั้น เพราะผู้ร้ายอาจฝังมัลแวร์ในซอฟต์แวร์ที่เปิดดาวน์โหลดได้ฟรี

[2] https://www.etda.or.th/content/found-ransom-malware-outbreaks.html เผยแพร่ 07.05.2015 (4 ปีที่ผ่านมา) | แก้ไขล่าสุด 09.07.2019

สำหรับกรณีที่ผู้ใช้งานอีเมลตกเป็นเหยื่อแรนซัมแวร์ ไทยเซิร์ต แนะนำให้

1. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อ กับระบบเครือข่ายคอมพิวเตอร์ขององค์กรและเครือข่ายอินเทอร์เน็ตในทันที

2. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับอุปกรณ์เก็บข้อมูลเคลื่อนที่ (Portable Storage) หรือระบบเก็บข้อมูลบนเครือข่าย (Network Storage) ทุกประเภท

3. หลังการตัดการเชื่อมต่อข้างต้น ให้ติดต่อกับเจ้าหน้าที่ IT ของหน่วยงานในทันที

ไทยเซิร์ตขอแนะนำให้ทุกคนระมัดระวังและไม่ควรเปิดอีเมลที่มีการส่งมาจากบุคคลที่ไม่รู้จัก พร้อมกับให้ลบอีเมลนั้นทิ้งไป เพราะอาจทำให้ติดแรนซัมแวร์ชนิดนี้ได้ สำหรับผู้ใช้งานที่ตกเป็นเหยื่อแรนซัมแวร์ หรือได้รับผลกระทบจากภัยคุกคามในลักษณะดังกล่าว

ต้องการคำแนะนำหรือความช่วยเหลือ สามารถแจ้งปัญหาเพื่อขอคำปรึกษาได้ที่ไทยเซิร์ต
ทาง e-Mail : report@thaicert.or.th หรือโทรศัพท์ 0 2123 1212

ข้อแนะนำในการป้องกันมัลแวร์เรียกค่าไถ่ (RansomWare) สำหรับผู้ดูแลระบบ[3]

ปัญหา Ransomware หรือมัลแวร์เรียกค่าไถ่นั้นเป็นสิ่งที่สร้างความเสียหายต่อการทำงานเป็นอย่างมาก โดยเฉพาะหากเกิดขึ้นกับระบบที่ใช้ในการทำธุรกิจ ที่ผ่านมาทางไทยเซิร์ตได้มีการเผยแพร่ข้อมูลแนวทางการป้องกันและรับมือมัลแวร์เรียกค่าไถ่สำหรับบุคคลทั่วไป เช่น การสำรองข้อมูลอยู่เป็นประจำ การอัปเดตซอฟต์แวร์และแอนติไวรัสอย่างสม่ำเสมอ รวมถึงการสังเกตลิงก์หรือไฟล์แนบอีเมลที่ผิดปกติ เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถศึกษาได้จากบทความและคลิปวิดีโอของไทยเซิร์ต
(https://www.facebook.com/thaicert/videos/657180994430037/)

ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจากบริษัท Red Canary ได้ให้คำแนะนำในการป้องกันมัลแวร์เรียกค่าไถ่ภายในองค์กร โดยเบื้องต้นควรมีการพิจารณาระดับความสำคัญและรูปแบบวิธีการปกป้องระบบของแต่ละส่วนงาน เนื่องจากลักษณะการใช้งานคอมพิวเตอร์ของแต่ละส่วนงานมีความแตกต่างกัน ไม่สามารถใช้วิธีการป้องกันหรือนโยบายเดียวให้ครอบคลุมทั้งองค์กรได้ ตัวอย่างเช่น ส่วนงานพัฒนาระบบจำเป็นต้องได้รับสิทธิในการติดตั้งและใช้งานเครื่องมือเฉพาะ ส่วนงาน HR จำเป็นต้องเปิดไฟล์แนบที่มากับอีเมล ส่วนงานการเงินจำเป็นต้องใช้ Macro ใน Microsoft Office ซึ่งหากถูกบล็อกไม่ให้ใช้งานอาจมีผลกระทบต่อการทำงานได้ คอมพิวเตอร์ของผู้บริหารก็จำเป็นต้องมีกระบวนการป้องกันในอีกรูปแบบ ผู้ดูแลระบบต้องพิจารณาว่าระบบใดควรใช้มาตรการป้องกันแบบใด หรือหากป้องกันไม่ได้เพราะจำเป็นต้องเปิดให้ใช้งาน ก็ต้องหามาตรการในการตรวจสอบความผิดปกติให้เร็วที่สุด

นักวิจัยด้านความมั่นคงปลอดภัยได้รวบรวมข้อมูลมัลแวร์เรียกค่าไถ่แต่ละสายพันธุ์ไว้ใน Google Sheet (https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#) และเปิดให้บุคคลทั่วไปสามารถเข้าถึงข้อมูลเหล่านี้ได้ ข้อมูลในเอกสารมีการอัปเดตอย่างสม่ำเสมอ ผู้ดูแลระบบควรหมั่นติดตามข้อมูลเหล่านี้เป็นระยะเพื่อให้ทราบถึงแนวโน้มและทิศทางการโจมตีจากมัลแวร์เรียกค่าไถ่สายพันธุ์ใหม่ๆ

ข้อแนะนำในการรับมือและป้องกันมัลแวร์เรียกค่าไถ่สำหรับผู้ดูแลระบบ มี 5 ข้อ ดังนี้

ใช้ Microsoft Applocker เพื่อบล็อกไม่ให้มีการรันไฟล์ที่น่าจะเป็นมัลแวร์เรียกค่าไถ่ (เช่น ไฟล์ .exe, .js, .vbs) จากไดเรกทอรีที่มีแนวโน้มว่าถูกใช้เก็บไฟล์มัลแวร์ (เช่น \user\appdata หรือ \programdata) รายละเอียดเพิ่มเติมเกี่ยวกับ Applocker ดูได้จากเว็บไซต์ของ Microsoft
(https://technet.microsoft.com/en-us/library/dd759117(v=ws.11).aspx)

ตัวอย่างสคริปต์สำหรับตั้งค่า Applocker ดูได้จากที่มา ปิดไม่ให้ใช้งาน Macro ใน Microsoft Office เนื่องจากเป็นหนึ่งในช่องทางหลักที่ถูกใช้ในการแพร่กระจายมัลแวร์ การปิด Macro ไว้เป็นค่าเริ่มต้นและเปิดให้ใช้งานได้เฉพาะในส่วนงานที่จำเป็นต้องใช้ (เช่น ฝ่ายการเงิน) ก็สามารถช่วยลดความเสี่ยงและจำกัดขอบเขตความเสียหายหากติดมัลแวร์ได้ ทั้งนี้ ควรมีการอบรมให้ความรู้กับเจ้าหน้าที่ในส่วนงานที่ต้องเปิดไฟล์แนบในอีเมลหรือต้องใช้ Macro ในการทำงาน เพื่อให้มีความตระหนักและสามารถแยกแยะอีเมลที่มีลักษณะน่าสงสัยได้

[3] ที่มา https://www.thaicert.or.th/newsbite/2017-05-08-02.html วันที่: 2017-05-08 | ที่มา: Red Canary

หากใช้ Windows Server ให้ตั้งค่า File Server Resource Manager เพื่อตรวจจับและป้องกันการแก้ไขข้อมูลจากมัลแวร์เรียกค่าไถ่ โดยเป็นการเฝ้าระวังว่ามีการสร้างไฟล์ที่มีลักษณะว่าเกิดจากการติดมัลแวร์เรียกค่าไถ่ (เช่น DECRYPT_INSTRUCTION.TXT) บนเซิร์ฟเวอร์หรือไม่ รวมถึงตรวจสอบนามสกุลไฟล์ที่ถูกสร้างโดยมัลแวร์เรียกค่าไถ่ ตัวอย่างวิธีการตั้งค่าสามารถดูได้จาก http://olivermarshall.net/using-file-screening-to-help-block-cryptolocker/

พิจารณาใช้เครื่องมือ Anti-Ransomware โดยจะเป็นการตรวจสอบการแก้ไขข้อมูลในไดเรกทอรีที่กำหนด รวมถึงตรวจสอบการแก้ไขข้อมูลไฟล์ระบบจำนวนมากซึ่งเข้าข่ายต้องสงสัยว่าเป็นพฤติกรรมของมัลแวร์เรียกค่าไถ่ ถึงแม้เครื่องมือเหล่านี้อาจไม่สามารถป้องกันมัลแวร์เรียกค่าไถ่ได้แบบ 100% เพราะผู้พัฒนามัลแวร์พยายามดัดแปลงเทคนิคหลบเลี่ยงการตรวจจับอยู่เสมอ แต่ก็อาจพิจารณาเพื่อนำมาใช้เป็นอีกหนึ่งช่องทางการตรวจสอบและป้องกันระบบได้

ให้ความรู้กับผู้ใช้ในองค์กร โดยควรจัดการอบรมหรือซักซ้อมรับมือการโจมตี (เช่น การโจมตีจากอีเมลฟิชชิ่ง) เพื่อให้ผู้ใช้ตระหนักถึงอันตรายและผลกระทบที่อาจเกิดขึ้นได้จากมัลแวร์เรียกค่าไถ่ รวมถึงควรมีการซักซ้อมการรับมือหากเกิดเหตุการณ์ขึ้นจริง เช่น การแจ้งฝ่ายไอที การนำข้อมูลสำรองกลับมาใช้งาน เพื่อให้ธุรกิจสามารถดำเนินต่อได้หากเกิดเหตุการณ์ขึ้นมาจริง

รายละเอียดอื่นๆ ทางเทคนิค สามารถอ่านเพิ่มเติมได้จากที่มา https://www.thaicert.or.th/newsbite/2017-05-08-02.html

ต้องการคำแนะนำหรือความช่วยเหลือ สามารถแจ้งปัญหาเพื่อขอคำปรึกษาได้ที่ไทยเซิร์ต
ทาง e-Mail : report@thaicert.or.th หรือโทรศัพท์ 0 2123 1212