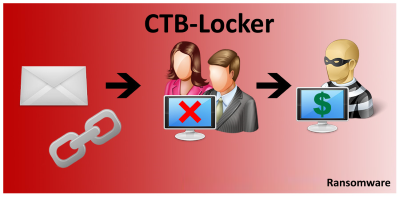
**เตือนภัยมัลแวร์ CTB Locker ระบาดหนักทั่วโลก เรียกค่าไถ่ผู้ใช้งานในการกู้ไฟล์ที่ถูกเข้ารหัสลับ**

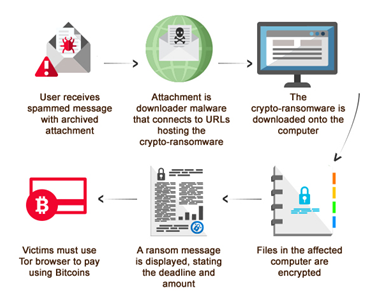
**ประเภทภัยคุกคาม:** Malicious code



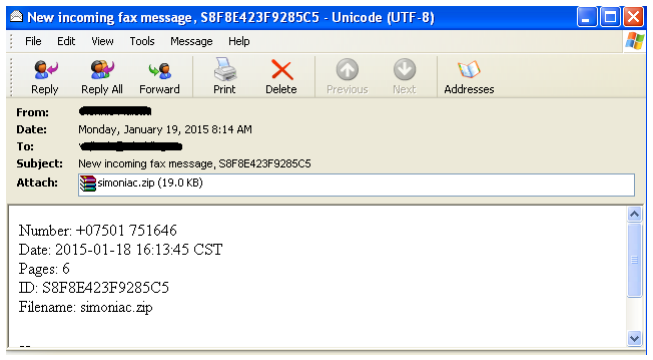
ในช่วงสัปดาห์ที่ผ่านมา ไทยเซิร์ตได้รับแจ้งเหตุภัยคุกคามเกี่ยวกับการติดมัลแวร์ CTB-Locker ในหน่วยงานสำคัญในประเทศไทยหลายแห่ง รวมถึงจากเครือข่ายความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทั่วโลกก็ได้มีการพูดถึงสถานการณ์ดังกล่าวเช่นกัน โดยจากข้อมูลทราบว่าผู้ไม่ประสงค์ดีทำการส่งอีเมลพร้อมแนบไฟล์มายังผู้ใช้งานในหน่วยงาน เมื่อผู้ใช้งานคลิกเปิดไฟล์ดังกล่าวจึงทำให้เกิดการติดมัลแวร์ทันที ชื่อเต็มของมัลแวร์ตัวดังกล่าวคือ Curve-Tor-Bitcoin Locker เป็นมัลแวร์ประเภท Ransomware มีจุดประสงค์ในการเข้ารหัสลับไฟล์เอกสารประเภทต่างๆ บนเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์ เช่น .pdf, .xls, .ppt, .txt, . py, .wb2, .jpg, .odb, .dbf, .md, .js, .pl, .doc เป็นต้น และจะพบหน้าต่างแสดงข้อมูลของการเรียกค่าไถ่กับผู้ใช้งานที่เป็นเจ้าของไฟล์ดังกล่าว ในการถอดรหัสลับไฟล์ข้อมูลทั้งหมดที่ถูกเข้ารหัสลับไว้ เจ้าของไฟล์จะต้องเสียเงินเป็นจำนวนประมาณ 630 ดอลล่าร์สหรัฐ (คิดเป็นเงินไทยประมาณ 20,000 บาท) จ่ายให้กับผู้ไม่ประสงค์ดี โดยมีข้อแม้ว่าต้องชำระด้วยสกุลเงินอิเล็กทรอนิกส์ชื่อ Bitcoin (เนื่องจากผู้ไม่ประสงค์ดีต้องการไม่ให้สามารถมีการตรวจสอบแหล่งที่มาได้โดยง่าย) จากนั้นผู้ไม่ประสงค์ดีจึงจะส่งซอฟต์แวร์และกุญแจที่ใช้ในการถอดรหัสลับไฟล์กลับมา แต่อย่างไรก็ตาม ยังไม่มีใครสามารถการันตีได้ว่าการจ่ายเงินให้จะทำให้สามารถได้ข้อมูลกลับคืนมาได้จริงอย่างที่อ้างไว้หรือไม่

โดยมัลแวร์ CTB-Locker ที่พบการแพร่ระบาดในช่วงนี้ ถือเป็นเวอร์ชันที่ 2 ของ CTB-Locker ที่มีจุดสังเกตคือมีการแปลเป็นภาษาจำนวน 4 ภาษา (ภาษาฝรั่งเศษ ภาษาอิตาลี ภาษาเยรมัน ภาษาอังกฤษ) มีการเสนอให้ผู้ใช้งานสามารถถอดรหัสลับไฟล์ได้ฟรีจำนวน 5 ไฟล์ และมีการขยายเวลาของการเรียกค่าไถ่ออกเป็น 96 วัน รวมถึงมีการเพิ่มจำนวนเงินที่ใช้ในการเรียกค่าไถ่มากขึ้นด้วย

## การติดมัลแวร์ CTB-Locker

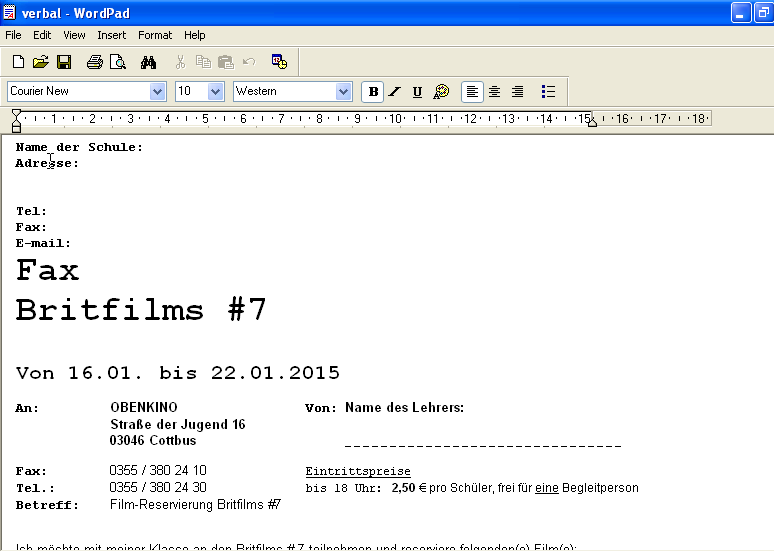


รูปที่ 1 ขั้นตอนการติดมัลแวร์ CTB-Locker

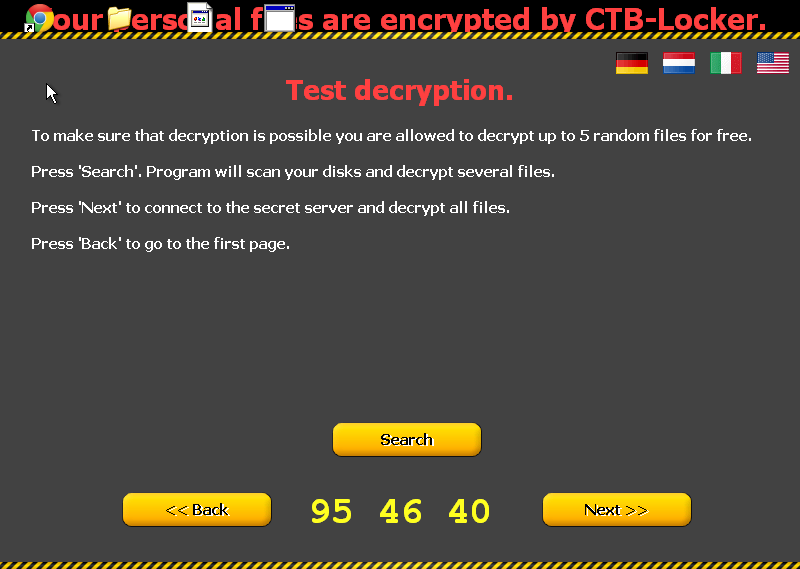


รูปที่ 2 อ้างอิงตัวอย่างของอีเมลที่ถูกใช้ส่งมัลแวร์ [[2]](https://www.thaicert.or.th/alerts/user/2015/al2015us001.html#2)

ลักษณะของการติดมัลแวร์ที่ได้รับแจ้ง สามารถอธิบายตามรูปแบบการโจมตีในรูปที่ 1 เริ่มต้นจากการที่**เหยื่อได้รับอีเมลหลอกลวงที่มีไฟล์แนบ (ไฟล์นามสกุล .zip)** หลังจากที่เหยื่อ**ดาวน์โหลดไฟล์ดังกล่าวและสั่งรันไฟล์ด้านใน (ไฟล์นามสกุล .scr)** มัลแวร์จึงเริ่มทำงาน และจะมีการแสดงเอกสารตามรูปที่ 3 ขึ้นมา ในขณะเดียวกันฟังก์ชันของ**มัลแวร์จะค้นหาไฟล์เอกสารทั้งหมดที่อยู่ในเครื่อง เพื่อทำการเข้ารหัสลับข้อมูล**ทำให้ผู้ใช้งานไม่สามารถอ่านหรือแก้ไขไฟล์เอกสารได้ โดยช่วงเวลาที่มัลแวร์เริ่มทำงานไปจนถึงทำการเข้ารหัสลับไฟล์ข้อมูลทั้งหมดที่เปิดได้จากเครื่องคอมพิวเตอร์จะอยู่ที่ประมาณ 8-10 นาที



รูปที่ 3 แสดงตัวอย่างภายหลังจากการสั่งรันไฟล์มัลแวร์ ซึ่งพบว่าคอมพิวเตอร์สั่งเปิดไฟล์เอกสารในรูปขึ้นมาทันที

หลังจากที่ไฟล์ถูกเข้ารหัสลับข้อมูลแล้วจะมีข้อความแจ้งเตือนปรากฏ เพื่อเรียกร้องให้จ่ายเงินเป็นจำนวน 3 BTC หรือประมาณ 630 ดอลล่าร์สหรัฐ ภายใน 96 ชั่วโมงแลกกับกุญแจที่ใช้ในการถอดรหัสลับข้อมูลตามรูปที่ 4 โดยมีการเสนอเรื่องการถอดรหัสลับไฟล์ข้อมูลให้ฟรีจำนวน 5 ไฟล์ เพื่อเป็นการยืนยันว่าหากมีการจ่ายเงินมายังผู้ไม่ประสงค์ดีแล้ว ไฟล์ทั้งหมดที่เข้ารหัสลับไว้จะสามารถทำการถอดรหัสลับออกมาอยู่ในรูปไฟล์ปกติได้

รูปที่ 4 ข้อความที่มัลแวร์แจ้งเตือนหลังจากที่ไฟล์ถูกเข้ารหัสลับข้อมูล

## พฤติกรรมการเชื่อมต่อทางเครือข่ายของ CTB-Locker

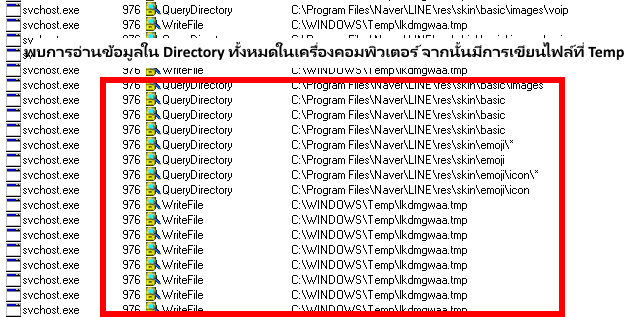
จากการวิเคราะห์การทำงานของมัลแวร์ พบว่ามัลแวร์มีลักษณะการเชื่อมต่อไปยังโดเมนปลายทางหลายแห่ง ซึ่งการบล๊อคการเชื่อมต่อกับโดเมนดังกล่าว อาจเป็นแนวทางหนึ่งในการตัดวงจรชีวิตการติดมัลแวร์ในหน่วยงานได้ โดยมีรายละเอียดดังต่อไปนี้

**[รายการโดเมนเนมต้องสงสัย]**

breteau-photographe.com  
jbmsystem.fr  
maisondessources.com  
pleiade.asso.fr  
scolapedia.org  
voigt-its.de

## ระบบที่ได้รับผลกระทบ

มัลแวร์ดังกล่าวมีวัตถุประสงค์เพื่อทำงานบนระบบปฏิบัติการ Windows โดยเฉพาะ และเมื่อคอมพิวเตอร์ถูกติดตั้งมัลแวร์ CTB Locker แล้ว มัลแวร์จะทำการเข้ารหัสลับข้อมูลทำให้ไม่สามารถอ่านหรือแก้ไขไฟล์เอกสารในเครื่องของผู้ใช้งาน โดยพบว่ามัลแวร์มีลักษณะของการพยายามอ่านเขียนไฟล์ทับในพื้นที่เดิมๆ ซ้ำๆ กัน ตามรูปที่ 5

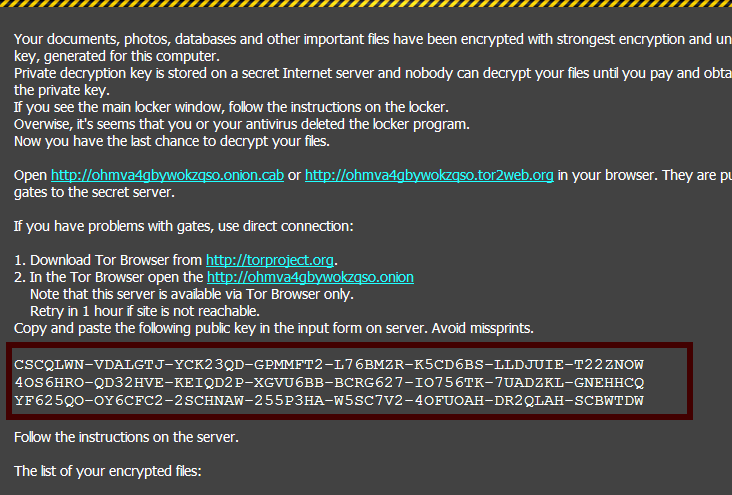


รูปที่ 5 มัลแวร์มีความพยายามในการอ่านข้อมูลจาก Directory บน Windows และมีการเขียนไฟล์ซ้ำๆ ใน Temp

## ข้อแนะนำในการแก้ไขและกู้คืนไฟล์ที่ถูกเข้ารหัสลับ

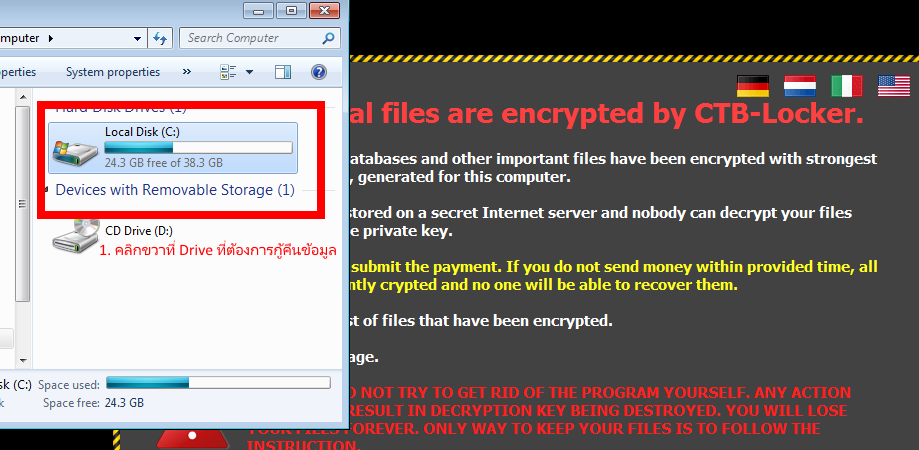
1. แยกเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ออกจากระบบ และไม่เชื่อมต่อ External Drive กับเครื่องดังกล่าว

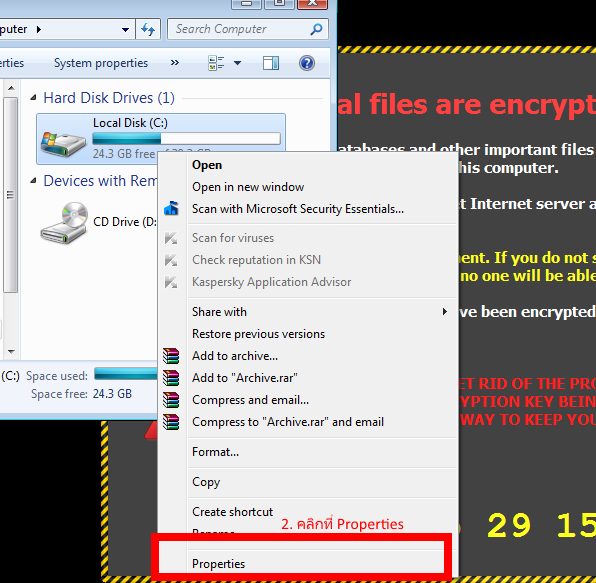
2. สำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ออกมา พร้อมกับ Public Key ที่แสดงผลไว้บนหน้าจอ ตามรูปที่ 6 ซึ่งข้อมูลดังกล่าวสามารถใช้เป็นส่วนประกอบในการถอดรหัสลับไฟล์ข้อมูลที่ได้รับผลกระทบจากมัลแวร์ CTB-Locker ในอนาคตได้ แต่การถอดรหัสลับไฟล์ข้อมูลได้จำเป็นต้องสามารถเข้าควบคุมเครื่องบริการของผู้ไม่ประสงค์ดีก่อนและจึงนำข้อมูล Private Key ที่จับคู่ตรงกับ Public Key ดังกล่าวมาถอดรหัสลับไฟล์ข้อมูลต่อไป

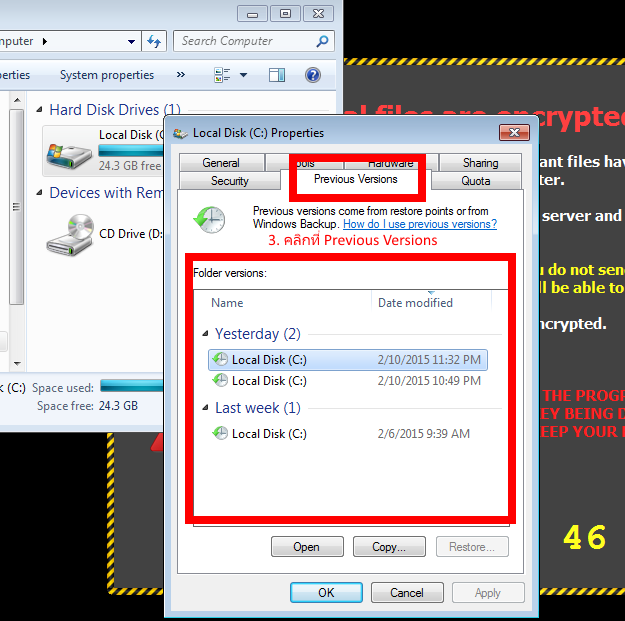


รูปที่ 6 ส่วนที่แสดงข้อมูล Public Key ที่แสดงบนหน้าจอ เมื่อมีการติดมัลแวร์ CTB-Locker

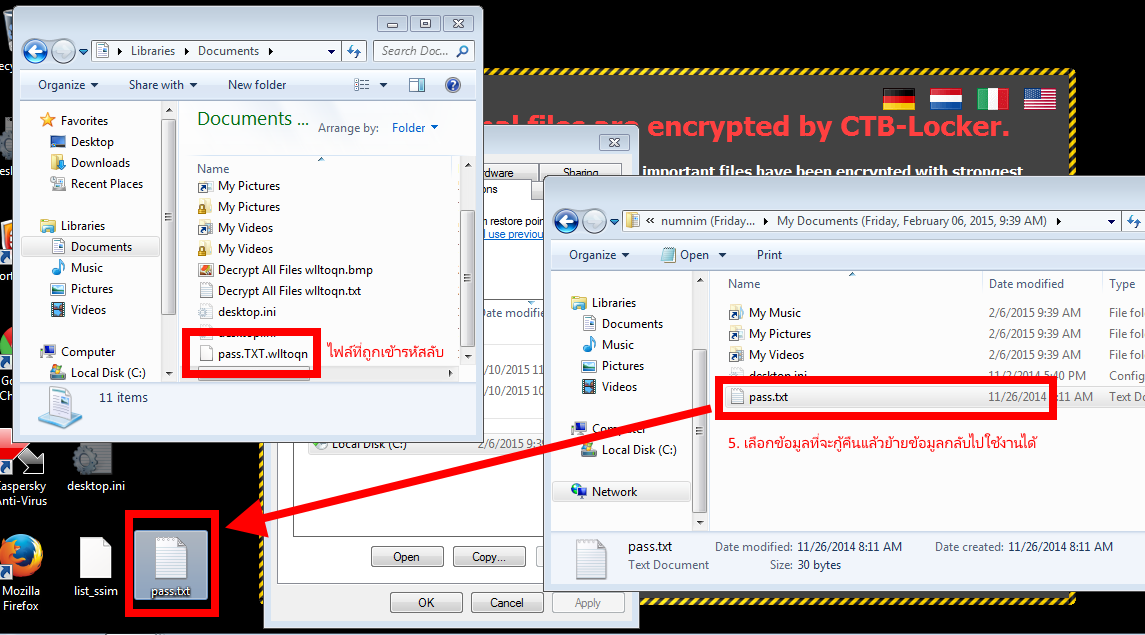
3. หากเครื่องที่ติดมัลแวร์เป็นระบบปฏิบัติการณ์วินโดส์ว 7 ขึ้นไป ผู้ใช้งานสามารถใช้งาน Shadow volumn copies volumn ในการกู้คืนไฟล์เดิมได้ ดังขั้นตอนตามรูปที่ 7-11











รูปที่ 7-11 แสดงขั้นตอนการใช้งานฟังก์ชัน Shadow volumn copies บนระบบปฏิบัติการณ์วินโดส์ว ในการกู้คืนไฟล์ที่ถูกเข้ารหัสลับของมัลแวร์ CTB-Locker

4. หากมีความต้องการใช้งานคอมพิวเตอร์นั้นอีกครั้ง ให้ทำการ Format ข้อมูลในเครื่องและติดตั้งระบบปฏิบัติการณ์ใหม่

**ข้อแนะนำในการป้องกันการติดมัลแวร์ CTB-Locker**

1. สำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ

2. ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส รวมถึงอัปเดตโปรแกรมอื่น ๆ โดยเฉพาะโปรแกรมที่มักมีปัญหาเรื่องช่องโหว่อยู่บ่อย ๆ เช่น Java และ Adobe Reader รวมถึงอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ

3. ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย หากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือหรือไม่ ให้สอบถามจากผู้ส่งโดยตรง

4. หากมีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิในการเข้าถึงข้อมูลแต่ละส่วน และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์อ่านหรือแก้ไขเฉพาะไฟล์ที่มีความจำเป็นต้องใช้สิทธิเหล่านั้น

5. ทำการบล๊อกหรือเฝ้าระวังการเชื่อมต่อจากเครือข่ายผู้ใช้งานภายในออกสู่อินเทอร์เน็ตตามโดเมนที่อยู่ในหัวข้อ **“พฤติกรรมการเชื่อมต่อทางเครือข่ายของ CTB-Locker”** ซึ่งหากสามารถบล๊อกการเชื่อมต่อกับโดเมนเหล่านี้ เท่ากับเป็นการตัดวงจรการทำงานของมัลแวร์ได้

ที่มา:อ้างอิง

1. <https://www.thaicert.or.th/alerts/user/2015/al2015us001.html>