@Post

ฉบับที่ ๖/๒๕๕๘ ประจำเดือน มิถุนายน พ.ศ. ๒๕๕๘ Free Copy

เตือนภัย Malware เรียกค่าไถ่

ปัจจุบันข้อมูลเกือบทุกอย่างถูกเก็บอยู่ในรูปแบบดิจิทัลไฟล์ เพื่อความสะดวกในการประมวลผล การค้นหา และการเข้าถึงข้อมูลที่ง่ายขึ้น ไม่ว่าจะเป็นการเก็บรูปภาพ ซึ่งสามารถเก็บไว้ดูได้นานขึ้นพร้อมกับความละเอียดที่ดีขึ้น สามารถเก็บไฟล์ข้อมูลปริมาณมาก ๆ ไว้ในอุปกรณ์ที่มีขนาดเล็กพกพาสะดวกจนกลายเป็นส่วนหนึ่งในชีวิตของผู้คนในปัจจุบันไปแล้ว ด้วยจุดนี้เองทำให้ผู้ไม่ประสงค์ดีคิดวิธีหาเงินแบบแปลก ๆ โดยการจับข้อมูลเราเป็นตัวประกันเพื่อเรียกค่าไถ่ผ่านโปรแกรมประสงค์ร้ายที่เราเรียกกันว่า “Malware” ประเภท “Ransomware” หรือ “โปรแกรมเรียกค่าไถ่” นั่นเอง

โปรแกรมเรียกค่าไถ่ หรือ Malware Ransomware แบ่งการทำงานหลัก ๆ ได้ ๒ รูปแบบ ดังนี้

๑. Lock Screen Ransomware การเรียกค่าไถ่แบบนี้ Ransomware จะทำการใช้งานฟังก์ชั่น Lock Screen ของระบบปฏิบัติการ (Operating System) ของอุปกรณ์ ทำให้ไม่สามารถเรียกใช้งานโปรแกรมประยุกต์ (Application) ของอุปกรณ์หรือเข้าถึงข้อมูลใด ๆ ได้

๒. Files-Encrypting Ransomware การเรียกค่าไถ่แบบนี้ Ransomware จะใช้วิธีเข้ารหัสไฟล์ไว้ (ล็อคไฟล์) ไม่ให้ผู้ใช้งานสามารถเข้าถึงไฟล์ของตัวเองได้ แต่ผู้ใช้สามารถใช้งานอุปกรณ์และ Application ของอุปกรณ์ได้ตามปกติ

สาเหตุที่ติด Malware Ransomware

ส่วนใหญ่มาจากการเปิดไฟล์ที่แนบมากับ e-mail ดังนั้นถ้าทำการเปิดไฟล์จะเป็นการสั่งให้ Ransomware ที่แฝงมาทำงาน โดยจะทำการเข้ารหัสหรือล็อคไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ Flash Drive หรือ External Harddisk ที่ต่อกับคอมพิวเตอร์ก็จะทำให้ไม่สามารถเปิดไฟล์ได้ จากนั้นจะส่ง e-mail มาเรียกค่าไถ่ว่า *“หากคุณอยากได้ข้อมูลสำคัญในเครื่องนี้คืนต้องจ่ายเงิน ถ้าไม่จ่ายจะเปิดไฟล์ไม่ได้”* และมีหน้าต่างแจ้งเตือนบังคับให้จ่ายเงินเพื่อปลดล็อคการเข้ารหัสไฟล์ข้อมูลผ่านทาง Bit Coin (ช่องทางการชำระเงินอิเล็กทรอนิกส์) และเมื่อมีการชำระเงินแล้วระบบจะโอนเข้าบัญชีธนาคารของเจ้าของ e-mail ที่ส่งมาให้ แต่ก็ไม่ได้รับประกันว่าจ่ายเงินค่าไถ่แล้วจะได้ข้อมูลกลับคืนมา

ข้อควรระมัดระวังในการใช้งานเพื่อป้องกันไม่ให้ติด Ransomware ได้ ดังนี้

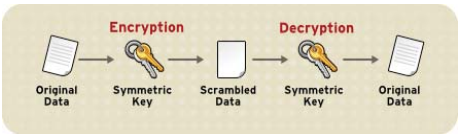
๑. ควรระมัดระวังการเปิดไฟล์ของ e-mail ที่ไม่ทราบแหล่งที่มา หากได้รับ e-mail ที่ส่งมาจากบุคคลที่ไม่รู้จักไม่ควรคลิกเปิดอ่านและควรลบจดหมายนั้นทิ้งทันที

๒. ติดตั้งโปรแกรม Antivirus และต้องอัพเดทอยู่เสมอ โดยทำการ Scan เครื่องคอมพิวเตอร์ที่ใช้งานอยู่เป็นประจำเพื่อค้นหาและกำจัด Malware ที่อาจแฝงตัวอยู่ได้

๓. อัพเดทระบบปฏิบัติการ (Operating System) อยู่เสมอ

๔. กำหนดรหัสผ่านของทุก User Account ให้ยากต่อการคาดเดา

๕. ทำการ Backup ไฟล์ที่สำคัญอย่างสม่ำเสมอ โดยการเก็บข้อมูลที่เรา Backup ในอุปกรณ์เก็บข้อมูลต่าง ๆ เช่น Flash Drive, External Harddisk หรือคอมพิวเตอร์เครื่องอื่น



นอกจากระบบรักษาความปลอดภัย Antivirus ที่มีแล้ว ผู้ใช้งานควรระมัดระวังการเปิดอ่าน e-mail ที่ไม่ทราบหรือไม่รู้จักผู้ส่ง e-mail มาให้

เพื่อความปลอดภัยและหลีกเลี่ยงความเสี่ยงที่ได้รับจากโปรแกรมไม่ประสงค์ดีต่าง ๆ ที่จะเข้ามาสร้างความยุ่งยากหรือเดือดร้อนให้แก่เรา

ที่มา : http://www.it24hrs.com/2015/ransomware-alert/

ประชาคมอาเซียน (ASEAN Community)

ERIA

ERIA (Economic Research Institute for ASEAN and East Asia) สถาบันวิจัยเศรษฐกิจเพื่ออาเซียนและเอเชียตะวันออก ทำหน้าที่ศึกษา ค้นคว้า และวิจัย เกี่ยวกับการบูรณาการทางเศรษฐกิจในอาเซียนโดยมีภารกิจในการส่งเสริมและสนับสนุนการรวมตัวทางเศรษฐกิจในภูมิภาคเอเชียตะวันออกในเรื่องการค้าการลงทุน การพัฒนาวิสาหกิจขนาดกลางและขนาดย่อม (SME) ทรัพยากรมนุษย์ โครงสร้างพื้นฐาน พลังงาน เพื่อกระตุ้นการขยายตัวทางเศรษฐกิจในภูมิภาค สนับสนุนการรวมกลุ่มทางเศรษฐกิจ เสริมสร้างความเป็นหุ้นส่วนของกลุ่มประเทศเอเชียตะวันออก และให้คำปรึกษาและข้อเสนอแนะในการดำเนินการต่าง ๆ ของประเทศสมาชิกอาเซียนเพื่อมุ่งไปสู่การรวมตัวเป็นประชาคมเศรษฐกิจอาเซียนในปี ๒๕๕๘

ที่มา : http://www.measwatch.org/news/3916