ดีเอสไอเตือนชาวเน็ต!! ระวังติดอีเมล์ไวรัสเรียกค่าไถ่

นำเสนอเมื่อ : 3 พ.ค. 2558

เมื่อวันที่ 2 พ.ค. พ.ต.ท.มนตรี บุณยโยธิน ผู้บัญชาการสำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ (สทศ.) กรมสอบสวนคดีพิเศษ (ดีเอสไอ) เปิดเผยถึงกรณีที่ สทศ.
มีหนังสือแจ้งเตือนเจ้าหน้าที่ภายในดีเอสไอเรื่องการเปิดอ่านจดหมายอิเล็กทรอนิกส์ ลงวันที่ 29 เม.ย. 2558
ซึ่งเป็นไวรัสคอมพิวเตอร์ชนิดใหม่ที่ส่งผ่านทางจดหมายอิเล็กทรอนิกส์ หรืออีเมล์ ว่า เรื่องดังกล่าวเป็นเรื่องจริง
โดยเมื่อช่วงหนึ่งเดือนที่ผ่านมา ระบบของ สทศ. สามารถกรองอีเมล์ และลบอีเมล์ไวรัสดังกล่าวได้ประมาณ 82
รายการ ซึ่งอีเมล์เหล่านี้ถูกส่งมาจากหลายเครือข่ายอินเทอร์เน็ต และส่งกลับทุก อีเมล์ เซิฟเวอร์ ในประเทศไทย
ซึ่งเมื่อวันที่ 29 เม.ย.ที่ผ่านมา ได้รับแจ้งสภาพปัญหาดังกล่าวจากผู้ให้บริการของหน่วยงานต่างๆ จำนวนมาก

พ.ต.ท.มนตรี กล่าวว่า สำหรับอีเมล์ไวรัสดังกล่าว จะมีลักษณะพฤติกรรม คือ
ส่งอีเมล์ให้กับเป้าหมายพร้อมแนบไฟล์ Attachment โดยไฟล์ที่แนบจะเป็นไฟล์นามสกุล เช่น .pdf, .xls, .ppt, .txt และ .doc เป็นต้น ซึ่งนามสกุลไฟล์ดังกล่าวเป็นแหล่งเก็บข้อมูลที่สำคัญ
โดยหัวข้อการส่งอีเมล์จะมีคำว่า account หรือ suspended หรือ locked
ซึ่งเป็นหัวข้อที่มีความเกี่ยวข้องด้านการเงิน การสั่งซื้อสินค้า หรือบัญชีธนาคาร
พร้อมระบุเนื้อหาของอีเมล์ว่าขอให้เปิดไฟล์ที่แนบ ซึ่งหากเปิดไฟล์จะทำให้ติดมัลแวร์หรือไวรัสทันที
โดยเป็นไวรัสที่มีจุดประสงค์ในการเข้ารหัสลับไฟล์เอกสารประเภทต่างๆบนเครื่องคอมพิวเตอร์
รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ที่เชื่อมต่อกับคอมพิวเตอร์ด้วย
จากนั้นเมื่อเครื่องคอมพิวเตอร์ติดไวรัสนี้แล้วจะทำให้ไม่สามารถเปิดเครื่องคอมพิวเตอร์ และค้นหาไฟล์ต่างๆได้
โดยผู้ที่ถูกติดตั้งไวรัสชนิดนี้จะเหมือนถูกเรียกค่าไถ่ โดยต้องจ่ายเงินเป็นสกุลเงินบิทคอยน์
ซึ่งเป็นสกุลเงินในระบบดิจิตอล คิดเป็นจำนวนเงินประมาณ 20,000 บาท
เพื่อเป็นค่าใช้จ่ายให้กับเจ้าของอีเมล์ที่ส่งมาให้ ทำการส่งรหัสสำหรับถอดข้อมูล

พ.ต.ท.มนตรี กล่าวต่อว่า ไวรัสทางอีเมล์ชนิดนี้ถือเป็นอาชญากรรมอีกประเภทหนึ่ง
ซึ่งหากประชาชนหลงเชื่อและเปิดไฟล์ดังกล่าวก็จะทำให้ถูกลอกโอนเงินไปให้
เพื่อแลกกับการนำข้อมูลในคอมพิวเตอร์กลับคืนมา อย่างไรก็ตาม หลังจากมีไวรัสชนิดนี้เข้ามายังดีเอสไอ
ได้มีเจ้าหน้าที่ดีเอสไอพบปัญหาดังกล่าวแล้ว 2-3 ราย แต่ไม่ได้หลงเชื่อและโอนเงินไปให้กับผู้ที่ส่งอีเมล์มา ซึ่งทาง
สทศ. ได้แก้ปัญหาด้วยการยอมเสียข้อมูลจากเครื่องคอมพิวเตอร์ดังกล่าวไป
เนื่องจากต้องทำการลบข้อมูลในเครื่องทั้งหมด ทั้งนี้
ขอให้ประชาชนทุกคนระมัดระวังและไม่ควรเปิดอีเมล์ที่มีการส่งมาจากบุคคลที่ไม่รู้จัก พร้อมกับให้ลบอีเมล์นั้นทิ้งไป
เพราะอาจทำให้ถูกไวรัสชนิดนี้ได้

ศูนย์สืบสวนสะกดรอย
เลขรับ 756
วันที่ 29 เม.ย. 2558
เวลา 11:28

ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ โทร.๙๐๑๑

ที่ ยธ.๐๘๑๗/ว ๗/๙๔ วันที่ ๒๙ เมษายน ๒๕๕๘

เรื่อง แจ้งเตือนการเปิดอ่านจดหมายอิเล็กทรอนิกส์

เรียน หัวหน้าส่วนราชการ กรมสอบสวนคดีพิเศษ

ด้วยขณะนี้ มีไวรัสคอมพิวเตอร์ชนิดใหม่ส่งผ่านทางจดหมายอิเล็กทรอนิกส์ ซึ่งช่วงหนึ่งเดือนที่ผ่านมาระบบกรอง E-mail สามารถลบ E-mail เหล่านี้ได้ประมาณ ๘๒ รายการ E-mail เหล่านี้ถูกส่งมาจากหลายแหล่งในเครือข่ายอินเทอร์เน็ต และส่งกับทุก Mail Server ในประเทศไทย ซึ่งในวันนี้(๒๙ เม.ย.๕๘) ได้รับแจ้งสภาพปัญหาจากผู้ให้บริการของหน่วยงานต่างๆ จำนวนมาก โดย E-mail ที่มีไวรัสจะมีลักษณะพฤติกรรม ดังนี้

๑. ส่ง E-mail ให้เป้าหมายพร้อมแนบไฟล์(Attachment) โดยไฟล์ที่แนบจะเป็นไฟล์นามสกุล เช่น .pdf, .xls, .ppt, .txt, . py, .wb2, .jpg, .odb, .dbf, .md, .js, .pl, .doc เป็นต้น

๒. หัวข้อการส่ง E-mail จะมีคำว่า account หรือ suspended หรือ locked หรืออื่นๆ ที่เกี่ยวข้องกับด้านการเงินหรือการสั่งซื้อสินค้าหรือบัญชีธนาคาร

๓. เนื้อหาจะขอให้เปิดไฟล์ที่แนบ ซึ่งการเปิดไฟล์ที่แนบจะทำให้ติดมัลแวร์(MALWARE)/ไวรัส ทันที ชื่อเต็มของมัลแวร์ตัวดังกล่าวคือ Curve-Tor-Bitcoin Locker เป็นมัลแวร์ประเภท Ransomware มีจุดประสงค์ในการเข้ารหัสสับไฟล์เอกสารประเภทต่างๆ บนเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์

๔. เมื่อเครื่องคอมพิวเตอร์ติดไวรัสนี้แล้วจะไม่สามารถเปิดเครื่องคอมพิวเตอร์ และค้นหาไฟล์ต่างๆ ได้ ผู้ที่ถูกติดตั้งไวรัสประเภทนี้จะเสมือนถูกเรียกค่าไถ่ โดยต้องจ่ายเงินเป็นสกุล Bitcoin เทียบเท่า 650 SUS หรือประมาณ ๒๐,๐๐๐ บาท เพื่อให้เจ้าของ E-mail ที่ส่งมาให้ เพื่อส่งรหัสสำหรับถอดข้อมูลมาให้

สทศ. จึงขอแจ้งเตือนทุกท่าน **ไม่ควรเปิด E-mail ที่มีการส่งมายัง E-mail ของหน่วยงาน หรือ Free E-mail ส่วนบุคคล(เช่น Hotmail , gmail เป็นต้น) และท่านไม่รู้จักผู้ส่งหรือรู้จักแต่ไม่ทราบเหตุผลการส่งขอให้โทรศัพท์สอบถามเจ้าของ แต่หากไม่รู้จักผู้ส่ง E-mail ให้ ขอให้ลบ E-mail นั้นทิ้ง เพื่อป้องกันปัญหาที่จะเกิดกับตัวท่าน**

จึงเรียนมาเพื่อโปรดทราบ และแจ้งข้าราชการในสังกัดทราบ

พ.ต.ท.
(มนตรี บุณยโยธิน)
ผบ.สทศ.

พ.ต.ท.
(ลฎาพร สุครพัฒน์)
ผอ.ศ.สร.
29 เม.ย. 2558

อ่านเพิ่มเติมได้ที่ ข่าวสดออนไลน์ วันที่ 02 พฤษภาคม พ.ศ. 2558