เทรนด์ ไมโคร แจ้งเตือน Ransomware ล่าสุด

Media Alert

เทรนด์ ไมโคร แจ้งเตือน Ransomware ล่าสุด

เทรนด์ แล็ป ตรวจพบมัลแวร์ในอีเมลขยะที่มีไฟล์แนบ
ที่ดูจะคล้ายเป็นใบศุลกากรไทย

Ransomware กำลังระบาดหนักมากขึ้นทั่วโลก ข้อมูลจากเทรนด์ ไมโคร ระบุว่าจากเดือนมกราคมถึงเดือนพฤษภาคมปีนี้ เทรนด์ ไมโครได้ตรวจจับ/บล็อกภัยคุกคามที่เกี่ยวกับมัลแวร์เรียกค่าไถ่มากกว่า 66 ล้านภัยคุกคามทั่วโลก ในจำนวนนี้ 64% เป็นภัยคุกคามจากมัลแวร์เรียกค่าไถ่ที่มากับอีเมล์

ล่าสุดเทรนด์ แล็ป ของเทรนด์ ไมโครตรวจพบ MIRCOP.A crypto-ransomware จากอีเมล์ขยะที่มีเอกสารแนบที่ทำให้ดูจะคล้ายเป็นแบบฟอร์มของใบศุลกากรไทยที่ใช้ในการนำเข้า-ส่งออกสินค้า (http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/)

ภาพที่ 1 แสดงข้อความข่มขู่จาก MIRCOP.A crypto-ransomware

ภาพที่ 2 แสดงตัวอย่างไฟล์แนบที่มากับ MIRCOP.A crypto-ransomware

MIRCOP.A มีพฤติกรรมที่แตกต่างจากมัลแวร์เรียกค่าไถ่อื่นๆ ที่ผู้ตกเป็นเหยื่อมักจะได้รับคำแนะนำขั้นตอนการจ่ายค่าไถ่ แต่ MIRCOP.A จะมีการกล่าวโทษผู้ตกเป็นเหยื่อว่าไปขโมยเงิน (bitcoin) มาและขู่ว่าหากไม่จ่ายค่าไถ่จะเกิดเหตุการณ์ต่างๆ โดยไม่กำหนดเวลาการจ่ายเงินและไม่บอกวิธีการจ่ายค่าไถ่ แต่ให้ bitcoin address ไว้ เหมือนจะมุ่งโจมตีเหยื่อที่คุ้นเคยกับการทำธุรกรรมผ่าน bitcoin จำนวนเงินค่าไถ่ที่พบคือ 48.48 bitcoin (หรือ 28,730.70 ดอลลาร์สหรัฐ ณ วันที่ 23 มิถุนายน 2559) เป็นค่าไถ่สูงสุดที่เคยพบมา ทั้งนี้ เทรนด์ ไมโครได้ตรวจสอบ bitcoin address ณ วันที่ 23 มิถุนายนยังไม่พบว่ามีการจ่ายเงินค่าไถ่ใดๆ

เมื่อผู้ใช้เปิดไฟล์แนบและเปิดการใช้งานแมโครจะเป็นการลิงก์เข้าไปยัง hxxp://www[.]blushy[.]nl/u/putty.exe. และจะดาวน์โหลดและรันมัลแวร์โดยอัตโนมัติ ส่วนเว็บไซต์ที่ถูกโจมตีจะถูกลิงก์ไปยัง adult shop ที่อยู่ในดัตช์ ทั้งนี้มัลแวร์เรียกค่าไถ่จะสร้างไฟล์สามไฟล์ไว้ใน C:\users\administrato\appdata\local\temp\. โดยไฟล์ c.exe ใช้ในการขโมยข้อมูล, x.exe และ y.exe จะทำการเข้าหรัสไฟล์ต่างๆ และแทนที่จะเข้ารหัสไฟล์ด้วยนามสกุล MIRCOP กลับใส่คำว่า “Lock” ไว้หน้าชื่อไฟล์นั้นๆ นอกจากนี้ยังเข้ารหัสโฟลเดอร์ด้วย เมื่อเปิดไฟล์ข้อความในไฟล์จะถูกเปลี่ยนเป็นตัวอักษรที่อ่านไม่ได้

คำแนะนำจากเทรนด์ ไมโคร

ผู้ใช้ควรระวังเมื่อได้รับอีเมล์จากแหล่งที่ไม่รู้จักและงดเว้นการดาวน์โหลดและเปิดไฟล์แนบ เทรนด์ ไมโครมีโซลูชั่นเพื่อช่วยลดความเสี่ยงจากมัลแวร์เรียกค่าไถ่ เช่น Trend Micro™ Deep Discovery™ Email Inspector และ InterScan™ Web Security เป็นโซลูชั่นสำหรับอีเมลและเว็บเกตเวย์ ช่วยป้องกันไม่ให้มัลแวร์เรียกค่าไถ่เข้าถึงเครื่องลูกข่าย ส่วนในระดับเครื่องลูกข่าย เทรนด์ ไมโครนำเสนอ Smart Protection Suites ซึ่งมีฟังก์ชั่นตรวจสอบและควบคุมพฤติกรรมการใช้งานและอุดช่องโหว่ซึ่งจะช่วยลดผลกระทบของภัยคุกคามนี้ โซลูชั่น Deep Discovery Inspector ของเทรนด์ ไมโคร ช่วยตรวจจับและบล็อกมัลแวร์เรียกค่าไถ่บนระบบเน็ตเวิร์ค นอกจากนี้ยังมี Trend Micro Deep Security™ ที่จะหยุดมัลแวร์เรียกค่าไถ่ไม่ให้เข้าถึงเซิร์ฟเวอร์ขององค์กร ไม่ว่าจะเป็นเซิร์ฟเวอร์ที่เป็นระบบมาตรฐานทั่วไป, เวอร์ชวล หรือ คลาวด์