มัลแวร์เรียกค่าไถ่ข้อมูล: 10 ปีของการคุกคาม สร้างความกลัว และขู่กรรโชก

มัลแวร์เรียกค่าไถ่ข้อมูล: 10 ปีของการคุกคาม สร้างความกลัว และขู่กรรโชก

เป็นเวลาราวหนึ่งทศวรรษมาแล้วที่เราเริ่มรู้จักมัลแวร์เรียกค่าไถ่ข้อมูล (Ransomware) ซึ่งเป็นซอฟต์แวร์อันตรายที่ยึดไฟล์ที่สำคัญที่สุดของเหยื่อไว้เป็นตัวประกันเพื่อแลกกับค่าไถ่ (Ransom ซึ่งเป็นที่มาของชื่อมัลแวร์ประเภทนี้) เราจะมาสำรวจพัฒนาการของมัลแวร์ที่เติบโตอย่างรวดเร็วและกระหายเงินมากที่สุดนี้ ด้วยการศึกษากรณีสำคัญบางกรณีที่เราได้ต่อสู้กับมันมาตลอดระยะเวลาหลายปีที่ผ่านมา

ปี 2549: จุดเริ่มต้น

แม้ว่าสื่อมวลชนได้รายงานเกี่ยวกับกรณีการโจมตีของ Ransomware มากมายตั้งแต่ช่วงกลางปี 2548 แต่รูปแบบของการเข้ารหัสข้อมูลที่ซับซ้อนมากขึ้นเริ่มปรากฏให้เห็นหนึ่งปีต่อมา นั่นคือในปี 2549 รูปแบบหนึ่งในช่วงเริ่มแรกตามที่เรารายงานและตรวจพบก็คือ TROJ_CRYPZIP.A ซึ่งจะค้นหาไฟล์ที่มีนามสกุลบางอย่างในฮาร์ดไดรฟ์ของเหยื่อ จากนั้นก็ซิปไฟล์เหล่านั้น พร้อมทั้งใส่รหัสผ่านให้กับไฟล์ซิป ก่อนที่จะลบไฟล์ต้นฉบับ หากผู้ใช้ไม่มีข้อมูลแบ็คอัพเก็บไว้ที่อื่น ก็จะเหลือเฉพาะไฟล์ที่ถูกเก็บไว้ในไฟล์ซิปดังกล่าว นอกจากนี้ TROJ_CRYPZIP.A ยังสร้างไฟล์ข้อความที่ทำหน้าที่เป็นจดหมายเรียกค่าไถ่ โดยจะแจ้งให้ผู้ใช้จ่ายค่าไถ่เป็นจำนวนเงิน 300 ดอลลาร์ เพื่อแลกกับรหัสผ่านสำหรับการเปิดไฟล์ซิป

แน่นอนว่านี่เป็นความพยายามแรกๆ ของ Ransomware ในการล่อลวงเงินจากผู้ใช้ที่ไม่รู้เรื่องรู้ราว แต่ก็ยังคงมีข้อบกพร่องอยู่ กล่าวคือ รหัสผ่านที่ใช้สำหรับเรียกค่าไถ่ที่จริงแล้วอยู่ในไฟล์ส่วนประกอบของมัลแวร์ นั่นคือไฟล์ .DLL ซึ่งเปิดดูได้ง่ายๆ โดยไม่มีการเข้ารหัสไว้แต่อย่างใด

ปี 2554: ช่วงเวลาของการทดลอง

5 ปีหลังจากนั้น เราพบว่า Ransomware ได้พัฒนาจนครอบคลุมระบบชำระเงินผ่านโทรศัพท์มือถือ โดยในช่วงปี 2554 ตรวจพบ TROJ_RANSOM.QOWA ที่แพร่ระบาดในรัสเซีย แทนที่จะยึดไฟล์เอาไว้เพื่อเรียกค่าไถ่ Ransomware ประเภทนี้ป้องกันไม่ให้ผู้ใช้เข้าถึงเดสก์ท็อป ด้วยการแสดงโฮมเพจที่เรียกร้องเงินค่าไถ่ 360 รูเบิล (ประมาณ 12 ดอลลาร์ในขณะนั้น) เหยื่อจะต้องโทรศัพท์ไปยังเลขหมายพิเศษที่กำหนดและยอมรับค่าธรรมเนียมเสียก่อนจึงจะสามารถเข้าถึงระบบได้อีกครั้ง

แม้ว่าปัญหานี้ยังไม่น่ากลัวเท่าไร แต่ในไม่ช้า Ransomware จะกลายเป็นอสูรร้ายที่เรียกร้องค่าไถ่ที่สูงลิ่ว และร้ายแรง ในครั้งนี้แม้ว่าจะเรียกร้องค่าไถ่เพียงแค่ 12 ดอลลาร์ แต่ปฏิบัติการนี้สามารถรวบรวมเงินได้อย่างน้อย 30,000 ดอลลาร์จากเหยื่อราว 2,500 รายในช่วงเวลาเพียงแค่ 5 สัปดาห์ ทั้งนี้พบว่ามัลแวร์ดังกล่าวถูกดาวน์โหลดจาก

เว็บไซต์ลามกอนาจารกว่า 137,000 ครั้ง ภายในช่วงเวลา 1 เดือนก่อนหน้านั้น โดยผู้ดาวน์โหลดส่วนใหญ่เป็นผู้ใช้ชาวรัสเซีย

ราคาที่ถูกและวิธีการชำระเงินที่ง่ายดายอาจช่วยให้แผนนี้ทำเงินได้มากขึ้น เพราะถ้าเป็นคุณเอง คุณก็อาจจะยอมจ่ายเงินเพียงแค่ 12 ดอลลาร์เพื่อให้สามารถใช้คอมพิวเตอร์ของคุณได้อีกครั้ง เงินจำนวนนี้เล็กน้อยมาก เมื่อเปรียบเทียบกับ Ransomware ตัวอื่นๆ ซึ่งนั่นก็อาจเป็นทางเลือกที่ง่ายดายเช่นกัน

ตัวเลขเหล่านี้แสดงให้เห็นถึงศักยภาพของ Ransomware ในการสร้างรายได้ อาชญากรไซเบอร์ที่ล่อลวงให้ผู้ใช้ดาวน์โหลดมัลแวร์ที่ทำให้ผู้ใช้เข้าใช้ไฟล์และคอมพิวเตอร์ของตัวเองไม่ได้นับว่ามีประสิทธิภาพอย่างมากเลยทีเดียว นอกจากนี้ยังแสดงให้เห็นถึงความสำคัญของการแพร่กระจายของมัลแวร์ที่มีประสิทธิภาพ กล่าวอย่างชัดเจนก็คือ กรณีนี้แสดงให้เห็นว่าสื่อลามกอนาจารสามารถล่อหลอกชาวรัสเซียจำนวนมากให้ดาวน์โหลดมัลแวร์

ปี 2555: ช่วงเติบโต และกลวิธีสร้างความกลัว

ปี 2555 เป็นช่วงเวลาที่ Ransomware เฟื่องฟู ไม่เพียงทั้งในแง่ของอันตราย รูปแบบการทำงาน และประสิทธิภาพโดยรวม แต่ยังรวมไปถึงการแพร่กระจายไปยังภูมิภาคใหม่ๆด้วย โดยในช่วงปีนี้ Ransomware เปลี่ยนแปลงวิธีการยึดไฟล์และคอมพิวเตอร์ไว้เป็นตัวประกัน รวมไปถึงวิธีการเรียกร้องค่าไถ่ นอกจากนี้ยังเริ่มเจาะกลุ่มเป้าหมายที่อยู่นอกรัสเซีย และในช่วงนี้เช่นกันที่ Ransomware เริ่มต้นใช้กลวิธีการสร้างความกลัวในกรณีที่เกี่ยวข้องกับ Police Ransomware ที่มีชื่อว่า REVETON โดยเป็นชุด Ransomware ที่โจมตีเหยื่อในยุโรปและสหรัฐฯ

REVETON ทำให้ผู้ใช้ยอมจ่ายเงิน ด้วยการโน้มน้าวว่าผู้ใช้ได้กระทำบางสิ่งที่ผิดกฎหมาย (เช่น ติดตั้งซอฟต์แวร์เถื่อน) ดังนั้นจะต้องจ่ายค่าปรับ หรือไม่ก็ต้องเสี่ยงต่อการถูกจับกุมหรือถูกตัดสินลงโทษจำคุก Ransomware ชนิดนี้จะตรวจสอบตำแหน่งพิกัดของระบบของเหยื่อ ซึ่งใช้สำหรับส่ง ‘จดหมายเรียกค่าไถ่’ ที่เขียนเป็นภาษาที่เหยื่อใช้ นอกจากนี้ ข้อความเรียกค่าไถ่ยังมีโลโก้ของหน่วยงานบังคับใช้กฎหมายในท้องถิ่นของเหยื่อ (เช่น ข้อความจาก FBI ในสหรัฐฯ หรือข้อความจากสำนักงานตำรวจแห่งชาติสำหรับผู้ใช้ในฝรั่งเศส) เพื่อขู่ให้เหยื่อหวาดกลัวและยอมจ่ายเงิน

ถึงแม้ว่าเหยื่อเกิดสงสัยและไม่ทำตามคำแจ้งเตือนนี้ เหยื่อก็ยังถูกบีบบังคับให้จ่ายค่าปรับอยู่ดี โดยจะต้องโอนเงินมากถึง 200 ดอลลาร์ผ่านบริการโอนเงิน เช่น Ukash เพราะ REVETON จะล็อคระบบทั้งหมด ทำให้ผู้ใช้ไม่สามารถเข้าถึงเนื้อหาหรือโปรแกรมใดๆ ได้

นอกจากนี้ REVETON ยังสามารถแพร่กระจายผ่านเว็บไซต์ที่ถูกโจมตีได้ ซึ่งนับเป็นช่องทางใหม่สำหรับ Ransomware เช่นกัน

ปี 2556: การเข้ารหัสถูกพัฒนาอย่างสมบูรณ์

ปี 2556 เป็นช่วงเวลาของการเปิดตัวรูปแบบที่อันตรายที่สุดของ Ransomware นั่นคือ Cryptolocker ซึ่งนอกจากจะล็อคระบบทั้งหมดจนไม่สามารถใช้งานได้แล้ว ยังเข้ารหัสไฟล์ในลักษณะที่ไม่สามารถกู้คืนได้ นอกเสียจากว่าผู้ใช้จะจ่ายค่าไถ่เสียก่อน

เข้ารหัส 2 วิธีในเวลาเดียวกัน โดยวิธีแรกใช้ AES (Advanced Encryption Standard ใช้คีย์ชุดเดียวในการเข้ารหัสและถอดรหัสข้อมูล) เพื่อเข้ารหัสไฟล์ในระบบที่ถูกโจมตี ถ้าหาก Cryptolocker ใช้วิธีนี้เพียงอย่างเดียว ก็จะสามารถแก้ไขปัญหาได้อย่างรวดเร็ว เพราะสิ่งที่ผู้ใช้จะต้องทำก็เพียงแค่ค้นหาคีย์นั้นๆ และคีย์ดังกล่าวก็ถูกเขียนไว้ในไฟล์ที่เข้ารหัส แม้ว่าจะต้องใช้เวลาและความพยายามอยู่บ้าง แต่ก็สามารถถอดรหัสข้อมูลได้โดยไม่จำเป็นต้องจ่ายค่าไถ่

แต่ที่จริงแล้ว Cryptolocker ไม่ได้หยุดเพียงแค่นั้น เพราะมีการใช้วิธีการเข้ารหัสอีกวิธีหนึ่ง นั่นคือ RSA เพื่อเข้ารหัสคีย์ AES ทั้งนี้ RSA เป็นวิธีการเข้ารหัสที่ใช้คีย์แยกต่างหาก 2 ชุดสำหรับการเข้ารหัสและถอดรหัส และในกรณีนี้อาชญากรไซเบอร์เก็บคีย์ถอดรหัสเอาไว้ ดังนั้นจึงไม่สามารถค้นหาหรือคาดเดาได้ โดยพื้นฐานแล้ว Cryptolocker บีบบังคับให้เหยื่อยอมจ่ายเงินค่าไถ่ หรือมิฉะนั้นก็จะต้องสูญเสียทุกสิ่ง อย่างไรก็ตาม นี่ไม่ใช่ปัญหาเล็กๆ ที่จะสามารถแก้ไขได้ด้วยการจ่ายค่าไถ่ 12 ดอลลาร์ เพราะค่าไถ่สำหรับ Cryptolocker อาจสูงถึง 300 ดอลลาร์เลยทีเดียว และเนื่องจากไม่มีหนทางที่จะถอดรหัสข้อมูลเองได้ ดังนั้นเหยื่อจึงอาจประสบปัญหาร้ายแรงอย่างมาก

นอกจากนั้น ในช่วงปี 2556 เรายังพบว่า Ransomware มีช่องทางใหม่ๆ ในการแพร่กระจาย กล่าวคือ แคมเปญสแปมทำหน้าที่แพร่กระจาย Cryptolocker โดยใช้ UPATRE และ ZBOT เพื่อแทรกซึมเข้าสู่ระบบของเหยื่อ จากนั้นเราก็พบ Ransomware ที่แพร่กระจายผ่านไดรฟ์แบบถอดออกได้ โดยใช้คำสั่งการแพร่ระบาดที่เหมือนกับที่ใช้โดยมัลแวร์ประเภทเวิร์ม (Worm) (โดยชื่อที่ตรวจพบคือ WORM_CRILOCK.A)

ปี 2557-2558: Crypto-ransomware และ Cryptocurrency

จากจุดนี้ Ransomware เริ่มจะมีพัฒนาการที่ช้าลง หลังจากที่ค้นพบ ‘รูปแบบที่ลงตัว’ และใช้รูปแบบนี้อย่างต่อเนื่อง แต่มีการปรับแต่งเพิ่มเติมเล็กๆ น้อยๆ มาโดยตลอด ช่วงต้นปี 2557 เราพบเจอ TROJ_CRYPTRBIT.H ซึ่งทำงานในลักษณะเดียวกันกับ Cryptolocker แต่มีการเปลี่ยนแปลงเล็กน้อย นั่นคือ เหยื่อจะต้องจ่ายค่าไถ่ด้วยเงินดิจิตอลหรือ “บิตคอยน์” (Bitcoins) แทนที่จะใช้วิธีการโอนเงินตามปกติ และหลังจากนั้นก็มี “การปรับปรุง” เพิ่มเติม เช่น การใช้มัลแวร์ที่ขโมยเงินจาก Bitcoin Wallet (CRIBIT) ของเหยื่อ และมัลแวร์ที่ใช้เบราว์เซอร์ Darknet เพื่อปกปิดร่องรอย (CTBLocker) โดย TorrentLocker ซึ่งเป็นหนึ่งใน Ransomware รุ่นล่าสุด จะใช้โค้ด CAPTCHA และการเปลี่ยนทิศทางไปยังเว็บไซต์ปลอม เพื่อโจมตีระบบของเหยื่อ

ช่วงเวลา 2557 ถึง 2558 ยังแสดงให้เห็นถึงพัฒนาการของมัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูล (Crypto-Ransomware) ซึ่งพุ่งเป้าโจมตีองค์กรต่างๆ โดยมีหลากหลายรูปแบบ เช่น CryptoFortress ซึ่งสามารถเข้ารหัสไฟล์ในทรัพยากรเครือข่ายที่ใช้งานร่วมกัน และ Ransomweb ซึ่งเข้ารหัสเว็บไซต์และเว็บเซิร์ฟเวอร์ Ransomware เหล่านี้ทำงานในลักษณะเดียวกัน แต่ก่อให้เกิดผลกระทบอย่างกว้างขวางมากขึ้น หาก Ransomware ล็อคคอมพิวเตอร์ภายในบ้านก็ถือว่าแย่พอแล้ว เพราะผู้ใช้จะไม่สามารถเข้าถึงไฟล์เพลงที่เก็บสะสมไว้ รวมถึงภาพถ่ายครอบครัวอันมีค่า หรือไฟล์เกมที่บันทึกเอาไว้ แต่หากมัลแวร์สามารถหยุดยั้งการดำเนินงานของบริษัทเพราะไม่มีใครสามารถเข้าใช้งานคอมพิวเตอร์ได้ คุณคิดว่าจะเกิดหายนะมากเพียงใด!!

2558-ปัจจุบัน: กรณีสำหรับอนาคตที่ปลอดจาก Ransomware

Ransomware คือมัลแวร์ประเภทหนึ่งที่อันตรายอย่างมาก หากระบบโดนจู่โจมจาก Ransomware รุ่นใหม่ๆ อย่าง เช่น Torrentlocker และ CTBLocker จะกลายเป็นฝันร้ายสำหรับผู้ใช้ที่ให้ความสำคัญกับข้อมูลที่มีอยู่ รวมไปถึงผู้ใช้ที่ไม่มีเงินมากพอสำหรับการจ่ายค่าไถ่ (เราขอแนะนำว่าคุณไม่ควรจ่ายค่าไถ่เป็นอันขาด เพราะจะเป็นการส่งเสริมให้อาชญากรรมไซเบอร์ประเภทนี้ยังคงมีอยู่ต่อไป) และตอนนี้ ยังไม่มีวิธีการแก้ไขปัญหาแบบครอบจักรวาลสำหรับกรณีการถูกจู่โจมของ Ransomware อย่างไรก็ตาม คุณสามารถตรวจสอบให้แน่ใจว่าคุณได้รับการปกป้องอย่างเหมาะสม

วิธีการเยียวยาและป้องกัน Ransomware

ผู้ใช้ที่โดนจู่โจมจาก Ransomware ควรดำเนินการดังต่อไปนี้:

- ปิดใช้งานการกู้คืนระบบ (System Restore)
- รันโปรแกรมป้องกันมัลแวร์ เพื่อสแกนและลบไฟล์ที่เกี่ยวข้องกับ Ransomware

Ransomware บางประเภทอาจต้องใช้ขั้นตอนเพิ่มเติมสำหรับการลบ เช่น การลบไฟล์ใน Windows Recovery Console โดยคุณจะต้องดำเนินการตามขั้นตอนทั้งหมดที่จำเป็น เพื่อลบไฟล์ Ransomware ที่เฉพาะเจาะจงออกจากคอมพิวเตอร์ของคุณ

เพื่อป้องกันความเสี่ยงในการถูกจู่โจมของ Ransomware ให้ปฏิบัติดังต่อไปนี้:

- แบ็คอัพไฟล์ของคุณอย่างสม่ำเสมอ
- ติดตั้งแพตช์ซอฟต์แวร์ทันทีที่มีการประกาศ เนื่องจาก Ransomware บางประเภทเล็ดลอดเข้าสู่ระบบโดยผ่านทางช่องโหว่
- ใส่บุ๊คมาร์คสำหรับเว็บไซต์ที่เชื่อถือได้ และเข้าถึงเว็บไซต์เหล่านั้นผ่านทางบุ๊คมาร์ค
- ดาวน์โหลดไฟล์แนบอีเมลจากแหล่งที่เชื่อถือได้เท่านั้น
- สแกนระบบของคุณอย่างสม่ำเสมอด้วยโปรแกรมป้องกันมัลแวร์

เกี่ยวกับเทรนด์ ไมโคร

บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกในด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะปกป้องโลกให้ปลอดภัยเพื่อรองรับการแลกเปลี่ยนข้อมูลดิจิตอล นวัตกรรมโซลูชั่นของเราให้บริการสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยในการปกป้องข้อมูลแบบแบ่งระดับชั้น (Layered content security) ในอุปกรณ์พกพา อุปกรณ์ปลายทาง เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย Trend Micro™ Smart Protection Network™ ซึ่งเป็นเครือข่ายข้อมูลเกี่ยวกับภัยคุกคามทั่วโลกบนระบบคลาวด์ พร้อมการสนับสนุนจากผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.com

##########

ติดต่อข้อมูลประชาสัมพันธ์
จารุวรรณ ฤกษ์พิชญโยธิน
บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด
+662 646 1968,

jaruwan_r@trendmicro.com

วราวอง จงรักษ์

ดุษฎี เย็นสุดใจ

บริษัท เอฟเอคิว จำกัด: +662 971 3700

Trendmicrothpr@faq.co.th