Ransomware: ภัยคุกคามที่รอโอกาส ข้อมูลเบื้องต้นเกี่ยวกับมัลแวร์เรียกค่าไถ่ อะไร อย่างไร และเพราะเหตุใด

Ransomware: ภัยคุกคามที่รอโอกาส
ข้อมูลเบื้องต้นเกี่ยวกับมัลแวร์เรียกค่าไถ่ อะไร อย่างไร และเพราะเหตุใด

โดย นายคงศักดิ์ ก่อตระกูล
ผู้จัดการอาวุโสด้านเทคนิค บริษัท เทรนด์ ไมโคร (ประเทศไทย) จำกัด

ถึงแม้ว่ามัลแวร์ Ransomware ไม่ใช่เรื่องใหม่ แต่ก็ยังมีผู้ใช้อีกจำนวนมากที่ยังคงตกเป็นเหยื่อของ Ransomware โดยไม่ตระหนักว่าอุปกรณ์ของตนเองโดนโจมตี ผู้ใช้อาจดาวน์โหลด Ransomware โดยไม่รู้ตัว ด้วยการเข้าชมเว็บไซต์อันตรายหรือเว็บไซต์ที่โดน Ransomware โจมตีอยู่แล้ว หรือมัลแวร์อื่นๆ อาจปล่อยหรือดาวน์โหลด Ransomware เข้าสู่ระบบของผู้ใช้ อย่างไรก็ดี การจ่ายค่าไถ่ไม่ได้เป็นการรับประกันว่าผู้ใช้จะเข้าถึงข้อมูลดิจิทัลของตนเองได้อีกครั้ง Ransomware เคยเป็นปัญหาระดับผู้ใช้งาน แต่ปัจจุบัน กลุ่มอาชญากรปล่อย Ransomware เข้าสู่ระบบเครือข่าย ไฟล์ที่ใช้ร่วมกัน ระบบแบ๊กอัพข้อมูล ฯลฯ ทำให้เกิดความเสี่ยงในองค์กรมากขึ้น แม้ว่าเป็นการยากมากที่จะให้มูลค่าที่แท้จริงของผลกระทบของ Ransomware ต่อองค์กรในระดับโลก แต่ข้อมูลจากเทรนด์ ไมโคร ระบุว่าในช่วงเดือนตุลาคม 2558 ถึงเดือนเมษายน 2559 (7 เดือน) เทรนด์ ไมโคร สามารถสกัดกั้น Ransomware ได้ถึง 99 ล้านภัยคุกคาม แสดงให้เห็นว่า Ransomware กำลังระบาดมากขึ้นทั่วโลก และเริ่มจะเน้นไปที่ภาคสาธารณสุขมากขึ้น

โดยล่าสุดทาง The Hollywood Presbytherian Medical Center ได้ถูกโจมตีโดย Ransomware ส่งผลต่อการบริการของโรงพยาบาล รวมถึงตัวผู้ป่วยเอง และถูกเรียกเงินถึง 40 Bitcoin หรือประมาณ 17,000 เหรียญสหรัฐฯ เพื่อถอดรหัสเพราะหากไม่จ่ายและพยายามที่จะปลดล็อคเอง Ransomware ก็จะทำลายข้อมูลไปเรื่อยๆ ทำให้เกิดความเสียหายมากขึ้น ซึ่งโดยทั่วไปแล้วแฮกเกอร์จะมีวิธีการที่แตกต่างกันตามสถานการณ์ แต่ก็มีเป้าหมายเดียวกันคือ ทำให้ผู้ใช้งานไม่สามารถเข้าถึงระบบที่ถูกแฮ็คได้ และเรียกร้องค่าไถ่

สำหรับประเทศไทย ข้อมูลบางส่วนจาก DSI ระบุว่า ตั้งแต่ปี 2558 เป็นต้นมา เริ่มจะมีมัลแวร์ระบาดผ่านระบบเครือข่ายออนไลน์เข้าสู่เครื่องคอมพิวเตอร์ส่วนตัว เพื่อเรียกค่าไถ่แลกกับโค้ดในการถอดรหัส โดยต้องพยายามอำพราง

ตัวเพื่อไม่ให้โปรแกรม Antivirus ตรวจจับได้ และเมื่อผู้ใช้เปิดไฟล์แนบที่ฝังมัลแวร์ไว้โดยการคลิ้กที่ป๊อปอัพหรือคลิกลิงค์ในอีเมล์ ก็จะถูกรีไดเร็คหน้าเว็บไซต์ไปยังเว็บไซต์ที่มีมัลแวร์อยู่ ทำให้แฮ็กเกอร์สามารถสร้างรายได้จากเหยื่อที่ไม่มีความรู้

Ransomware บางประเภทได้พัฒนาจากมัลแวร์ที่สร้างความกลัว (Scareware) ไปสู่มัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูล (Crypto-Ransomware) ซึ่งเป็น Ransomware ขั้นสูงที่ล้ำหน้ามากขึ้น ด้วยการเข้ารหัสไฟล์ที่ตกเป็นตัวประกัน ในช่วงปลายปี 2556 เราตรวจพบมัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูลที่มีชื่อว่า CryptoLocker ซึ่งเข้ารหัสไฟล์และล็อคระบบของเหยื่อ สิ่งที่ต่างจาก Ransomware รุ่นก่อนหน้าก็คือ CryptoLocker เรียกร้องเงินค่าไถ่จากผู้ใช้ เพื่อแลกกับการปลดล็อคไฟล์ที่เข้ารหัส CryptoLocker พัฒนาและเพิ่มเติมกลวิธีใหม่ๆ อย่างต่อเนื่อง เพื่อหลบเลี่ยงการตรวจจับ

ในช่วงไตรมาสที่สามของปี 2557 มัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูลครองสัดส่วนหนึ่งในสามของ Ransomware ทุกประเภทที่พบในระบบที่ติดเชื้อ มัลแวร์ประเภทนี้มีแพร่กระจายเพิ่มขึ้นอย่างต่อเนื่อง ข้อมูลที่เก็บรวบรวมได้ในช่วงไตรมาสสุดท้ายของปี 2557 แสดงให้เห็นว่า Crypto-Ransomware เพิ่มขึ้นจาก 19% เป็นกว่า 30% ในช่วง 12 เดือนที่ผ่านมา

เมื่อไม่นานมานี้ เราตรวจสอบ Ransomware ชนิดใหม่ที่มีชื่อว่า TorrentLocker ซึ่งพุ่งเป้าโจมตีองค์กรต่างๆ เกือบ 4,000 แห่ง และส่งผลกระทบต่อผู้ใช้ทั่วโลก โดยทำให้เหยื่อไม่สามารถเข้าใช้ไฟล์ของตนเองได้ นอกเสียจากว่าจะจ่ายเงินค่าไถ่จำนวนมากเสียก่อน

ชมวิดีโอเกี่ยวกับวิธีการโจมตีของ TorrentLocker ได้ที่ https://www.youtube.com/watch?v=fNyQVePEyxg

วิธีการทำงานของมัลแวร์เรียกค่าไถ่

ลักษณะการโจมตีของ Ransomware จะขึ้นอยู่กับแรงจูงใจของผู้โจมตี โดยทั่วไปแล้ว อาชญากรไซเบอร์มักจะสร้างโค้ดที่ออกแบบเป็นพิเศษเพื่อเข้าควบคุมคอมพิวเตอร์และยึดไฟล์ไว้เป็นตัวประกัน ไฟล์ดังกล่าวจะถูกเข้ารหัส และเหยื่อจะไม่สามารถเข้าถึงไฟล์ได้อีกต่อไป Ransomware นี้เมื่อเริ่มทำงานในระบบคอมพิวเตอร์ จะสามารถ (1) ล็อคหน้าจอคอมพิวเตอร์ หรือ (2) เข้ารหัสไฟล์ที่กำหนด ในกรณีแรก ระบบที่ติดเชื้อจะแสดงภาพเต็มหน้าจอหรือการแจ้งเตือนที่ระบุว่าเหยื่อจะไม่สามารถใช้ระบบดังกล่าวได้ นอกเสียจากว่าจะจ่ายค่าธรรมเนียมหรือ “ค่าไถ่” นอกจากนี้ยังแสดงคำแนะนำเกี่ยวกับวิธีการจ่ายค่าไถ่ เพื่อแลกกับการเข้าถึงระบบ ส่วน Ransomware ชนิดที่สองจะล็อคไฟล์ต่างๆ เช่น เอกสาร สเปรดชีต และไฟล์สำคัญอื่นๆ

จำนวนเงินค่าไถ่อาจแตกต่างกันไป ตั้งแต่จำนวนเล็กน้อยไปจนถึงหลายร้อยดอลลาร์ ผู้โจมตีจะยังคงสามารถแสวงหากำไรได้ ไม่ว่าจำนวนเงินค่าไถ่จะมากน้อยเพียงใดก็ตาม เพราะสิ่งสำคัญขึ้นอยู่กับจำนวนคอมพิวเตอร์ที่ติด

เชื้อ เหยื่อมักจะถูกเรียกร้องให้จ่ายเงินค่าไถ่ด้วยวิธีการทางออนไลน์ หากผู้ใช้ไม่ยอมจ่ายเงินค่าไถ่ ผู้โจมตีก็อาจสร้างมัลแวร์เพิ่มเติมเพื่อทำลายไฟล์จนกว่าจะมีการจ่ายเงินค่าไถ่

วิธีป้องกันไม่ให้ตกเป็นเหยื่อ Ransomware

Ransomware เป็นมัลแวร์ที่ซับซ้อนเป็นพิเศษ และแม้ว่าผู้เชี่ยวชาญอาจรู้วิธีการปิดใช้งานมัลแวร์ประเภทนี้ แต่ผู้ใช้ทั่วไปก็สามารถป้องกันปัญหาด้วยการปฏิบัติตามมาตรการด้านความปลอดภัย พึงระลึกไว้ว่าในบางกรณี อาจไม่สามารถทำการกู้คืนระบบโดยไม่จ่ายค่าไถ่ และนี่คือเหตุผลที่เราควรจะแบ็คอัพไฟล์ข้อมูลอย่างสม่ำเสมอเพื่อป้องกันความสูญเสีย

เคล็ดลับบางประการที่จะช่วยปกป้องคุณให้ปลอดภัยจากการโจมตี:

• แบ็คอัพไฟล์ของคุณอย่างสม่ำเสมอ กฎ 3-2-1 ใช้ได้กับกรณีนี้ กล่าวคือ แบ็คอัพข้อมูลของคุณเอาไว้ 3 ชุด และเก็บไว้บนสื่อบันทึก 2 ชุดที่แตกต่างกัน โดยสำเนา 1 ชุดจะต้องเก็บไว้ในสถานที่ตั้งที่แยกต่างหาก

• ใส่บุ๊คมาร์คสำหรับเว็บไซต์ที่คุณชื่นชอบ และเข้าถึงเว็บไซต์ดังกล่าวผ่านทางบุ๊คมาร์คเท่านั้น – ผู้โจมตีจะสามารถสอดแทรกโค้ดอันตรายไว้ใน URL และนำผู้ใช้ไปยังเว็บไซต์อันตรายเพื่อให้ดาวน์โหลดมัลแวร์เรียกค่าไถ่ การใส่บุ๊คมาร์คสำหรับเว็บไซต์ที่เชื่อถือได้ซึ่งคุณเข้าเยี่ยมชมเป็นประจำจะช่วยป้องกันไม่ให้คุณพิมพ์ป้อนแอดเดรสผิดพลาด

• ตรวจสอบแหล่งที่มาของอีเมล – แม้ว่าแนวทางนี้อาจดูยุ่งยาก แต่การเพิ่มความระมัดระวังก่อนที่จะเปิดลิงค์หรือไฟล์แนบอีเมลย่อมจะเป็นประโยชน์แก่คุณ ทางที่ดีคุณควรจะตรวจสอบกับผู้ติดต่อก่อนที่จะคลิก

• อัพเดตซอฟต์แวร์ความปลอดภัย – การใช้ซอฟต์แวร์ความปลอดภัยจะช่วยเพิ่มเติมการปกป้องอีกระดับ เพื่อป้องกันการติดเชื้อในทุกๆ จุดที่เป็นไปได้ โดยเฉพาะอย่างยิ่งจะช่วยป้องกันการเข้าถึงเว็บไซต์อันตรายที่มี Ransomware และที่สำคัญก็คือ จะทำหน้าที่ตรวจจับและลบ Ransomware ที่พบในระบบ

[ศึกษาข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th]