คม·ชัด·ลึก

ปีที่ 14 ฉบับที่ 4999 วันอาทิตย์ที่ 28 มิถุนายน พ.ศ. 2558 หน้า 4

มัลแวร์เรียกค่าไถ่ : อะไร-อย่างไรและเพราะเหตุใด

ถึงแม้ว่ามัลแวร์ Ransomware ไม่ใช่เรื่องใหม่ แต่ก็ยังมีผู้ใช้อีกจำนวนมากที่ยังคงตกเป็นเหยื่อของ Ransomware โดยไม่รู้ว่าอุปกรณ์ของตนเองโดนโจมตี ผู้ใช้อาจดาวน์โหลด Ransomware โดยไม่รู้ตัว ด้วยการเข้าชมเว็บไซต์อันตราย หรือเว็บไซต์ที่โดน Ransomware โจมตีอยู่แล้ว หรือมัลแวร์อื่นๆ อาจปล่อยหรือดาวน์โหลด Ransomware เข้าสู่ระบบของผู้ใช้ อย่างไรก็ดี การจ่ายค่าไถ่ไม่ได้เป็นการรับประกันว่าผู้ใช้จะเข้าถึงข้อมูลดิจิตอลของตนเองได้อีกครั้ง

Ransomware เริ่มเป็นที่พูดถึงในช่วงหลายปีที่ผ่านมา สามารถสร้างรายได้จากเหยื่อที่ไม่มีความรู้ ตั้งแต่ช่วงปี 2548-2549 ในประเทศรัสเซีย โดยในช่วงเริ่มแรก Ransomware ยึดไฟล์ของผู้ใช้เป็นตัวประกันเพื่อเรียกค่าไถ่ ด้วยการค้นหาไฟล์ที่มีนามสกุลบางอย่าง ซิปไฟล์ดังกล่าว และเขียนทับไฟล์ต้นฉบับ หลังจากนั้น วิธีการที่ใช้ได้พัฒนาเปลี่ยนแปลงเรื่อยมา ในช่วงปี 2554 เราเริ่มพบเห็น SMS Ransomware ที่ผู้ใช้ระบบที่ติดเชื้อจะได้รับคำสั่งให้โทรศัพท์ไปยังเลขหมาย SMS ที่คิดค่าบริการพิเศษ

Ransomware บางประเภทได้พัฒนาจากมัลแวร์ที่สร้างความกลัว (Scareware) ไปสู่มัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูล (Crypto-Ransomware) ซึ่งเป็น Ransomware ขั้นสูงที่ล้ำหน้ามากขึ้น ด้วยการเข้ารหัสไฟล์ที่ตกเป็นตัวประกัน ในช่วงปลายปี 2556 เราตรวจพบมัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูลที่มีชื่อว่า CryptoLocker ซึ่งเข้ารหัสไฟล์และล็อกระบบของเหยื่อ สิ่งที่เหมือนกับ Ransomware รุ่นก่อนหน้าก็คือ CryptoLocker เรียกร้องเงินค่าไถ่จากผู้ใช้ เพื่อแลกกับการปลดล็อกไฟล์ที่เข้ารหัส CryptoLocker พัฒนาและเพิ่มเติมกลวิธีใหม่ๆ อย่างต่อเนื่อง เพื่อหลบเลี่ยงการตรวจจับ

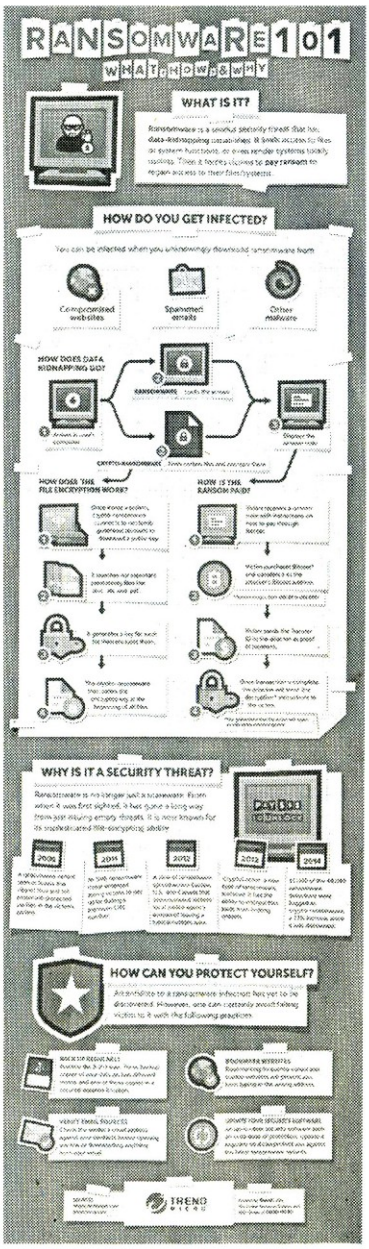
ในช่วงไตรมาสที่สามของปี 2557 มัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูลครองสัดส่วนหนึ่งในสามของ Ransomware ทุกประเภทที่พบในระบบที่ติดเชื้อ มัลแวร์ประเภทนี้มีแพร่กระจายเพิ่มขึ้นอย่างต่อเนื่อง ข้อมูลที่เก็บรวบรวมได้ในช่วงไตรมาสสุดท้ายของปี 2557 แสดงให้เห็นว่า Crypto-Ransomware เพิ่มขึ้นจาก 19% เป็นกว่า 30% ในช่วง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

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

วิธีการทำงานของมัลแวร์เรียกค่าไถ่

ลักษณะการโจมตีของ Ransomware ขึ้นอยู่กับแรงจูงใจของผู้โจมตี โดยทั่วไปแล้ว อาชญากรไซเบอร์มักจะสร้างโค้ดที่ออกแบบเป็นพิเศษเพื่อเข้าควบคุมคอมพิวเตอร์และยึดไฟล์ไว้เป็นตัวประกัน ไฟล์ดังกล่าวจะถูกเข้ารหัส และเหยื่อจะไม่สามารถเข้าถึงไฟล์ได้อีกต่อไป Ransomware นี้เมื่อเริ่มทำงานในระบบคอมพิวเตอร์ จะสามารถ (1) ล็อกหน้าจอคอมพิวเตอร์ หรือ (2) เข้ารหัสไฟล์ที่กำหนด ในกรณีแรก ระบบที่ติดเชื้อจะแสดงภาพเต็มหน้าจอหรือการแจ้งเตือนที่ระบุว่าเหยื่อจะไม่สามารถใช้ระบบดังกล่าวได้ นอกเสียจากว่าจะจ่ายค่าธรรมเนียมหรือ “ค่าไถ่” นอกจากนี้ ยังแสดงคำแนะนำเกี่ยวกับวิธีการจ่ายค่าไถ่เพื่อแลกกับการเข้าถึงระบบ

จำนวนเงินค่าไถ่อาจแตกต่างกันไป ตั้งแต่จำนวนเล็กน้อยไปจนถึงหลายร้อยดอลลาร์ ผู้โจมตีจะยังคงสามารถแสวงหากำไรได้ ไม่ว่าจำนวนเงินค่าไถ่จะมาก



(ต่อด้านหลัง)

น้อยเพียงใดก็ตาม เพราะสิ่งสำคัญขึ้นอยู่กับจำนวนคอมพิวเตอร์ที่ติดเชื้อ เหยื่อมักจะถูกเรียกร้องให้จ่ายเงินค่าไถ่ด้วยวิธีการทางออนไลน์ หากผู้ใช้ไม่ยอมจ่ายเงินค่าไถ่ ผู้โจมตีก็อาจสร้างมัลแวร์เพิ่มเติมเพื่อทำลายไฟล์จนกว่าจะมีการจ่ายเงินค่าไถ่

●● วิธีป้องกันไม่ให้ตกเป็นเหยื่อ

- แบ็กอัพไฟล์ของคุณอย่างสม่ำเสมอ กฎ 3-2-1 ใช้ได้กับกรณีนี้ กล่าวคือ แบ็กอัพข้อมูลของคุณเอาไว้ 3 ชุด และเก็บไว้บนสื่อบันทึก 2 ชุดที่แตกต่างกัน โดยสำเนา 1 ชุดจะต้องเก็บไว้ในสถานที่ตั้งที่แยกต่างหาก

- ใส่บุ๊คมาร์คสำหรับเว็บไซต์ที่คุณชื่นชอบและเข้าถึงเว็บไซต์ดังกล่าวผ่านทางบุ๊คมาร์คเท่านั้น ผู้โจมตีจะสามารถสอดแทรกโค้ดอันตรายไว้ใน URL และนำผู้ใช้ไปยังเว็บไซต์อันตรายเพื่อให้ดาวน์โหลดมัลแวร์เรียกค่าไถ่ การใส่บุ๊คมาร์คสำหรับเว็บไซต์ที่เชื่อถือได้ซึ่งคุณเข้าเยี่ยมชมเป็นประจำจะช่วยป้องกันไม่ให้คุณพิมพ์ป้อนแอดเดรสผิดพลาด

- ตรวจสอบแหล่งที่มาของอีเมล แม้ว่าแนวทางนี้อาจดูยุ่งยาก แต่การเพิ่มความระมัดระวังก่อนที่จะเปิดลิงค์หรือไฟล์แนบอีเมลย่อมจะเป็นประโยชน์แก่คุณ ทางที่ดีคุณควรจะตรวจสอบกับผู้ติดต่อก่อนที่จะคลิก

- อัพเดตซอฟต์แวร์ความปลอดภัย การใช้ซอฟต์แวร์ความปลอดภัยจะช่วยเพิ่มเติมการปกป้องอีกระดับ เพื่อป้องกันการติดเชื้อในทุกๆ จุดที่เป็นไปได้ โดยเฉพาะอย่างยิ่งจะช่วยป้องกันการเข้าถึงเว็บไซต์อันตรายที่มี Ransomware และที่สำคัญก็คือ จะทำหน้าที่ตรวจจับและลบ Ransomware ที่พบในระบบ