มัลแวร์เรียกค่าไถ่: ภัยคุกคามองค์กรที่ไม่อาจมองข้าม

RANSOMWARE: A CORPORATE THREAT THAT CANNOT BE OVERLOOKED

พนา อังกาบ[1]

เทอดพงษ์ แดงสี[2]

Pana Ungkap[1]

Therdpong Daengsi[2]

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร กรุงเทพฯ 10800[1 และ 2]

Rajamangala University of Technology Phra Nakhon, Bangkok 10800 Thailand[1 and 2]

Corresponding E-mail : therdpong.d@rmutp.ac.th

Received Date August 16, 2021
Revised Date May 22, 2022
Accepted Date May 30, 2022

บทคัดย่อ

มัลแวร์เรียกค่าไถ่เป็นภัยคุกคามทางไซเบอร์รูปแบบหนึ่งที่สามารถสร้างผลกระทบในวงกว้างหรืออาจสร้างความเสียหายให้กับองค์กรได้อย่างมหาศาล บทความนี้จึงศึกษาเกี่ยวกับมัลแวร์เรียกค่าไถ่ในมิติที่เกี่ยวข้องกับผู้ดูแลระบบ ผู้บริหาร และพนักงานในองค์กรต่าง ๆ โดยศึกษาจากเอกสารและรวบรวมข้อมูลที่เกี่ยวข้อง ครอบคลุมตั้งแต่วิวัฒนาการ หลักการทำงาน รูปแบบและกลยุทธ์ในการโจมตี รวมทั้งแนวทางในการรับมือมัลแวร์เรียกค่าไถ่ นอกจากนี้ ยังได้รวบรวมข่าวและเหตุการณ์ที่รายงานผ่านสื่ออินเทอร์เน็ตที่เกี่ยวกับมัลแวร์เรียกค่าไถ่ ทั้งที่เกิดขึ้นในประเทศและต่างประเทศ จากการศึกษาพบว่า มัลแวร์เรียกค่าไถ่เป็นการขัดขวางการเข้าถึงข้อมูลด้วยการเข้ารหัสข้อมูลหรือล็อกการใช้งานเครื่องมือหรือระบบทั้งหมด มีรูปแบบการโจมตีที่หลากหลาย โดยมีวัตถุประสงค์หลักคือต้องการเงินค่าไถ่จากองค์กรภาคเอกชนขนาดใหญ่ หน่วยงานภาครัฐ และโครงสร้างพื้นฐานระดับประเทศ ซึ่งการเรียกค่าไถ่ในระดับร้ายแรงที่สุด จะไม่สามารถเปิดไฟล์ข้อมูลได้แบบถาวรแม้จะได้รับเงินค่าไถ่แล้วก็ตาม ดังนั้น หน่วยงานทั้งภาคเอกชนและภาครัฐจะต้องสร้างการตระหนักรู้สำหรับภัยคุกคามทางไซเบอร์ในองค์กรรูปแบบนี้ด้วยกระบวนการต่าง ๆ เช่น การอบรมถ่ายทอดความรู้ส่งเสริมบุคลากรระดับต่าง ๆ โดยเฉพาะอย่างยิ่งผู้ดูแลระบบสารสนเทศและผู้ใช้งาน ให้มีความรู้ความสามารถเพิ่มขึ้นสำหรับการป้องกันและรับมือกับปัญหาที่อาจเกิดขึ้นจากการถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่

คำสำคัญ: มัลแวร์เรียกค่าไถ่ ความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์ การโจมตีทางไซเบอร์ เหยื่อ

Abstract

Ransomware became a form of cyber threats that was able to broadly impact or may enormously damage organizations. This article aims to transfer knowledge and enhance awareness associated with ransomware among related stakeholders, namely system administrators, executives, and staff within the organizations. The authors had studied and collected related information about ransomware, including its evolution, concept, form, and strategies, and also the guidelines to deal with ransomware. In addition, the news about ransomware in Thailand and overseas reported on the Internet was also assembled. From this study, it was found that ransomware obstructed the information access by logging in or locking all the tools and systems. There were various kinds of ransomware. Most cases of ransomware targeted large private corporations, government organizations and national infrastructure systems. The most serious ransomware was the case that the files were permanently lost although the ransom had been paid. Therefore, both private and public organizations needed to raise awareness of the cyber threats in their organizations through various processes, such as training, knowledge transfer, and capacity enhancing of personnel at different levels, in particular information system administrators and users, so that they were knowledgeable and capable of preventing and dealing with problems that might occur from ransomware attacks. Able of preventing and dealing with problems that may occur from ransomware attacks.

Keywords: Ransomware, Cybersecurity, Cyber threats, Cyber attacks, Victims

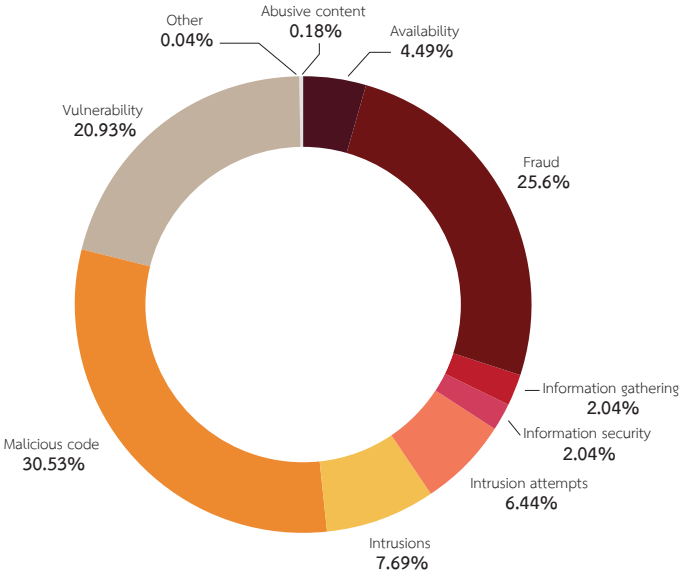
1. บทนำ

มัลแวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ (Malware) รูปแบบหนึ่งที่ถูกนำมาใช้เพื่อโจมตีข้อมูลส่วนตัวบนคอมพิวเตอร์ของผู้ใช้งานหรือองค์กรต่าง ๆ เพื่อเรียกค่าไถ่หรือขู่กรรโชกทรัพย์ทางดิจิทัล โดยใช้วิธีการเข้ารหัสข้อมูล (Encrypt) แบบเฉพาะทำให้ไม่สามารถเข้าถึงข้อมูลหรือใช้งานระบบได้ จนกว่าจะมีการจ่ายเงินค่าไถ่เพื่อกู้ข้อมูลด้วยรหัสจากผู้ที่ทำการโจมตี ระบบจึงสามารถกลับมาใช้งานได้ปกติ (“Ransomware หรือมัลแวร์เรียกค่าไถ่ฯ”, 2563) อย่างไรก็ตาม การโจมตีทางไซเบอร์ (Cyber attacks) ด้วยมัลแวร์เรียกค่าไถ่ของผู้ไม่ประสงค์ดี อาจไม่ได้จำกัดเฉพาะเรื่องความต้องการเงินค่าไถ่เท่านั้น แต่อาจโจมตีด้วยวัตถุประสงค์อื่น ๆ เช่น การก่อกวนสร้างความเดือดร้อน ความท้าทาย และวัตถุประสงค์ทางการเมือง เป็นต้น

การโจมตีของมัลแวร์เรียกค่าไถ่สามารถเป็นได้ทั้งแบบออฟไลน์และออนไลน์ ในแบบออฟไลน์อาจจะใช้วิธีโจมตีเป้าหมายโดยติดตั้งมัลแวร์เรียกค่าไถ่ผ่านอุปกรณ์เก็บข้อมูล (Storage device) แต่ส่วนใหญ่ผู้ที่โจมตีจะใช้วิธีออนไลน์โดยการส่งลิงก์ (Link) ที่แฝงมัลแวร์เรียกค่าไถ่อยู่ภายในไปยังอีเมลและข้อความแชต หรือแม้กระทั่งบนเว็บไซต์เพื่อหลอกล่อให้เป้าหมายติดตั้งลงบนเครื่องโดยไม่ทันระวังตัว เมื่อผู้ใช้งานคอมพิวเตอร์ติดมัลแวร์เรียกค่าไถ่นี้ จะไม่สามารถใช้งานระบบหรือเปิดใช้งานไฟล์ได้ และจะมีหน้าต่างแจ้งเตือนขึ้นมาเป็นการบอกวิธีการจ่ายเงินเพื่อรับรหัสปลดล็อกข้อมูล โดยผู้โจมตีมักจะใช้ช่องทางการรับเงินในรูปแบบสกุลเงินดิจิทัลบิตคอยน์ (Bitcoin: BTC) หรือสกุลเงินดิจิทัล (Cryptocurrency) ประเภทอื่น ๆ เนื่องจากทำการตรวจสอบได้ยาก

จากรายงานทางสถิติของสหรัฐอเมริกาในปี พ.ศ. 2563 (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2564ก) พบการแพร่กระจายมัลแวร์เรียกค่าไถ่เพิ่มสูงขึ้นกว่าปกติในเดือนมีนาคม ซึ่งสูงกว่าเดือนกุมภาพันธ์ถึงร้อยละ 148 ซึ่งสอดคล้องกับสถานการณ์การแพร่ระบาดของโควิด-19 ที่ทางรัฐบาลออกคำสั่งเรื่องมาตรการป้องกันการแพร่ระบาดของเชื้อไวรัส มีการส่งเสริมให้พนักงานทำงานจากที่บ้านโดยการเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของหน่วยงาน นอกจากนี้ยังพบว่าองค์กรในภาคการเงินได้ตกเป็นเป้าหมายหลักของการโจมตีจากมัลแวร์เรียกค่าไถ่มากถึงร้อยละ 52 ซึ่งเกิดความเสียหายและส่งผลกระทบต่อองค์กรเป็นอย่างมาก

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยได้จำแนกประเภทของภัยคุกคามทางไซเบอร์ (Cyber threats) ตามวัตถุประสงค์ของการโจมตี ออกเป็น 10 ประเภท และรวบรวมข้อมูลเพื่อจัดทำเป็นสถิติที่เกิดขึ้นในปี พ.ศ. 2563 (ดังแสดงในภาพที่ 1) ซึ่งพบว่า การโจมตีด้วยซอฟต์แวร์ที่เป็นอันตรายหรือซอฟต์แวร์ไม่พึงประสงค์ (Malicious software หรือ Malicious code) หรือที่นิยมเรียกกันสั้น ๆ ว่า มัลแวร์ (Malware) มีสัดส่วนสูงถึงร้อยละ 30.5 (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2564ข) ซึ่งมากที่สุดเมื่อเทียบกับภัยคุกคามรูปแบบอื่น โดยการโจมตีประเภทนี้ครอบคลุมมัลแวร์ชนิดต่าง ๆ ไม่ว่าจะเป็นไวรัส (Virus) ม้าโทรจัน (Trojan horse) หรือโทรจัน (Trojan) สปายแวร์ (Spyware) แอดแวร์ (Adware) หนอน หรือเวิร์ม (Worm) และมัลแวร์เรียกค่าไถ่ เป็นต้น (“รู้กันยัง Malicious Code ฯ”, 2558)



ภาพที่ 1 การจำแนกประเภทภัยคุกคามทางไซเบอร์ (มกราคม-ธันวาคม พ.ศ. 2563)
ที่มา: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (2564ข)

นอกจากนี้ ยังมีรายงานจากบริษัทที่เชี่ยวชาญในการป้องกันมัลแวร์เรียกค่าไถ่แห่งหนึ่งได้รายงานว่า ค่าเฉลี่ยของค่าไถ่ในไตรมาสที่ 3 ของปี พ.ศ. 2563 อยู่ที่ 178,254 ดอลลาร์สหรัฐฯ (ประมาณ 5.5 ล้านบาท) (Freedman, 2020) และในรายงานยังระบุด้วยว่า ช่องทางการโจมตีของมัลแวร์เรียกค่าไถ่ส่วนใหญ่มาจากโปรแกรมควบคุมเครื่องคอมพิวเตอร์ระยะไกล รองลงมาคือ การหลอกลวงทางอีเมลหรืออีเมลฟิชชิง (E-mail phishing) และช่องโหว่ของระบบ (Vulnerability) ตามลำดับ (Freedman, 2020) ซึ่งมีความสอดคล้องกับความจำเป็นในการทำงานที่บ้าน (Work from Home) ที่เพิ่มขึ้นที่เป็นผลมาจากการแพร่ระบาดของโควิด-19 ทำให้มีองค์กรที่เปิดการใช้งานโปรแกรมควบคุมเครื่องคอมพิวเตอร์ระยะไกลมากขึ้น และมีการคาดการณ์ว่าในปี พ.ศ. 2564 ธุรกิจทั่วโลกจะตกเป็นเหยื่อการโจมตีของมัลแวร์เรียกค่าไถ่ในทุก ๆ 11 วินาที (Freedman, 2020) และค่าใช้จ่ายในการป้องกันการโจมตีของมัลแวร์เรียกค่าไถ่สำหรับธุรกิจทั่วโลกอาจจะสูงถึงสองหมื่นล้านดอลลาร์สหรัฐฯ นอกจากนี้มีการประมาณการความเสียหายทั่วโลกที่เกี่ยวข้องกับการโจมตีทางไซเบอร์จะสูงถึง 6 ล้านล้านดอลลาร์สหรัฐฯ

จากสถิติและรายงานที่กล่าวมาข้างต้น จะเห็นได้ว่าปัญหามัลแวร์เรียกค่าไถ่เป็นภัยคุกคามรูปแบบใหม่ที่มีแนวโน้มขยายตัวขึ้นอย่างต่อเนื่อง และเป็นภัยคุกคามองค์กรที่บุคลากรทุกระดับภายในองค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชนต้องให้ความสำคัญและไม่ควรมองข้าม ดังนั้น เพื่อสร้างความตระหนักรู้เกี่ยวกับมัลแวร์เรียกค่าไถ่ จึงได้มีการศึกษาเกี่ยวกับวิวัฒนาการ หลักการทำงาน และลักษณะการโจมตี ระดับชั้นการเรียกค่าไถ่ กลไกการจ่ายเงินค่าไถ่ ตลอดจนข่าวสารเหตุการณ์ที่เคยเกิดขึ้นทั้งในประเทศไทยและต่างประเทศ และเพื่อให้บุคลากรทุกระดับในองค์กร ตลอดจนนักศึกษา นักวิชาการ และผู้สนใจทั่วไป มีความตระหนักรู้ถึงภัยที่อาจคุกคามองค์กรของตนเอง สามารถนำความรู้ที่ได้จากบทความนี้ไปประยุกต์ใช้ในการเตรียมความพร้อมรับมือกับภัยคุกคามที่อาจเกิดจากมัลแวร์เรียกค่าไถ่ที่มีแนวโน้มความเสียหายเพิ่มสูงขึ้นอย่างต่อเนื่อง

2. วิธีการศึกษา

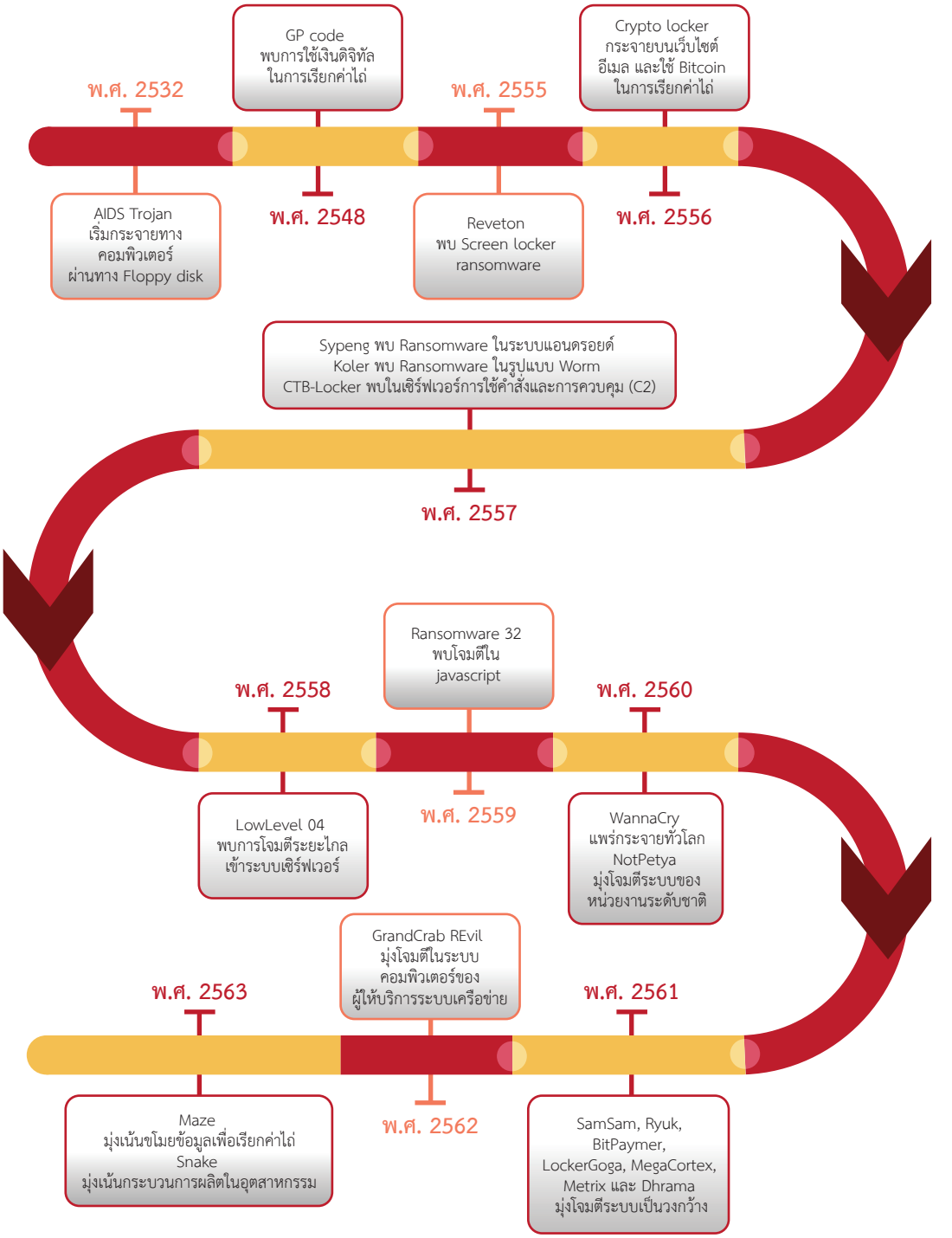
บทความนี้ศึกษาจากเอกสารที่เกี่ยวข้องและสืบค้นข้อมูลจากอินเทอร์เน็ต โดยช่องทางหลักที่ผู้วิจัยเลือกใช้คือ กูเกิลสกอลาร์ (Google scholar) ซึ่งเป็นช่องทางที่มีความสามารถในการเข้าถึงบทความวิจัยและบทความวิชาการที่อยู่ในฐานข้อมูลอื่น ๆ เช่น ฐานข้อมูล Scopus โดยใช้คำว่า “Ransomware” เป็นคำสำคัญในการค้นหา จากนั้นคัดเลือกบทความที่มีชื่อและเนื้อหาในบทคัดย่อที่สอดคล้องกับเค้าโครงบทความที่ผู้วิจัยกำหนดไว้มากที่สุดมาทำการศึกษาในรายละเอียด นอกจากนี้ ผู้เขียนยังสืบค้นข้อมูลด้วยคำสำคัญทั้งภาษาไทยและภาษาอังกฤษอื่น ๆ เพื่อรวบรวมข่าวสารเหตุการณ์ที่เกี่ยวข้องกับการโจมตีด้วยมัลแวร์เรียกค่าไถ่ที่ทันสมัยและเรียบเรียงเป็นส่วนหนึ่งของเนื้อหาในบทความนี้

3. การศึกษารายประเด็น

จากการศึกษาสามารถจำแนกประเด็นต่าง ๆ ที่เกี่ยวข้องกับมัลแวร์เรียกค่าไถ่ได้ 8 ประเด็นหลัก ดังนี้

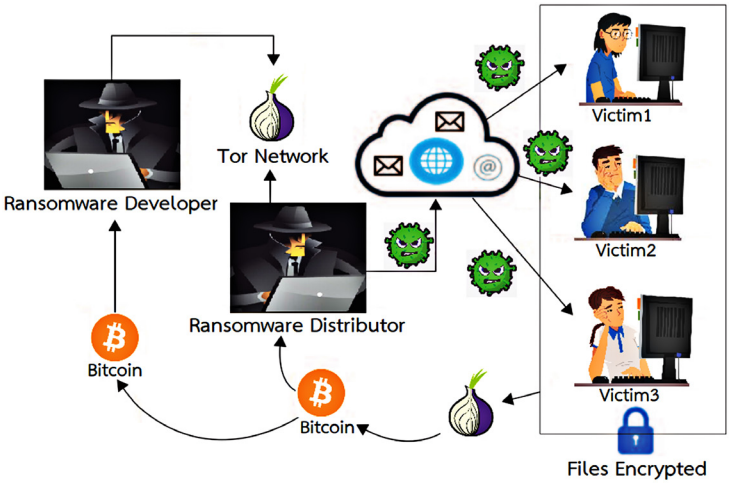
3.1 วิวัฒนาการของมัลแวร์เรียกค่าไถ่

แนวคิดเรื่องการใช้ไฟล์ข้อมูลหรือคอมพิวเตอร์ของเหยื่อเป็นตัวประกันหรือการล็อกไม่ให้ใช้งานเครื่องแล้วเรียกค่าไถ่นั้นมีมานานแล้ว (“วิวัฒนาการของ Ransomwareฯ”, 2563) โดยมีรายงานว่าเมื่อ พ.ศ. 2523 มีการขโมยเครื่องคอมพิวเตอร์ แล้วส่งจดหมายเรียกค่าไถ่ที่บ้าน หลังจากนั้นก็พัฒนากลายมาเป็นมัลแวร์เรียกค่าไถ่ โดยมัลแวร์เรียกค่าไถ่ตัวแรกที่ได้รับการจดบันทึกคือ AIDS Trojan ซึ่งแพร่กระจายผ่านแผ่นบันทึกหรือแผ่นดิสก์ (Floppy disk) เมื่อ พ.ศ. 2532 เหยื่อต้องจ่ายค่าไถ่ผ่านไปรษณีย์เพื่อกู้ไฟล์ข้อมูลและมัลแวร์เรียกค่าไถ่ดังกล่าวจึงถือเป็นต้นกำเนิดของมัลแวร์เรียกค่าไถ่ในปัจจุบัน ซึ่งวิวัฒนาการมัลแวร์เรียกค่าไถ่สามารถแสดงได้ดังภาพที่ 2 อย่างไรก็ตาม พบว่าการสร้างมัลแวร์เรียกค่าไถ่ในปัจจุบันสามารถทำได้ง่ายขึ้นดังตัวอย่างในภาพที่ 3 โดยนักพัฒนาโปรแกรมบางส่วนได้หันมาสร้างมัลแวร์เรียกค่าไถ่ในรูปแบบ Ransomware-as-a-Service (RaaS) เพื่อจำหน่ายให้กับผู้ซื้อในตลาดมืดหรือตลาดใต้ดิน โดยนักพัฒนาอาจจะได้ส่วนแบ่งเงินเรียกเก็บค่าไถ่ในแต่ละครั้ง (Sood et al., 2018)



ภาพที่ 2 วิวัฒนาการมัลแวร์เรียกค่าไถ่จนถึงปัจจุบัน

ที่มา: “Sophos 2020 Threat Report” (2019) (ดัดแปลงโดยผู้เขียน)



ภาพที่ 3 วงจรการสร้างมัลแวร์เรียกค่าไถ่ในตลาดมืด
ที่มา: Sood et al. (2018)

3.2 หลักการทำงานของมัลแวร์เรียกค่าไถ่

มัลแวร์เรียกค่าไถ่แบ่งออกเป็นสองประเภทหลัก ๆ (Savage et al., 2015) ได้แก่ ประเภทคริปโต (Crypto) ที่มุ่งเน้นการเข้ารหัสข้อมูล เช่น การเข้ารหัสข้อมูลเอกสาร หรือไฟล์ต่าง ๆ ที่มีค่าบนเครื่องผู้ใช้งาน ทำให้ผู้ใช้งานไม่สามารถเข้าถึงข้อมูลเหล่านั้นได้ ส่วนอีกประเภทเรียกว่า ประเภทล็อกเกอร์ (Locker) ซึ่งอาจโจมตีด้วยการล็อกการใช้งานทั้งระบบ ทำให้ผู้ใช้งานไม่สามารถเข้าใช้งานเครื่องคอมพิวเตอร์ที่ถูกโจมตีได้ อย่างไรก็ตาม สำหรับหลักการทำงานทั่วไปของมัลแวร์เรียกค่าไถ่ในบทความนี้จะอธิบายเพิ่มเติมเฉพาะมัลแวร์เรียกค่าไถ่ประเภทคริปโตเท่านั้น เนื่องจากเป็นประเภทเดียวกับมัลแวร์เรียกค่าไถ่ส่วนใหญ่ที่เคยแพร่ระบาด เช่น WannaCry เป็นต้น ซึ่งสามารถอธิบายได้ดังนี้

3.2.1 การแทรกซึม มัลแวร์เรียกค่าไถ่ต้องถูกติดตั้งบนคอมพิวเตอร์ของเหยื่อเพื่อเริ่มไฟล์กระบวนการเข้ารหัส นักพัฒนามัลแวร์เรียกค่าไถ่จะแทรกซึมเข้าสู่ระบบด้วยการหลอกล่อเหยื่อให้ติดตั้งมัลแวร์เรียกค่าไถ่ โดยอาศัยช่องโหว่ของระบบรักษาความมั่นคงปลอดภัย หรือผ่านโปรแกรมควบคุมเครื่องจากระยะไกล เช่น การส่งอีเมลเพื่อหลอกเหยื่อซึ่งอาจจะเป็นพนักงานฝ่ายบัญชีว่ามีการส่งใบแจ้งหนี้ส่งมาให้เพื่อให้เหยื่อเปิดไฟล์ แต่ความจริงคือไฟล์ดังกล่าวเป็นไฟล์หลอก พอเหยื่อหลงกลเปิดไฟล์ ก็จะเป็นการเรียกใช้งานโค้ดสำหรับติดตั้งมัลแวร์เรียกค่าไถ่บนเครื่องคอมพิวเตอร์ของเหยื่อ

3.2.2 การรับกุญแจเข้ารหัส เมื่อมัลแวร์เรียกค่าไถ่ได้แทรกซึมเข้าไปในระบบแล้วจะพยายามทำการรับกุญแจเข้ารหัสข้อมูล ซึ่งมักเป็นกุญแจสมมาตรเนื่องจากเข้ารหัสได้รวดเร็ว ซึ่งกระบวนการนี้จะต้องอาศัยการสื่อสารและทำงานร่วมกับมัลแวร์เรียกค่าไถ่ที่ติดตั้งบนระบบหรือเครื่องคอมพิวเตอร์ของเหยื่อ

3.2.3 การเข้ารหัสข้อมูล มัลแวร์เรียกค่าไถ่จะทำการค้นหาไฟล์เฉพาะ เช่น .docx, .xlsx, .pdf, และ .jpg เพื่อเข้ารหัสเฉพาะไฟล์ แต่ยอมให้เครื่องคอมพิวเตอร์ยังคงใช้งานได้ และทำการเข้ารหัสข้อมูลทีละไฟล์โดยใช้กุญแจสมมาตร หลังจากเข้ารหัสเสร็จสมบูรณ์ กุญแจสมมาตรบนเครื่องคอมพิวเตอร์จะถูกทำลายทันทีเพื่อป้องกันการกู้คืนกุญแจ

3.2.4 การข่มขู่เรียกค่าไถ่และวิธีการจ่ายเงินค่าไถ่ มีการแจ้งเกี่ยวกับเงินค่าไถ่ให้แก่เหยื่อและอธิบายสิ่งที่เกิดขึ้น ตลอดจนวิธีการกู้คืนไฟล์ซึ่งการจ่ายเงินค่าไถ่โดยปกติจะใช้สกุลเงินดิจิทัล และชำระผ่านระบบความปลอดภัยที่ไม่ระบุตัวตน (The onion router: Tor) แต่หลังจากจ่ายเงินค่าไถ่แล้วก็ไม่สามารถรับประกันได้ว่าจะได้รับกุญแจถอดรหัสข้อมูล หรือแม้แต่เมื่อได้รับกุญแจดังกล่าวแล้ว ก็ไม่รับประกันว่าจะสามารถกู้คืนไฟล์ทั้งหมดได้

3.3 ลักษณะการโจมตีของมัลแวร์เรียกค่าไถ่

กลยุทธ์หรือเทคนิคที่ผู้โจมตีใช้ในการโจมตีเหยื่อหรือแพร่กระจายมัลแวร์เรียกค่าไถ่ไปยังเหยื่อมีหลายรูปแบบ ได้แก่ (Challita, 2018; Gallegos-Segovia et al., 2017; Sood et al., 2018)

3.3.1 การโจมตีด้วยการดาวน์โหลด มี 3 แบบ ประกอบด้วย 1) การโจมตีในลักษณะซ่อนตัว ซึ่งหมายถึงการที่เบราว์เซอร์แสดงผลหน้าเว็บไซต์โดยไม่ได้รับอนุญาต แล้วโค้ด (Code) จะถูกเรียกใช้งาน และดาวน์โหลดมัลแวร์เรียกค่าไถ่ทันที 2) การโจมตีโดยตรงซึ่งเป็นการดาวน์โหลดมัลแวร์เรียกค่าไถ่โดยตรงจากโดเมน (Domain) ที่เป็นอันตราย และ 3) การโจมตีทางอ้อมซึ่งหมายถึงการดาวน์โหลดมัลแวร์เรียกค่าไถ่โดยอาศัยช่องโหว่ของระบบในการโจมตี

3.3.2 การโจมตีด้วยอีเมลฟิชชิง เป็นการโจมตีที่แพร่หลายเพื่อหลอกล่อให้ผู้ใช้งานเปิดสิ่งที่แนบมาหรือดึงดูดเพื่อคลิกเว็บไซต์ที่ฝังมัลแวร์เรียกค่าไถ่ ในทั้งสองกรณีไฟล์แนบที่ดาวน์โหลดมาสามารถเปิดใช้งานโค้ดที่เป็นอันตรายเพื่อดาวน์โหลดไฟล์มัลแวร์เรียกค่าไถ่โดยอาศัยช่องโหว่ของระบบ หรือใช้ฟังก์ชันบางอย่างของระบบปฏิบัติการในทางที่ผิด อย่างไรก็ตาม การโจมตีด้วยอีเมลฟิชชิงส่วนใหญ่มักจะอาศัยการโจมตีด้วยการดาวน์โหลดร่วมด้วย

3.3.3 การโจมตีผ่านโฆษณามัลแวร์ มักใช้โฆษณาและข้อเสนอเลียนแบบโฆษณาของจริงเพื่อแพร่กระจายมัลแวร์ โดยมุ่งเป้าไปที่การดาวน์โหลดมัลแวร์เรียกค่าไถ่ผ่านทางหน้าเว็บไซต์ปกติ แต่มีการส่งต่อไปเว็บไซต์ที่แฝงมัลแวร์เรียกค่าไถ่

3.3.4 การโจมตีผ่านโพรโทคอลอาร์ดีพี (Remote Desktop Protocol: RDP) เป็นวิธีที่ได้รับความนิยมมากขึ้น เนื่องจากปัจจุบันนี้มีการทำกิจกรรมต่าง ๆ ผ่านระบบออนไลน์กันอย่างแพร่หลาย จึงมีการเปิดใช้งานโพรโทคอลอาร์ดีพี เพื่อให้ผู้ดูแลระบบสามารถเข้าถึงเครื่องของผู้ใช้จากระยะไกลผ่านพอร์ต (Port) เช่น พอร์ต 3389 เพื่อกำหนดค่าหรือช่วยในการแก้ไขปัญหา ผู้ไม่ประสงค์ดีจึงหาวิธีการในการติดตั้งมัลแวร์เรียกค่าไถ่ผ่านช่องทางนี้

3.3.5 การโจมตีด้วยวิศวกรรมสังคม (Social engineering) เป็นทั้งศาสตร์และศิลป์ในการหลอกล่อหรือโน้มน้าวจิตใจของเหยื่อที่มีมานานแล้ว โดยอาศัยจุดอ่อนของเหยื่อ เช่น ความประมาทและความรู้เท่าไม่ถึงการณ์ ปัจจุบันการโจมตีนี้มักแฝงหรือถูกใช้ร่วมกับการโจมตีอื่น เช่น การฟิชชิง (Phishing) การโจมตีด้วยวิศวกรรมสังคม อาจกระทำโดยอาศัยเทคนิคง่าย ๆ เช่น การปลอมเป็นเจ้าหน้าที่แล้วแอบติดตั้งมัลแวร์เรียกค่าไถ่บนเครื่องหรือระบบของเหยื่อผ่านแฟลชไดรฟ์ (Flash drive)

3.3.6 การโจมตีผ่านเครือข่ายสังคมออนไลน์ (Social network) การโจมตีรูปแบบนี้จะมีการแบ่งปันข้อความที่มียูอาร์แอล (Universal Resource Locators: URL) หรือลิงก์ที่เป็นอันตรายระหว่างผู้ใช้ที่อยู่ในกลุ่มเครือข่ายสังคมออนไลน์เดียวกัน หากผู้ใช้ที่ได้รับข้อความคลิกลิงก์ดังกล่าว จะเกิดการดาวน์โหลดมัลแวร์เรียกค่าไถ่ลงในเครื่องทันที

3.3.7 การโจมตีผ่านแอปพลิเคชันที่เก็บข้อมูลบนคลาวด์ (Cloud) ผู้โจมตีใช้แอปพลิเคชันที่เก็บข้อมูลบนคลาวด์ในการโจมตี และแบ่งปันลิงก์ต่อสาธารณะผ่านอีเมลฟิชชิง เพื่อหลอกให้กดลิงก์สำหรับดาวน์โหลดไฟล์มัลแวร์เรียกค่าไถ่

3.3.8 การโจมตีผ่านช่องโหว่ของระบบ มัลแวร์เรียกค่าไถ่ถูกพัฒนาให้มีประสิทธิภาพมากขึ้น โดยกำหนดเป้าหมายการเรียกใช้โค้ดที่สามารถโจมตีช่องโหว่ของระบบปฏิบัติการได้ เช่น EternalBlue เป็นช่องโหว่ของระบบปฏิบัติการวินโดวส์ (Microsoft Windows) ที่มัลแวร์เรียกค่าไถ่ WannaCry และ Petya 14 ใช้ในการแพร่กระจาย

3.3.9 การโจมตีด้วยการสุ่มรหัสผ่าน เป็นการโจมตีโดยการสุ่มรหัสผ่านที่ผู้ใช้ไม่ได้ตั้งไว้ให้รัดกุมเพื่อเข้าสู่ระบบ ซึ่งสามารถโจมตีได้จากการควบคุมระยะไกล เมื่อผู้โจมตีเข้าระบบได้แล้วก็สามารถเปิดใช้งานโค้ดที่เป็นอันตรายเพื่อดาวน์โหลดไฟล์มัลแวร์เพื่อทำการโจมตีได้

3.4 ระดับชั้นของการเรียกค่าไถ่

สำหรับระดับชั้นของการเรียกค่าไถ่ สามารถแบ่งตามลักษณะของการถอดรหัสและการจัดการข้อมูลของเหยื่อหรือผู้เสียหาย โดยจัดเป็น 3 ระดับ ดังนี้ (Sood et al., 2018)

3.4.1 การเรียกค่าไถ่ระดับที่ 1 เป็นการเข้ารหัสข้อมูลเท่านั้น และจะมีการปลดล็อกหรือถอดรหัสให้หากมีการจ่ายเงินค่าไถ่ตามต้องการ โดยไม่มีการควบคุมไฟล์ข้อมูลเหล่านั้นอีกแต่อย่างใด

3.4.2 การเรียกค่าไถ่ระดับที่ 2 นอกจากจะเข้ารหัสข้อมูลแล้ว ยังขโมยข้อมูลอีกด้วย เมื่อได้ค่าไถ่แล้วมีการถอดรหัสให้ แต่ยังสำเนาข้อมูลเก็บไว้เพื่อควบคุมหรือเรียกร้องบางอย่างในภายหลัง

3.4.3 การเรียกค่าไถ่ระดับที่ 3 ผู้โจมตีจะไม่ทำการถอดรหัสข้อมูลให้ แม้ว่าจะได้รับเงินค่าไถ่จากเหยื่อแล้วก็ตาม นั่นหมายความว่าข้อมูลของเหยื่อที่ถูกเรียกค่าไถ่ จะไม่สามารถเปิดไฟล์ข้อมูลได้แบบถาวร

3.5 กลไกการจ่ายเงินค่าไถ่

กลไกการจ่ายเงินค่าไถ่ ประกอบด้วย 3 ขั้นตอน ดังนี้ (โจ ไทดี, 2564; Sood et al., 2018)

3.5.1 แจ้งหมายเลขบัญชีให้เหยื่อทราบ เพื่อให้ทำการจ่ายเงินค่าไถ่ในรูปแบบของเงินอิเล็กทรอนิกส์ (eCurrency) เช่น บิตคอยน์ ซึ่งการจ่ายเงินค่าไถ่รูปแบบนี้ เหยื่อจะต้องทำการเปิดบัญชีบิตคอยน์เพื่อทำการฝากเงินและโอนเงินตามคำแนะนำของผู้โจมตีซึ่งไม่ต้องการให้มีการระบุตัวตนของผู้โจมตี

3.5.2 บังคับให้เหยื่อดาวน์โหลดไคลเอนต์ระบบความปลอดภัยที่ไม่ระบุตัวตน ซึ่งเป็นบริการที่สร้างขึ้นเพื่อให้ผู้คนสามารถท่องอินเทอร์เน็ตได้โดยไม่เปิดเผยตัวตน ทำให้เหยื่อสามารถสื่อสารผ่านเบราว์เซอร์ Tor เพื่อเปิดใช้งานการจ่ายเงินค่าไถ่แบบไม่ระบุตัวตนได้

3.5.3 จ่ายเงินค่าไถ่ การจ่ายเงินนี้อาจเป็นการจ่ายด้วยสกุลเงินอิเล็กทรอนิกส์ใดก็ได้ที่มิจฉาชีพออนไลน์กำหนด ซึ่งเหยื่อจะต้องระบุหมายเลขประจำตัวที่มัลแวร์เรียกค่าไถ่ให้มา และถือเป็นส่วนหนึ่งของกระบวนการแจ้งเตือนเพื่อรับข้อมูลซึ่งถือเป็นความลับสำหรับใช้ในการถอดรหัสข้อมูล

3.6 เหตุการณ์สำคัญที่เกี่ยวข้องกับการโจมตีด้วยมัลแวร์เรียกค่าไถ่

3.6.1 เหตุการณ์ในต่างประเทศ จากการศึกษานี้พบว่า มัลแวร์เรียกค่าไถ่มักจะมุ่งเน้นโจมตีหน่วยงานภาครัฐและภาคเอกชนขนาดใหญ่ ซึ่งสามารถส่งผลกระทบกับประชาชนทั่วไปในวงกว้าง โดยมีวัตถุประสงค์ในการโจมตีที่หลากหลาย แต่โดยส่วนใหญ่มักต้องการเงินจากค่าไถ่เป็นหลัก ดังตัวอย่างเหตุการณ์ที่เคยเกิดขึ้นในต่างประเทศที่ได้รวบรวมไว้ ดังนี้

ในเดือนพฤศจิกายน พ.ศ. 2559 ระบบคอมพิวเตอร์จัดการตั๋วและระบบอีเมลของรถไฟฟ้าในเมืองซานฟรานซิสโก สหรัฐอเมริกา ถูกมัลแวร์เรียกค่าไถ่โจมตี ทำให้ต้องเปิดให้บริการฟรีในช่วงที่เกิดปัญหา (“San Francisco Rail System Hacker Hacked”, 2016) และถูกเรียกค่าไถ่ข้อมูลเป็นจำนวน 100 บิตคอยน์ (ปัจจุบันประมาณ 145 ล้านบาท) พร้อมขู่ว่าจะเปิดเผยข้อมูลส่วนตัวของพนักงานและลูกค้าออกสู่สาธารณะ อย่างไรก็ตาม หน่วยงานมีประสบการณ์การแก้ปัญหาระบบควบคุมการเดินรถ จึงมีระบบสำรองที่ช่วยให้กู้คืนระบบหลักให้กลับมาเป็นปกติได้อย่างรวดเร็ว

ปี พ.ศ. 2560 ระบบการรักษาพยาบาลในอังกฤษ และส่วนอื่น ๆ ของยุโรป ได้ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ WannaCry ทำให้โรงพยาบาลหลาย ๆ แห่งต้องหยุดการให้บริการ นอกจากนี้ มัลแวร์ดังกล่าวยังได้ส่งผลกระทบไปอีกหลายประเทศทั่วโลก โดยลุกลามไปยังเครื่องคอมพิวเตอร์ประมาณ 200,000 เครื่อง (Chappell, 2017; Rousseau, 2017; “The top 5 UK ransomware attacks”, n.d.) และเมื่อต้นไตรมาสที่ 3 ปีเดียวกัน Maersk ซึ่งเป็นบริษัทขนส่งสินค้าทางทะเลรายใหญ่ของเดนมาร์ก ได้ถูกมัลแวร์เรียกค่าไถ่ NotPetya โจมตี (Thomson, 2017) ทำให้ระบบต่าง ๆ ภายในท่าเรือ 76 แห่งทั่วโลกใช้งานไม่ได้และต้องปิดระบบเครือข่ายภายในองค์กรหลายวัน รวมถึงระบบอีเมลด้วย ซึ่งส่งผลกระทบต่อรายรับในไตรมาสนั้นที่ลดลงกว่า 200 ล้านดอลลาร์สหรัฐฯ (6,600 ล้านบาท)

ในอีก 1 ปีถัดมา (พ.ศ. 2561) ได้มีเหตุการณ์ที่มัลแวร์เรียกค่าไถ่ SamSam โจมตีระบบการจ่ายเงินค่าสาธารณูปโภคออนไลน์ของเมืองแอตแลนตา ในรัฐจอร์เจีย สหรัฐอเมริกา เมื่อเดือนเมษายน โดยค่าไถ่ที่ผู้โจมตีเรียกร้องคือ 6 บิตคอยน์ เป็นเงิน 7,600 ล้านบาท (มูลค่า ณ วันที่ 5 กรกฎาคม พ.ศ. 2564) สำหรับการถอดรหัสคอมพิวเตอร์ทุกเครื่องที่ได้รับผลกระทบ ทำให้ผู้บริหารเมืองต้องใช้เงิน 2.6 ล้านดอลลาร์สหรัฐฯ ในการว่าจ้างผู้เชี่ยวชาญในการแก้ไขระบบ (Newman, 2018; O'Donnell, 2018)

กลางไตรมาสที่ 3 พ.ศ. 2563 Garmin ซึ่งเป็นบริษัทเทคโนโลยีได้แจ้งปิดระบบและบริการต่าง ๆ ทั่วโลก ได้ถูกมัลแวร์เรียกค่าไถโจมตีโดยเรียกค่าไถ่สูงถึง 10 ล้านดอลลาร์สหรัฐฯ (ปัจจุบันประมาณ 332 ล้านบาท) ซึ่งส่งผลทำให้บริการต่าง ๆ ของ Garmin Connect ไม่สามารถใช้งานได้ โดยมีรายงานว่า Garmin ยอมจ่ายเงินค่าไถ่เพื่อกู้คืนระบบ ทั้งนี้ผู้เชี่ยวชาญเชื่อว่ามัลแวร์เรียกค่าไถ่ดังกล่าวคือ WastedLocker (Abrams, 2020) หลังจากนั้นราว 2 เดือน โรงพยาบาลแห่งมหาวิทยาลัยดุสเซนดอร์ฟ (University Hospital Düsseldorf) ในสหพันธ์สาธารณรัฐเยอรมนี ได้ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ ทำให้ระบบคอมพิวเตอร์ของโรงพยาบาลขัดข้อง จึงไม่สามารถรับผู้ป่วยนอกและรักษาแบบฉุกเฉินได้ ต้องส่งตัวผู้ป่วยรายหนึ่งไปยังโรงพยาบาลที่อยู่ห่างออกไปกว่า 30 กิโลเมตร และเสียชีวิตระหว่างทาง อย่างไรก็ตาม ตำรวจได้ติดต่อและแจ้งผู้โจมตีว่าระบบที่ถูกโจมตีเป็นระบบคอมพิวเตอร์ของโรงพยาบาล ผู้โจมตีจึงได้มอบกุญแจดิจิทัลให้เจ้าหน้าที่ทำการกู้คืนระบบเพื่อให้ระบบกลับมาใช้งานได้อีกครั้ง (Abrams, 2020)

จากนั้นในเดือนตุลาคมปีเดียวกัน มัลแวร์เรียกค่าไถ่ที่ชื่อ DoppelPaymer ถูกใช้ในการโจมตีเครือข่ายคอมพิวเตอร์ของเมืองฮอลล์เคาตี้ ในรัฐจอร์เจีย สหรัฐอเมริกา ซึ่งเครือข่ายคอมพิวเตอร์ดังกล่าวเชื่อมต่อกับหลายระบบ โดยเฉพาะอย่างยิ่งระบบจัดการการเลือกตั้งซึ่งจัดเก็บข้อมูลของผู้มีสิทธิ์เลือกตั้งบางส่วนเอาไว้ อย่างไรก็ตาม เนื่องจากทางเมืองฮอลล์เคาตี้ไม่ยอมจ่ายเงินค่าไถ่ ผู้โจมตีจึงได้ทำการเผยแพร่ตัวอย่างข้อมูลที่ผู้โจมตีได้ไป โดยข้อมูลดังกล่าวมีข้อมูลส่วนบุคคล เช่น หมายเลขประกันสังคม ซึ่งถือเป็นข้อมูลส่วนบุคคลของผู้มีสิทธิ์เลือกตั้งรวมอยู่ด้วย ซึ่งกรณีนี้ถือเป็นกรณีแรกในปี พ.ศ. 2563 ที่การโจมตีด้วยมัลแวร์เรียกค่าไถ่ส่งผลกระทบต่อโครงสร้างพื้นฐานการเลือกตั้งที่เกี่ยวโยงกับการเลือกตั้งประธานาธิบดีในเดือนพฤศจิกายน (Fung, 2020; Hobbs, 2020)

3.6.2 เหตุการณ์ในประเทศไทย จากการศึกษาและรวบรวมข้อมูลจากแหล่งต่าง ๆ ที่มีการรายงานและเปิดเผยข้อมูล พบว่ามีเหตุการณ์การโจมตีโดยมัลแวร์เรียกค่าไถ่ในประเทศไทยเกิดขึ้นหลายครั้ง ดังที่ผู้เขียนได้สรุปไว้ในภาพที่ 4 ซึ่งอธิบายได้พอสังเขปดังนี้

พ.ศ. 2558	ศูนย์เทคโนโลยีสารสนเทศแจ้งเตือนภัยจากมัลแวร์เรียกค่าไถ่ครั้งแรก หลังจากมีการตรวจพบอีเมลที่มีผู้หลอกโจมตีจำนวนมาก
พ.ศ. 2560	• มัลแวร์เรียกค่าไถ่ WannaCry โจมตีเซิร์ฟเวอร์เกมออนไลน์ Garena บริษัทแจ้งปิดระบบจนกว่าจะแก้ไขเสร็จ • มัลแวร์เรียกค่าไถ่โจมตีระบบป้ายโฆษณาดิจิทัลบนถนนวิทยุและถนนวิภาวดี กรุงเทพมหานคร • สำนักงานตำรวจแห่งชาติถูกมัลแวร์เรียกค่าไถ่ WannaCry โจมตี ทำให้ไม่สามารถแจ้งเหตุด่วนเหตุร้ายผ่านระบบเครือข่ายคอมพิวเตอร์ได้
พ.ศ. 2562	โรงงาน Hoya Corporation ในประเทศไทยถูกมัลแวร์เรียกค่าไถ่โจมตี ทำให้ไม่สามารถดูคำสั่งซื้อและออกใบแจ้งหนี้ได้
พ.ศ. 2563	• การไฟฟ้าส่วนภูมิภาคถูกมัลแวร์เรียกค่าไถ่ Maze โจมตี ทำให้ไม่สามารถใช้แอปพลิเคชันค่าบริการได้ • บริษัท ไทยเบฟเวอเรจ จำกัด (มหาชน) (ThaiBev) ถูกมัลแวร์เรียกค่าไถ่ Maze โจมตี ทำให้ไม่สามารถเปิดไฟล์ข้อมูลได้ • โรงพยาบาลสระบุรีถูกมัลแวร์เรียกค่าไถ่โจมตี ทำให้ข้อมูลประวัติการรักษาของผู้ป่วยสูญหาย
พ.ศ. 2564	• G-Able บริษัทให้บริการเครือข่ายสารสนเทศถูกมัลแวร์เรียกค่าไถ่โจมตีและถูกลักลอบนำข้อมูลออกจากระบบมากกว่า 100 MB • สายการบินบางกอกแอร์เวย์ส (Bangkok Airways) ถูกกลุ่ม LockBit กลุ่มแฮกเกอร์สายมัลแวร์เรียกค่าไถ่โจมตีและลักลอบนำข้อมูลออกจากระบบมากกว่า 200 GB

ภาพที่ 4 สรุปลำดับเหตุการณ์มัลแวร์เรียกค่าไถ่ในประเทศไทย

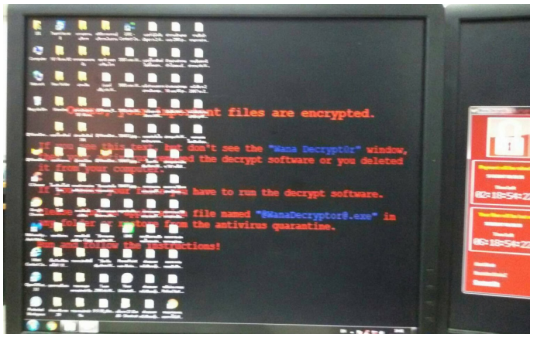
ต้นไตรมาสที่ 2 พ.ศ. 2558 ศูนย์เทคโนโลยีและสารสนเทศ (The Technology and Information Centre: TIC) ได้ออกแถลงการณ์แจ้งเตือนผู้ใช้คอมพิวเตอร์ว่ามีการส่งมัลแวร์เรียกค่าไถ่แพร่กระจายทางอีเมล โดยใช้ชื่อหัวเรื่องที่มีคำว่า “บัญชีถูกล็อก” หรือ “ถูกระงับ” ซึ่งอีเมลเหล่านี้มีไฟล์แนบหลอกให้เข้าไปเปิดไฟล์ แล้วเครื่องคอมพิวเตอร์จะถูกล็อก และถูกเรียกให้จ่ายค่าไถ่ด้วยเงินบิตคอยน์มูลค่า 650 ดอลลาร์สหรัฐฯ (ประมาณ 20,000 บาท) เพื่อแลกกับรหัสปลดล็อกคอมพิวเตอร์ โดยตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี มีการตรวจพบถึง 82 อีเมลที่มีผู้หลอกโจมตีซึ่งเผยแพร่โดยเครื่องแม่ข่ายอีเมลในประเทศไทย โดยทางศูนย์ฯ ได้แนะนำให้ผู้ที่ได้รับอีเมลลักษณะดังกล่าวให้ลบทิ้งทันที มัลแวร์เรียกค่าไถ่ดังกล่าวเป็นมัลแวร์เรียกค่าไถ่ประเภท CTB Locker ซึ่งมีต้นกำเนิดในสหพันธรัฐรัสเซียและยูเครน (Eakkapop, 2015)

กลางเดือนพฤษภาคม พ.ศ. 2560 เครื่องแม่ข่ายเกมออนไลน์ Garena Online (Thailand) ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ WannaCry ซึ่งเพิ่งโจมตีหลายประเทศทั่วโลก เกมออนไลน์ชื่อ Blade & Soul ได้ทำการปิดระบบออนไลน์ เนื่องจากเครื่องแม่ข่ายถูกโจมตี แล้วบริษัทได้กู้คืนระบบและสามารถกู้คืนข้อมูลของผู้เล่นแต่ละคนไว้ได้เหมือนเดิมเมื่อเกมกลับมาออนไลน์ได้ และผู้เล่นสามารถเล่นเกมต่อจากจุดที่เคยเล่นไว้ได้ทันที (Fredrickson, 2017)

ในช่วงเดือนเดียวกัน (15 พฤษภาคม พ.ศ. 2560) มีการเผยแพร่ภาพบนทวิตเตอร์ (Twitter) ซึ่งเป็นภาพป้ายโฆษณาดิจิทัลบนถนนวิทยุ (ดังภาพที่ 5) และถนนวิภาวดี กรุงเทพมหานคร ซึ่งมีข้อความที่แสดงให้เห็นว่า ระบบของป้ายโฆษณาดิจิทัลดังกล่าวถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ WannaCry จากเหตุการณ์นี้สำนักงานตำรวจแห่งชาติแจ้งเตือนให้ทุกหน่วยงานระมัดระวังในการดาวน์โหลดไฟล์จากอินเทอร์เน็ตเพื่อจำกัดความเสี่ยงของการติดมัลแวร์เรียกค่าไถ่ WannaCry (Thaivisa, 2017) อย่างไรก็ตาม 5 วันถัดมา สำนักงานตำรวจแห่งชาติได้เปิดเผยว่ามีมัลแวร์เรียกค่าไถ่ WannaCry โจมตีระบบคอมพิวเตอร์ของศูนย์รับแจ้งเหตุฉุกเฉิน 191 ของจังหวัดศรีสะเกษ และจังหวัดฉะเชิงเทรา (ดังภาพที่ 6) ทำให้ระบบไม่สามารถรองรับการรับแจ้งเหตุ (“งานเข้า ศูนย์ฯ 191 โดนมัลแวร์เรียกค่าไถ่โจมตีฯ”, 2560)

ภาพที่ 5 ป้ายโฆษณาดิจิทัลบนถนนวิทยุ ถูกมัลแวร์เรียกค่าไถ่โจมตี

ที่มา: Thaivisa (2017)



ภาพที่ 6 คอมพิวเตอร์ของสำนักงานตำรวจแห่งชาติ ถูกมัลแวร์เรียกค่าไถ่ WannaCry โจมตี

ที่มา: “งานเข้า ศูนย์ฯ 191 โดนมัลแวร์เรียกค่าไถ่โจมตีฯ” (2560)

นอกจากนี้ ยังมีรายงานว่า บริษัท HOYA Corporation ผู้ผลิตผลิตภัณฑ์ออปติกจากญี่ปุ่นถูกโจมตีทางไซเบอร์เมื่อปลายเดือนกุมภาพันธ์ พ.ศ. 2562 ทำให้ต้องปิดสายการผลิตบางส่วนในประเทศไทยเป็นเวลา 3 วัน ทั้งนี้บริษัทเปิดเผยว่า คอมพิวเตอร์ราว 100 เครื่องติดมัลแวร์ที่ออกแบบมาเพื่อขโมยข้อมูล นอกจากนี้ ยังทำให้พนักงานไม่สามารถดูคำสั่งซื้อได้ และคอมพิวเตอร์ที่สำนักงานใหญ่ในญี่ปุ่นก็ได้รับผลกระทบไปด้วย จึงไม่สามารถออกใบแจ้งหนี้ได้ ส่งผลทำให้กำลังการผลิตของโรงงานลดลงประมาณร้อยละ 60 (Gatlan, 2019) ในเดือนมิถุนายน พ.ศ. 2563 มัลแวร์เรียกค่าไถ่ Maze ได้โจมตีการไฟฟ้าส่วนภูมิภาค (กฟภ.) ผ่านทางอีเมล ส่งผลให้ประชาชนไม่สามารถจ่ายค่าไฟผ่านแอปพลิเคชันบนโทรศัพท์มือถือได้ (“การไฟฟ้าฯ”, 2563) กฟภ. จึงได้ปิดระบบเพื่อแก้ไขปัญหาและเปิดระบบใหม่ แล้วถูกโจมตีซ้ำด้วยมัลแวร์เรียกค่าไถ่อีกครั้งในอีกไม่กี่วันถัดมา ซึ่งครั้งนี้มีเจ้าหน้าที่ของศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เข้ามาร่วมตรวจสอบระบบและร่วมให้คำแนะนำในการกู้คืนระบบ (Varghese, 2020) จากนั้นในช่วงต้นเดือนสิงหาคมปีเดียวกัน

บริษัท ไทยเบฟเวอเรจ จำกัด (มหาชน) ก็ได้ถูกมัลแวร์เรียกค่าไถ่ Maze โจมตีระบบคอมพิวเตอร์ ซึ่งเป็นชนิดเดียวกันกับที่มีการโจมตี กฟภ. และมีรายงานของกลุ่ม Maze ที่ระบุรายละเอียดของบริษัทที่ตกเป็นเหยื่อของการโจมตีดังกล่าวด้วย รวมถึงการระบุชื่อไฟล์ที่เข้ารหัสเรียกค่าไถ่ขนาด 713 MB โดยผู้โจมตีประกาศว่าให้เวลา 10 วัน ในการดำเนินการจ่ายค่าไถ่ (Lebowski, 2020)

นอกจากนี้ยังมีกรณีของโรงพยาบาลสระบุรีที่เป็นข่าวดัง ซึ่งถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ชื่อ Voidcrypt/Spade ซึ่งเข้าโจมตีเมื่อวันที่ 5 กันยายน พ.ศ. 2563 (ณัชธนัท จุโฬทก, 2563) ส่งผลให้เครื่องคอมพิวเตอร์แม่ข่าย เครือข่ายระบบโทรศัพท์ภายในโรงพยาบาล รวมถึงฐานข้อมูลของผู้ป่วยและภาพสแกนเวชระเบียนผู้ป่วยไม่สามารถใช้งานได้ทั้งหมด อย่างไรก็ตาม มีรายงานว่า ตามที่มีข่าวการเรียกเงินค่าไถ่จำนวน 200,000 บิตคอยน์ (ประมาณ 63,000 ล้านบาท) ในสื่อนั้นไม่เป็นความจริง นอกจากกรณีของโรงพยาบาลสระบุรียังมีรายงานด้วยว่าที่โรงพยาบาลมหาราชนครเชียงใหม่ก็เคยถูกโจมตีเช่นกันเมื่อ พ.ศ. 2562 (“แคสเปอร์สกี้กระตุ้นโรงพยาบาลไทยฯ”, 2563)

สำหรับกรณีล่าสุด มัลแวร์เรียกค่าไถ่ได้โจมตีบริษัทผู้บริการด้านระบบสารสนเทศชั้นนำแห่งหนึ่งในประเทศไทย เมื่อวันที่ 25 สิงหาคม พ.ศ. 2564 โดยกลุ่มที่ชื่อว่า BlackMatter ซึ่งได้ประกาศการโจมตีระบบของบริษัท G-Able ซึ่งเป็นบริษัทที่ให้บริการด้านการป้องกันระบบและเครือข่ายสารสนเทศ ส่งผลให้ข้อมูลในระบบถูกล็อก ในรายงานข่าวระบุว่า มีการอ้างในเว็บไซต์ของกลุ่ม BlackMatter ว่าได้นำไฟล์ข้อมูลออกมาจากระบบของบริษัทดังกล่าวมากกว่า 100 กิกะไบต์ และมีการปล่อยไฟล์จำนวนหนึ่งออกมาเพื่อเป็นการยืนยันว่ากลุ่มดังกล่าวมีการครอบครองไฟล์ข้อมูลอยู่จริง อย่างไรก็ตาม ทางบริษัทได้ชี้แจงว่าบริษัทได้ตรวจพบความผิดปกติของระบบเครือข่ายจากมัลแวร์ประเภทหนึ่ง และได้เข้าควบคุมและกู้คืนระบบที่ได้รับผลกระทบแล้วจากระบบสำรองข้อมูล และระบุว่าเหตุการณ์นี้ไม่มีผลกระทบต่อการดำเนินงานของบริษัทและลูกค้าแต่อย่างใด (“G-Able ถูกเรียกค่าไถ่ฯ”, 2564)

สำหรับกรณีสุดท้ายในบทความนี้ ในช่วงต้นเดือนกันยายน พ.ศ. 2564 มีรายงานข่าวว่าสายการบินบางกอกแอร์เวย์ส (Bangkok Airways) ได้ทำการแจ้งเตือนลูกค้าให้รีบทำการเปลี่ยนรหัสผ่าน และติดต่อกับผู้ให้บริการบัตรเครดิตโดยด่วน เนื่องจากบริษัทถูกกลุ่มแฮ็กเกอร์ LockBit โจมตีด้วยมัลแวร์เรียกค่าไถ่ และมีรายงานว่า มีข้อมูลเกี่ยวกับธุรกิจกว่า 200 GB ถูกเผยแพร่ออกมา หลังจากที่บริษัทฯ ปฏิเสธที่จะจ่ายเงินค่าไถ่ อย่างไรก็ตาม มีข้อมูลส่วนตัวของผู้โดยสารที่เคยใช้บริการถูกปล่อยออกมาด้วย เช่น ชื่อ-นามสกุล เบอร์โทรศัพท์ อีเมล ที่อยู่ ข้อมูลหนังสือเดินทาง และเลขบัตรเครดิต เป็นต้น (“ข้อมูลลูกค้า Bangkok Airways”, 2564)

3.7 มาตรการเตรียมพร้อมรับมือมัลแวร์เรียกค่าไถ่

เพื่อรองรับปัญหามัลแวร์เรียกค่าไถ่ที่อาจเกิดขึ้นกับองค์กร ผู้บริหาร ผู้ดูแลระบบสารสนเทศตลอดจนผู้ใช้งานควรดำเนินการดังนี้ (สุรชัย ฉัตรเฉลิมพันธุ์ และเทอดพงษ์ แดงสี, 2563, น. 4-5; Gallegos-Segovia et al., 2017; Microsoft, n.d.; Sood et al., 2018)

3.7.1 ดำเนินการสำรองข้อมูลระบบ การดำเนินการอย่างแรกและเป็นการดำเนินการที่ได้ผลดีที่สุดคือ การกู้คืนจากข้อมูลสำรอง ดังนั้น การสำรองข้อมูลควรทำอย่างสม่ำเสมอและสมบูรณ์ โดยเฉพาะอย่างยิ่ง การสำรองข้อมูลสำคัญหลาย ๆ ครั้งเป็นสิ่งที่จำเป็น นอกจากนี้การสำรองข้อมูลบนคลาวด์จะดีกว่าการเก็บรักษาสำเนาในเครื่อง เนื่องจากมัลแวร์เรียกค่าไถ่สามารถค้นหาและลบหรือเข้ารหัสข้อมูลสำรองบนโฮสต์ (Host) และเครือข่ายได้ หากไม่สามารถสำรองข้อมูลบนบริการคลาวด์ได้ การสำรองข้อมูลจะต้องแยกออกจากกัน เช่น การสำรองข้อมูลจากระบบของสำนักงานใหญ่ การเก็บไว้บนระบบจัดเก็บข้อมูลของสำนักงานสาขาที่มีความมั่นคงปลอดภัย เป็นต้น ในกรณีที่ใช้ระบบปฏิบัติการวินโดวส์ ควรทำการสำรองข้อมูลและลองทำการคืนค่าไฟล์เมื่อถูกโจมตีโดยมัลแวร์เรียกค่าไถ่

3.7.2 ดำเนินการอัปเดตระบบ มัลแวร์เรียกค่าไถ่บางตัว เช่น WannaCry และ Petya ใช้ประโยชน์จากช่องโหว่ที่เป็นที่รู้จักในระบบปฏิบัติการในการแพร่กระจายตัวเอง ดังนั้น การอัปเดตระบบปฏิบัติการให้ทันสมัยอยู่เสมอจะช่วยป้องกันมัลแวร์เรียกค่าไถ่ดังกล่าวได้ นอกจากนั้นแล้ว ต้องทำการอัปเดตโปรแกรมทั้งหมดที่มีการใช้งานด้วย เช่น เบราว์เซอร์ เนื่องจากอาจมีช่องโหว่ให้ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ได้เช่นกัน

3.7.3 ดำเนินการควบคุมการเข้าถึงเว็บไซต์และเนื้อหาที่มีความเสี่ยง โดยทั่วไปแผนกไอทีมีบทบาทและหน้าที่ในการจัดการเกี่ยวกับความเสี่ยงจากภัยคุกคามจากมัลแวร์ต่าง ๆ อย่างไรก็ตาม สำหรับองค์กรขนาดใหญ่จะมีกลุ่มงานที่ดูแลด้านความมั่นคงปลอดภัยโดยเฉพาะ ซึ่งทำหน้าที่ควบคุมการเข้าถึงเว็บไซต์และเนื้อหาที่มีความเสี่ยงหรืออาจเป็นแหล่งแพร่มัลแวร์ต่าง ๆ โดยทำการขึ้นบัญชี หรือแบล็กลิสต์ (Blacklist) ของโดเมนเนม (Domain name) ที่ไม่เหมาะสมหรือเสี่ยงที่จะเป็นแหล่งแพร่มัลแวร์ โดยเฉพาะอย่างยิ่งโดเมนเนมหรือไอพีแอดเดรส (IP address) ที่มัลแวร์ใช้ในการสร้างโดเมนเนมปลอมแบบสุ่มด้วยอัลกอริทึม DGA (Domain Generation Algorithms: DGA)

3.7.4 ดำเนินการติดตั้งโปรแกรมและระบบป้องกัน โปรแกรมป้องกันไวรัส (Antivirus software) รวมถึงมัลแวร์เรียกค่าไถ่จะสแกนไฟล์ที่น่าสงสัยทั้งหมดและทำการวิเคราะห์ว่าไฟล์เหล่านั้นปลอดภัยหรือไม่ และหากตรวจพบก็จะทำการหยุดการทำงานของมัลแวร์เหล่านั้น ส่วนไฟร์วอลล์ (Firewall) เป็นระบบที่สามารถป้องกันการรับส่งข้อมูลที่เป็นอันตราย เช่น การสื่อสารจากมัลแวร์เรียกค่าไถ่ไปยังเครื่องแม่ข่ายระบบคำสั่งและการควบคุมซึ่งสามารถป้องกันไม่ให้มัลแวร์เรียกค่าไถ่ทำงานได้ นอกจากนี้ องค์กรควรมีระบบวีพีเอ็น (Virtual Private Network: VPN) สำหรับให้พนักงานสามารถเข้าถึงระบบสารสนเทศขององค์กรผ่านเครือข่ายสาธารณะได้อย่างปลอดภัย

3.7.5 ปิดการใช้งานยูทิลิตีของวินโดวส์ที่ไม่จำเป็น มัลแวร์เรียกค่าไถ่ (บางตัว) สามารถลบไฟล์ Visio Stencil (VSS) บนวินโดวส์ได้ ด้วยการใช้งานวินโดวส์ยูทิลิตี (Utility program) ที่มีความสามารถในการลบไฟล์ VSS และในทำนองเดียวกัน Windows Script Host (WSH) ก็มักจะมีมัลแวร์เรียกค่าไถ่บางตัวที่ถูกพัฒนาบนพื้นฐานของ JavaScript นำไปใช้งานในทางที่ผิดด้วย ดังนั้นจึงควรปิดการใช้งานวินโดวส์ยูทิลิตีที่ไม่จำเป็นซึ่งรวมไปถึงสคริปต์ PowerShell ด้วย

3.7.6 ใช้รหัสผ่านที่คาดเดาได้ยาก มัลแวร์เรียกค่าไถ่บางตัว เช่น WYSIWYE และ SamSam สามารถโจมตีระบบได้ด้วยการสุ่มเดารหัสผ่านของ RDP login ซึ่งเป็นโพรโทคอล (Protocol) ที่ใช้สำหรับโปรแกรมควบคุมเครื่องคอมพิวเตอร์ระยะไกล อย่างไรก็ตาม ปัญหานี้เป็นปัญหาที่สามารถป้องกันได้ง่าย ๆ ด้วยการตั้งรหัสผ่านสำหรับการเข้าถึงระยะไกล (Remote access) ทั้งหมดให้มีความซับซ้อนและคาดเดาได้ยาก รวมไปถึงการกำหนดนโยบายที่เหมาะสมบนไฟร์วอลล์เพื่อสกัดกั้นทราฟฟิก (Traffic) ที่ไม่ได้รับอนุญาตหรือไม่มีสิทธิ์ในการเข้าถึงระบบ

3.7.7 ดำเนินการฝึกอบรมและการสร้างความตระหนักรู้ให้กับพนักงาน ดำเนินการฝึกอบรมและสร้างความตระหนักรู้ให้กับพนักงานด้วยกระบวนการต่าง ๆ เช่น การอบรมถ่ายทอดความรู้ การแนะนำให้หลีกเลี่ยงการดาวน์โหลดจากแหล่งที่ไม่น่าเชื่อถือ ให้ระวังในการเปิดไฟล์แนบที่หลอกล่อด้วยคำหรือเนื้อหาที่ดูน่าสนใจ เช่น ใบแจ้งหนี้ (ยกเว้นกรณีที่ส่งมาจากแหล่งที่เชื่อถือได้) ห้ามกดหรือคลิกลิงก์หรือยูอาร์แอลที่น่าสงสัย ไม่รู้จัก หรือไม่น่าเชื่อถือ และหลีกเลี่ยงการต่อแฟลชไดรฟ์ที่ไม่รู้จักหรือไม่น่าเชื่อถือ เป็นต้น และอาจรวมถึงการจำลองการโจมตีเพื่อให้พนักงานมีความตระหนักและรู้เท่าทันภัยทางไซเบอร์

3.7.8 ดำเนินการจัดทำแผนฉุกเฉินและแผนความต่อเนื่องทางธุรกิจ เพื่อให้องค์กรสามารถดำเนินงานหรือกิจกรรมต่าง ๆ ได้อย่างต่อเนื่องแม้จะประสบปัญหาวิกฤตที่อาจเกิดจากการถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ ควรมีการจัดทำแผนฉุกเฉินหรือแผนบริหารความต่อเนื่อง โดยจะต้องทำการศึกษาผลกระทบที่อาจเกิดขึ้นจากการโจมตีของมัลแวร์ต่าง ๆ มีการวิเคราะห์และคาดการณ์ความเสี่ยง ตลอดจนกำหนดแผนฟื้นฟู อย่างไรก็ตาม จะต้องมีการทดสอบแผนและมีการซ้อมแผน เพื่อจะได้ปรับปรุงแผนหากพบปัญหาในระหว่างการทดสอบหรือซ้อมแผน

3.7.9 ติดตามข่าวสารช่องโหว่หรือภัยคุกคามต่าง ๆ ควรติดตามข่าวสารเกี่ยวกับช่องโหว่หรือภัยคุกคามต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เช่น ข่าวสารจากที่เผยแพร่ผ่านเว็บไซต์ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) เป็นต้น รวมถึงการศึกษาหาความรู้เกี่ยวกับวิธีการป้องกันมัลแวร์เรียกค่าไถ่และมัลแวร์หรือการโจมตีอื่น ๆ เพื่อไม่ให้ตกเป็นเหยื่อของเหล่าผู้ไม่หวังดีหรือมิจฉาชีพออนไลน์ และเพื่อความปลอดภัยขององค์กรและตัวผู้ใช้งานเอง

3.8 มาตรการรับมือเมื่อถูกโจมตีโดยมัลแวร์เรียกค่าไถ่

เพื่อให้สามารถรับมือได้อย่างทันท่วงทีในกรณีที่มีเครื่องคอมพิวเตอร์ในองค์กรถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ ผู้ดูแลระบบสารสนเทศควรดำเนินการตามมาตรการต่อไปนี้ (โจ ไทดี, 2564; “About the Project”, n.d.; Avast, n.d.; Elradi et al., 2021; Microsoft, n.d.)

3.8.1 ดำเนินการตัดการเชื่อมต่อกับเครือข่ายทุกช่องทาง โดยถอดสายแลน (Local Area Network: LAN) ปิดการทำงานของอุปกรณ์เชื่อมต่ออินเทอร์เน็ตแบบไร้สาย (Wi-Fi) ตลอดจนฮอตสปอต (Hot spot) และเครือข่ายไร้สายส่วนบุคคลหรือบลูทูท (Bluetooth) เพื่อหยุดการแพร่กระจายมัลแวร์เรียกค่าไถ่ไปยังคอมพิวเตอร์และเครื่องแม่ข่ายอื่น ๆ

3.8.2 ตรวจสอบขอบเขตการแพร่กระจายของมัลแวร์เรียกค่าไถ่ โดยตรวจสอบแฟ้มข้อมูลหรือโฟลเดอร์ (Folder) ที่มีการใช้งานร่วมกันกับคอมพิวเตอร์เครื่องอื่นและตรวจสอบเครื่องคอมพิวเตอร์เหล่านั้น รวมไปถึงอุปกรณ์จัดเก็บข้อมูลต่าง ๆ ทั้งที่เชื่อมต่อผ่านเครือข่าย เช่น สตอเรจ (Storage) และที่ไม่ได้เชื่อมต่อผ่านเครือข่าย เช่น ฮาร์ดดิสก์ภายนอก (External hard disk) หรือแฟลชไดรฟ์ นอกจากนี้ควรตรวจสอบด้วยว่าไฟล์ข้อมูลที่จัดเก็บอยู่บนคลาวด์ เช่น Google Drive, DropBox เป็นต้น ถูกมัลแวร์เรียกค่าไถ่ล็อกการเข้าถึงหรือไม่

3.8.3 ตรวจสอบและระบุประเภทและชื่อของมัลแวร์เรียกค่าไถ่ เมื่อมัลแวร์เรียกค่าไถ่โจมตีเครื่องคอมพิวเตอร์ของเหยื่อหรือเป้าหมายแล้ว จะแสดงข้อความบนหน้าจอเพื่อแจ้งให้เหยื่อทราบว่าเครื่องคอมพิวเตอร์ถูกควบคุมโดยมัลแวร์เรียกค่าไถ่แล้ว พร้อมกับข้อความเรียกค่าไถ่ หากต้องการกู้คืนข้อมูล ในกรณีที่เป็นการโจมตีในระดับองค์กร ผู้ดูแลระบบจะต้องตรวจสอบแล้วระบุให้ได้ว่าถูกโจมตีด้วยมัลแวร์ใด เพื่อประสิทธิภาพในการแก้ไขปัญหา รวมไปถึงการร้องขอความช่วยเหลือจากผู้เชี่ยวชาญหรือบริษัทที่ให้บริการระบบรักษาความมั่นคงปลอดภัยไซเบอร์

3.8.4 ตอบสนองอย่างเหมาะสม การตอบสนองอาจแตกต่างกันไปตามสถานการณ์และความรุนแรง ในกรณีที่เป็นองค์กร ต้องทำการแจ้งเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศและหัวหน้าส่วนงานให้รับทราบ (ซึ่งอาจรวมไปถึงการแจ้งข่าวสารไปยังชุมชนออนไลน์ที่เกี่ยวข้องให้ได้รับทราบด้วยเพื่อเป็นการเตือนภัย) ทั้งนี้ ผู้เชี่ยวชาญไม่แนะนำให้จ่ายเงินค่าไถ่ เพราะไม่มีอะไรรับประกันว่าจะสามารถกู้คืนไฟล์ข้อมูลได้ สำหรับแนวทางที่ควรปฏิบัติ ปกติจะเริ่มต้นด้วยการค้นหาข้อมูลสำรอง และหาวิธีลบมัลแวร์เรียกค่าไถ่ออกจากระบบหรือเครื่องคอมพิวเตอร์ที่ติด แล้วทำการกู้คืนข้อมูลจากชุดข้อมูลที่มีการสำรองไว้ อย่างไรก็ตาม หากต้องการที่จะถอดรหัสไฟล์ข้อมูล จำเป็นต้องอาศัยเทคนิคที่อาจมีการเผยแพร่ไว้ในชุมชนออนไลน์หรือเว็บไซต์ของผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้เชี่ยวชาญ ซึ่งปัจจุบันมีมัลแวร์เรียกค่าไถ่หลายตัวที่สามารถถอดรหัสได้แล้ว และเมื่อสามารถแก้ไขปัญหาได้ ควรมีการถอดบทเรียนจากเหตุการณ์ที่เกิดขึ้นและเรียนรู้ร่วมกันระหว่างผู้เกี่ยวข้อง

4. ผลจากการศึกษารายประเด็นและอภิปรายผล

จากการศึกษารายประเด็นนี้พบว่า มัลแวร์เรียกค่าไถ่มีต้นกำเนิดมาจากการใช้ไฟล์ข้อมูลหรือคอมพิวเตอร์ของเหยื่อเป็นตัวประกันเมื่อกว่า 40 ปีที่แล้ว ก่อนที่จะมีวิวัฒนาการมาเป็นมัลแวร์เรียกค่าไถ่ดังเช่นปัจจุบัน ซึ่งมัลแวร์เรียกค่าไถ่ที่เคยแพร่ระบาดส่วนใหญ่เป็นประเภทคริปโตที่มุ่งเน้นการเข้ารหัสข้อมูลแล้วข่มขู่เรียกค่าไถ่ สำหรับลักษณะการโจมตีก็มีหลายรูปแบบ เช่น การโจมตีด้วยการดาวน์โหลด การโจมตีด้วยอีเมลฟิชชิง การโจมตีผ่านช่องโหว่ของระบบ และการโจมตีด้วยการสุ่มรหัสผ่าน เป็นต้น การเรียกค่าไถ่แบ่งได้ 3 ระดับ โดยระดับที่ 3 ร้ายแรงที่สุด เพราะแม้จะได้รับเงินค่าไถ่แล้วก็จะไม่สามารถเปิดไฟล์ข้อมูลได้แบบถาวร แม้เหยื่อจะโอนเงินเพื่อจ่ายค่าไถ่ในรูปแบบของเงินอิเล็กทรอนิกส์ เช่น บิตคอยน์ แล้วก็ตาม ในช่วง 5-6 ปีที่ผ่านมาพบเหตุการณ์การโจมตีด้วยมัลแวร์เรียกค่าไถ่ครั้งใหญ่ ๆ หลายครั้ง ทั้งในและต่างประเทศ เช่น เหตุการณ์ที่ Garmin ซึ่งเป็นบริษัทเทคโนโลยีได้ถูกโจมตีเมื่อช่วงไตรมาสที่ 3 พ.ศ. 2563 ซึ่งเป็นช่วงไล่เลี่ยกับเหตุการณ์การโจมตีโรงพยาบาลสระบุรีที่เป็นข่าวดังในประเทศไทย ที่ส่งผลให้ไม่สามารถเข้าถึงระบบต่าง ๆ รวมถึงข้อมูลเวชระเบียนผู้ป่วยได้ ดังนั้น ผู้มีส่วนเกี่ยวข้องภายในองค์กรจะต้องมีมาตรการเตรียมพร้อมรับมือมัลแวร์เรียกค่าไถ่ เช่น การสำรองข้อมูล การอัปเดตระบบ การฝึกอบรม และการสร้างความตระหนักรู้ให้กับบุคลากร และการจัดทำแผนฉุกเฉินและแผนความต่อเนื่องทางธุรกิจ เป็นต้น นอกจากนี้ จะต้องเตรียมมาตรการรับมือเมื่อถูกโจมตีโดยมัลแวร์เรียกค่าไถ่เอาไว้ด้วย ซึ่งมาตรการเตรียมพร้อมรับมือการโจมตีและรับมือเมื่อถูกโจมตีแต่ละข้อที่เป็นรายละเอียดปลีกย่อยล้วนมีความสำคัญในมิติที่แตกต่างกันที่ผู้เกี่ยวข้องไม่ควรละเลย อย่างไรก็ตาม การดำเนินการตามมาตรการดังกล่าว จำเป็นจะต้องมีงบประมาณสนับสนุนที่อาจเป็นตัวเลขที่ค่อนข้างสูงในช่วงปีแรกที่ดำเนินการ ซึ่งเป็นประเด็นที่ผู้บริหารองค์กรต้องเป็นผู้พิจารณาและดำเนินการขับเคลื่อนเพื่อให้ได้มาซึ่งงบประมาณสำหรับการลงทุนในมาตรการต่าง ๆ เพื่อหลีกเลี่ยงความเสียหายที่อาจประเมินค่ามิได้หากถูกโจมตีโดยมัลแวร์เรียกค่าไถ่

จากการศึกษานี้ ชัดเจนว่า มัลแวร์เรียกค่าไถ่สามารถทำการขัดขวางการเข้าถึงข้อมูลด้วยการเข้ารหัสข้อมูลหรือการล็อกการเข้าถึงข้อมูลด้วยวิธีล็อกการใช้งานเครื่องหรือระบบทั้งหมด ผู้โจมตีอาจใช้มัลแวร์เรียกค่าไถ่ด้วยวัตถุประสงค์ที่หลากหลาย แต่วัตถุประสงค์หลักคือ เพื่อต้องการเงินค่าไถ่จากองค์กรต่าง ๆ โดยเฉพาะอย่างยิ่งภาคเอกชนขนาดใหญ่ หน่วยงานภาครัฐ และโครงสร้างพื้นฐานระดับประเทศ เพื่อให้การโจมตีมีผลกระทบในวงกว้าง เช่น ระบบรถไฟขนส่งผู้โดยสาร ระบบขนส่งสินค้า โรงพยาบาล โรงผลิตไฟฟ้า

อย่างไรก็ตาม คาดว่ามีองค์กรขนาดเล็กจำนวนหนึ่งที่ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ด้วยเช่นกัน เพียงแต่ไม่เป็นข่าวตามสื่อต่าง ๆ นอกจากนี้ยังพบว่า ปัจจุบันมีการโจมตีผ่านโปรแกรมควบคุมเครื่องคอมพิวเตอร์ระยะไกลเพิ่มมากขึ้น ซึ่งเกี่ยวข้องกับการทำงานจากบ้านที่เพิ่มขึ้นอย่างมากในปัจจุบัน อันเป็นผลมาจากการแพร่ระบาดของโควิด-19 ที่ทำให้มีการเปิดการใช้งานแอปพลิเคชันที่ใช้โพรโทคอลอาร์ดีพีมากขึ้น ยิ่งไปกว่านั้นยังพบว่าพฤติกรรมของมัลแวร์เรียกค่าไถ่ได้เปลี่ยนไป โดยผู้โจมตีจะขโมยข้อมูลออกมาก่อน จากนั้นจึงทำการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่โดยแสดงข้อความแจ้งบนหน้าจอคอมพิวเตอร์ นอกจากนี้ยังนำตัวอย่างข้อมูลที่ขโมยออกไปแนบกับอีเมลเพื่อขู่กรรโชกว่าจะนำข้อมูลเผยแพร่ในโลกออนไลน์หากไม่ได้รับการจ่ายเงินภายในเวลาที่กำหนด

5. บทสรุป

จากการศึกษานี้สามารถสรุปได้ว่า มัลแวร์เรียกค่าไถ่เป็นภัยคุกคามทางไซเบอร์ที่สามารถสร้างผลกระทบและสร้างความเสียหายให้กับองค์กรได้อย่างคาดไม่ถึง อย่างไรก็ตาม หากผู้ดูแลระบบสารสนเทศและผู้ใช้งานมีความตระหนักและปฏิบัติตามมาตรการและข้อเสนอแนะในการรับมือมัลแวร์เรียกค่าไถ่อย่างเหมาะสม เช่น การสำรองข้อมูลอย่างสม่ำเสมอ ปรับปรุงระบบปฏิบัติการของระบบวินโดวส์ให้เป็นเวอร์ชันล่าสุด การงดเยี่ยมชมเว็บไซต์ที่มีความเสี่ยงหรือไม่น่าเชื่อถือ และการฝึกอบรมและการสร้างความตระหนักรู้ให้กับพนักงาน เป็นต้น จะสามารถช่วยลดความเสี่ยงและบรรเทาปัญหาที่เกิดจากภัยคุกคามรูปแบบนี้ได้ โดยเฉพาะอย่างยิ่งองค์กรขนาดใหญ่ หน่วยงานรัฐและหน่วยงานที่กำกับดูแลจะต้องปรับตัวให้ทันกับภัยคุกคามทางไซเบอร์ชนิดนี้ และควรมีการเผยแพร่ข้อมูลข่าวสารเกี่ยวกับมัลแวร์เรียกค่าไถ่ ตลอดจนภัยคุกคามรูปแบบอื่น ๆ เพื่อเสริมสร้างความเข้าใจและความตระหนักรู้ให้กับผู้ใช้งาน ในขณะที่ผู้ใช้งานก็ควรรู้เท่าทันเทคโนโลยีอินเทอร์เน็ตและภัยคุกคามทางไซเบอร์ที่อาจมากับเทคโนโลยีนี้ นอกจากนี้ควรสังเกตและตรวจสอบความผิดปกติของระบบคอมพิวเตอร์อย่างสม่ำเสมอ ไม่เปิดเอกสารแนบอีเมล ลิงก์เว็บไซต์ที่ไม่น่าเชื่อถือ โดยควรตรวจสอบที่มาให้แน่ใจก่อนเปิดอ่าน หากสงสัยว่ามีมัลแวร์เรียกค่าไถ่ฝังตัว ให้ยกเลิกการแชร์ไฟล์ โดยเฉพาะอย่างยิ่งการแชร์พื้นที่ในการจัดเก็บข้อมูลกับภายนอก และต้องรายงานเหตุการณ์ต่อผู้ดูแลระบบสารสนเทศหรือผู้เกี่ยวข้องทันที เพื่อเป็นการแจ้งเตือนและป้องกันไม่ให้มัลแวร์เรียกค่าไถ่แพร่กระจายในวงกว้าง

6. ข้อเสนอแนะ

6.1 ข้อเสนอแนะสำหรับการศึกษาในอนาคต บทความนี้นำเสนอเฉพาะมัลแวร์เรียกค่าไถ่เท่านั้น ทั้งนี้ในปัจจุบัน มีภัยคุกคามทางไซเบอร์รูปแบบอื่น ๆ ที่ถูกพัฒนาขึ้นโดยผู้ไม่ประสงค์ดีที่สามารถสร้างความเสียหายให้กับองค์กรได้ไม่ยิ่งหย่อนไปกว่ากัน จึงควรมีการศึกษาค้นคว้าเพิ่มเติมและนำเสนอประเด็นเหล่านั้นในโอกาสต่อไป

6.2 ข้อเสนอแนะเชิงนโยบายสำหรับกิจการสื่อสาร หน่วยงานรัฐที่ทำหน้าที่กำกับดูแลองค์กรหรือหน่วยธุรกิจต่าง ๆ ไม่ว่าจะเป็นสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และกระทรวงพาณิชย์ เป็นต้น อาจออกประกาศที่มีผลบังคับให้องค์กรหรือหน่วยธุรกิจที่อยู่ภายใต้การกำกับดูแลจัดหาระบบสำรองข้อมูลและจัดทำแผนสำรองฉุกเฉินเพื่อรับมือกับการถูกโจมตีทางไซเบอร์ที่อาจเกิดขึ้นได้ในอนาคต ซึ่งจะต้องครอบคลุมกรณีที่ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ด้วย อย่างไรก็ตาม ควรมีบทเฉพาะกาลที่มีการกำหนดกรอบเวลาที่เหมาะสม เพื่อให้องค์กรหรือหน่วยงานที่ต้องปฏิบัติตามประกาศได้มีเวลาเตรียมความพร้อมเพื่อการดำเนินการดังกล่าวด้วย

กิตติกรรมประกาศ

ขอขอบคุณคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ที่ให้การสนับสนุนงานวิจัยนี้

รายการเอกสารอ้างอิง

การไฟฟ้าฯ ยอมรับ โดนมัลแวร์เรียกค่าไถ่โจมตี ทำแอพล่มข้ามอาทิตย์. (2563, 18 มิถุนายน). ข่าวสดออนไลน์. https://www.khaosod.co.th/special-stories/news_4340712

ข้อมูลลูกค้า Bangkok Airways หลุดกว่า 200GB หลังบริษัทฯ ปฏิเสธจ่ายค่าไถ่ให้กลุ่มแฮคเกอร์ LockBit. (2564). Droidsans. https://droidsans.com/bangkok-airways-data-leak-following-ransomeware-hack-lockbit/#:~:text=Bangkok%20Airways%20ออกมาประกาศ,เร่งตรวจสอบและพยายาม

แคสเปอร์สกี้กระตุ้นโรงพยาบาลไทยล่าตัวเอาโทษ หลังถูกแรนซัมแวร์เล่นงาน. (2563, 10 กันยายน). ผู้จัดการออนไลน์. https://mgronline.com/cyberbiz/detail/9630000092735

งานเข้า ศูนย์ฯ 191 โดนมัลแวร์เรียกค่าไถ่โจมตี ปชช. แจ้งเหตุ. (2560, 20 พฤษภาคม). ไทยรัฐออนไลน์. https://www.thairath.co.th/news/crime/947410

โจ ไทดี. (2564). *จ่ายค่าไถ่ให้แฮกเกอร์ : สองมุมมองของผู้เชี่ยวชาญว่าควรทำหรือไม่.* บีบีซีนิวส์. https://www.bbc.com/thai/international-57185714

ณัชธนัท จุโฬทก. (2563). *อัปเดตความคืบหน้า RANSOMWARE รพ.สระบุรี ได้อะไรกลับมาแล้ว.* แบไต๋. https://www.beartai.com/news/it-thai-news/478322

รู้กันยัง Malicious Code ภัยคุกคามไซเบอร์อันดับ 1 ของไทย และเป็นภัยเสี่ยงด้านชำระเงินออนไลน์อีกด้วย. (2558). เดลิเทค. https://www.dailytech.in.th/malicious-code

วิวัฒนาการของ Ransomware และวิธีรับมือโดย CrowdStrike. (2563). เทคทอร์คไทย. https://www.techtalkthai.com/the-evolution-of-ransomware-by-crowdstrike

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2564ก). *VMWare เผยสถิติการโจมตีจากมัลแวร์เรียกค่าไถ่เพิ่มขึ้น 148 % จากสถานการณ์ COVID-19.* ไทยเซิร์ต. https://www.thaicert.or.th/newsbite/2020-04-16-02.html

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2564ข). *สถิติภัย.* ไทยเซิร์ต. https://www.thaicert.or.th/statistics/statistics2020.html

สุรชัย ฉัตรเฉลิมพันธุ์ และเทอดพงษ์ แดงสี. (2563). การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลองการโจมตีด้วยฟิชชิ่ง. *วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธนบุรี, 4*(2), 1-11.

About the Project. (n.d.). No More Ransome. https://www.nomoreransom.org/en/about-the-project.html

Abrams, L. (2020). *Confirmed Garmin received decryptor for WastedLocker ransomware.* Bleeping Computer. https://www.bleepingcomputer.com/news/security/confirmed-garmin- received-decryptor-for-wastedlocker-ransomware

Avast. (n.d.). *เครื่องมือถอดรหัสแรนซัมแวร์ฟรี.* https://www.avast.com/th-th/ransomware-decryption-tools

Challita, A. (2018). *The four most popular methods hackers use to spread ransomware.* ITProPortal. https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/

Chappell, B. (2017). *WannaCry Ransomware: What we know Monday.* NPR. https://www.npr.org/sections/thetwoway/2017/05/15/528451534/wannacry-ransomware-what-we-know-Monday

Eakkapop, T. (2015). *Cybercops warn of wave of ransomware in Thailand.* The Phuket News. https://www.thephuketnews.com/cybercops-warn-of-wave-of-ransomware-in-thailand-52135.php

Elradi, M. D., Mohamed, M. H., & Ali, M. E. (2021). Ransomware Attack: Rescue-checklist Cyber Security Awareness Program. *Artificial Intelligence Advances, 3*(1), 57-62. http://dx.doi.org/10.30564/aia.v3i1.3162

Fredrickson, T. (2017, May 15). *Garena game in Thailand shut down by cyber-attack.* Bangkok Post. https://www.bangkokpost.com/learning/advanced/1249843/garena-game-in-thailand-shut-down-by-cyber-attack

Freedman, L. F. (2020). *Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion.* The National Law Review. https://www.natlawreview.com/ article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion

Fung, B. (2020). *Ransomware hits election infrastructure in Georgia county.* CNN Business. https://edition.cnn.com/2020/10/22/tech/ransomware-election-georgia/index.html

G-Able ถูกเรียกค่าไถโดยมัลแวร์ BlackMatter ข้อมูลบางส่วนถูกเผยแพร่. (2564). Blognone. https://www.blognone.com/node/124406

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017). *Social engineering as an attack vector for ransomware. CHILECON* (pp. 1-6). IEEE.

Gatlan, S. (2019). *Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days.* Bleeping Computer. https://www.bleepingcomputer.com/news/security/cyber-attack-shuts-down-hoya-corps-thailand-plant-for-three-days/

Hobbs, D. T. (2020). *Hacker Releases Georgia County Election Data After Ransom Not Paid.* The Wall Street Journal. https://www.wsj.com/articles/hacker-releases-georgia-county-election-data-after-ransom-not-paid-11603923101

Lebowski, D. (2020). *Thaibev ถูกแฮ็กเกอร์โจมตีเรียกค่าไถ่ จาก MAZE Ransomware ที่การไฟฟ้าส่วนภูมิภาคเคยโดนไปก่อนหน้านี้.* Droidsans. https://droidsans.com/thaibev-maze-ransomware/

Microsoft. (n.d.). *ปกป้องพีซีของคุณจากแรนซัมแวร์.* https://support.microsoft.com/th-th/windows/ปกป้องพีซีของคุณจากแรนซัมแวร์-08ed68a7-939f-726c-7e84-a72ba92c01c3

Newman, L. H. (2018). *Atlanta spent $2.6 M to recover from a $52,000 ransomware scare.* WIRED. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare

O'Donnell, L. (2018). *Ransomware attack cripples several Atlanta city systems.* Threat Post. https://threatpost.com/ransomware-attack-cripplesseveral-atlanta-city systems/130739

Ransomware หรือมัลแวร์เรียกค่าไถ่ คืออะไร เกิดจากอะไร และ Ransomware มีกี่ประเภท. (2563). ไทยแวร์. https://tips.thaiware.com/1381.html

Rousseau, A. (2017). *WCRY/WanaCry Ransomware Technical Analysis. Elastic.* https://www.elastic.co/blog/wcrywanacry-ransomware-technical-analysis

San Francisco Rail System Hacker Hacked. (2016). Krebs on Security. https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked

Savage, K., Coogan, P., & Lau, H. (2015). *The Evolution of ransomware.* Florida State University. https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf

Sood, K. A., Bajpai, P. & Enbody, R. (2018). Evidential Study of Ransomware Cryptoviral Infections and Countermeasures. *ISACA Journal, 5*(5), 1-10. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-5/evidential-study-of-ransomware_joa_eng_1018.pdf

Sophos 2020 Threat Report. (2019). Sophos. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf

Thaivisa. (2017, May 15). *WannaCry ransomware hits the heart of Bangkok.* The Nation Thailand. https://www.nationthailand.com/national/30315265

The top 5 UK ransomware attacks. (n.d.). Acronis. https://www.acronis.com/en-gb/articles/ransomware-attacks/

Thomson, I. (2017). *NotPetya ransomware attack cost us $300 m – shipping giant Maersk.* The Register. https://www.theregister.com/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk

Varghese, S. (2020). *Attackers hit Thai power authority using Maze ransomware.* IT Wire. https://www.itwire.com/security/attackers-hit-thai-power-authority-using-maze-ransomware.html