แรนซัมแวร์ จากภัยคุกคามรายบุคคลสู่ภัยพิบัติขององค์การ
Ransomware from Individual Threats to Corporate Disasters

สรวิศ บุญมี[1] และสุภกัญญา ชวนิชย์[2]
Sorawit Boonmee[1] and Supakanya Chavanich[2]
[1]คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยอีสเทิร์นเอเชีย
[1]School of Information Technology, Eastern Asia University
[2] คณะนิติศาสตร์ มหาวิทยาลัยอีสเทิร์นเอเชีย
[2] School of Law, Eastern Asia University
Received: October 5, 2020
Revised: January 25, 2021
Accepted: February 1, 2021

บทคัดย่อ

แรนซัมแวร์หรือมัลแวร์เรียกค่าไถ่ คือ มัลแวร์ที่ใช้ข้อมูลของเหยื่อเป็นตัวประกันเพื่อแลกกับการจ่ายค่าไถ่ เป็นภัยคุกคามที่สร้างความเสียหายอย่างมากในปัจจุบัน โดยมีการพัฒนาเปลี่ยนรูปแบบจากไวรัสเป็นโทรจันและเวิร์ม และใช้เทคนิคใหม่ ๆ เพื่อหลบเลี่ยงการถูกตรวจจับ อีกทั้งยังนำการเข้ารหัสซึ่งเป็นเทคโนโลยีในการรักษาความลับมาเป็นอาวุธโจมตีเหยื่อ เปลี่ยนรูปแบบการแพร่กระจายไปเรื่อย ๆ ตามเทคโนโลยี และเปลี่ยนเป้าหมายจากผู้ใช้ทั่วไปเป็นองค์การต่าง ๆ เพื่อเพิ่มโอกาสในการได้ค่าไถ่ที่มากขึ้น บทความนี้มุ่งนำเสนอที่มา ขั้นตอนการทำงานของแรนซัมแวร์แบบต่าง ๆ ในเชิงลึก และแนวทางในการป้องกันเพื่อลดความเสี่ยงจากความเสียหายในการสูญเสียสารสนเทศสำคัญ

คำสำคัญ: แรนซัมแวร์ มัลแวร์เรียกค่าไถ่ ความมั่นคงปลอดภัยด้านสารสนเทศ

Abstract

Ransomware is the malware that uses the victim's information as a hostage in exchange for paying the ransom. It's a very destructive threat today. With the development of changing styles from viruses to trojans and worms and use new techniques to evade detection. It also uses encryption, confidentiality technology, as a weapon to attack victims. It keep changing the pattern of spreading according to technology and targeting from general users to organizations to increase the chances of getting more ransom. This article aims to present the background, in-depth procedures of various ransomware, and prevention to reduce the risk of loss of critical information.

Keywords: ransomware, malware, information security

บทนำ

มัลแวร์มีพัฒนาการควบคู่มากับเทคโนโลยีคอมพิวเตอร์ตลอดตั้งแต่อดีต ทั้งรูปแบบที่เริ่มจากไวรัสคอมพิวเตอร์เพื่อวัตถุประสงค์ในการทดสอบแนวคิด หรือก่อกวนสร้างความเดือดร้อนและความเสียหายเพียงเล็กน้อย จนกลายเป็นแรนซัมแวร์หรือมัลแวร์เรียกค่าไถ่ ซึ่งใช้เทคนิคขั้นสูงขึ้นในการสร้างความเสียหายตั้งแต่ระดับบุคคล ไปจนถึงองค์กรขนาดใหญ่ และสร้างผลตอบแทนให้แฮกเกอร์เพิ่มขึ้นเรื่อย ๆ มีรายงานจากการประชุมใหญ่ของผู้เชี่ยวชาญด้านการรักษาความปลอดภัยไซเบอร์ประจำปี ค.ศ. 2020 โดยเจ้าหน้าที่พิเศษของเอฟบีไอประเทศสหรัฐอเมริกาได้อธิบายวิธีตรวจสอบการใช้งานกระเป๋าเงินบิตคอยน์ที่ใช้จ่ายค่าไถ่จากข้อความเรียกค่าไถ่ ทำให้รู้ว่าผู้ที่ตกเป็นเหยื่อของแรนซัมแวร์จ่ายเงินค่าไถ่ไปเท่าไหร่ โดยพบว่า ตั้งแต่เดือนตุลาคมค.ศ. 2013 จนถึงพฤศจิกายน ค.ศ. 2019 มีการจ่ายค่าไถ่ด้วยบิตคอยน์เป็นจำนวนเงินถึง 144,350,000 ดอลลาร์สหรัฐ แต่มูลค่าที่แท้จริงน่าจะสูงกว่าจำนวนที่ตรวจสอบได้เป็นอย่างมากโดยเฉพาะในภาคธุรกิจ (Spadafora, 2020) นอกจากนี้บริษัท FireEye ได้คาดการณ์ว่าปริมาณการโจมตีของแรนซัมแวร์แบบใช้คนสั่งการต่อภาคธุรกิจได้เพิ่มขึ้นถึง 860% ตั้งแต่ปี ค.ศ. 2017 (Vanderlee, 2020)

จากปัญหาดังกล่าว การเข้าใจที่มา และขั้นตอนการทำงานของแรนซัมแวร์ที่สำคัญจะนำไปสู่แนวทางในการป้องกันเพื่อลดความเสี่ยงจากความเสียหายในการสูญเสียสารสนเทศสำคัญได้

ประวัติความเป็นมาของมัลแวร์

พัฒนาการของมัลแวร์ซึ่งเป็นซอฟต์แวร์ที่เจตนาออกแบบมาเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์ตามลำดับเวลาที่สำคัญมีดังต่อไปนี้ (Wikipedia, 2020)

ก่อนปีค.ศ. 1970

- บทความของ John von Neumann เรื่อง Theory of self-reproducing automata ตีพิมพ์ในปี ค.ศ. 1966 บทความนี้มาจากการบรรยายเกี่ยวกับ Theory and Organization of Complicated Automata ในปี ค.ศ. 1949 เป็นผลงานทางวิชาการชิ้นแรกเกี่ยวกับทฤษฎีที่โปรแกรมคอมพิวเตอร์สามารถสำเนาตัวเอง

ค.ศ. 1971–1974

- 1971 ระบบ Creeper ซึ่งเป็นการทดลองสร้างโปรแกรมที่สามารถสำเนาตัวเองเขียนโดย Bob Thomas ที่ BBN Technologies เพื่อทดสอบทฤษฎีของ John von Neumann โดย Creeper แพร่เชื้อสู่คอมพิวเตอร์ DEC

PDP-10 ที่ใช้ระบบปฏิบัติการ TENEX สามารถเจาะเข้าเครือข่าย ARPANET และคัดลอกตัวเองไปยังระบบระยะไกลพร้อมทั้งแสดงข้อความ I'm the creeper, catch me if you can! ต่อมาโปรแกรม Reaper จึงถูกสร้างขึ้นในภายหลังเพื่อลบ Creeper

- 1973 ในภาพยนตร์เรื่อง Westworld ของ Michael Crichton ได้เริ่มกล่าวถึงแนวคิดของไวรัสคอมพิวเตอร์

- 1974 ไวรัส Rabbit (หรือ Wabbit) ซึ่งเป็น fork bomb มากกว่าไวรัส เพราะสามารถสร้างสำเนาของตัวเองหลายชุดบนคอมพิวเตอร์เครื่องเดียว (และถูกตั้งชื่อว่า Rabbit เพราะความเร็วที่ทำได้) จนกระทั่งใช้ทรัพยากรระบบจนหมดและลดประสิทธิภาพของระบบส่งผลให้ระบบล่มในที่สุด

- 1975 เกมส์ Animal ถึงแม้จะไม่ทำความเสียหายให้ระบบแต่ก็ถือเป็นโทรจันตัวแรก โดยมันจะแอบทำสำเนาตัวเองและไวรัสชื่อ PERVADE ไว้ในทุกไดเรกทอรีของผู้ใช้

ค.ศ. 1981–1989

- 1981 โปรแกรมที่เรียกว่า Elk Cloner ซึ่งเขียนขึ้นสำหรับระบบ Apple II ถูกสร้างขึ้นโดย Richard Skrenta นักเรียนมัธยมปลาย โดยอาศัยช่องโหว่ในระบบปฏิบัติการเกี่ยวกับฟล็อปปี้ดิสก์ นับเป็นการแพร่ระบาดของไวรัสคอมพิวเตอร์ขนาดใหญ่ครั้งแรกในประวัติศาสตร์

- 1983 คำว่า virus ได้รับการบัญญัติขึ้นใหม่โดย Frederick B. Cohen ในการอธิบายโปรแกรมคอมพิวเตอร์ที่สามารถสำเนาตัวเอง ในปี 1984 Cohen ใช้วลี computer virus (จากการแนะนำโดยครูของเขา Leonard Adleman) เพื่ออธิบายการทำงานของโปรแกรมดังกล่าวในแง่ของ "การติดเชื้อ" เขาให้คำจำกัดความของ "virus" ว่าเป็น "โปรแกรมที่สามารถแพร่เชื้อสู่โปรแกรมอื่น ๆ ได้โดยการดัดแปลงให้รวมสำเนาของตัวมันเอง" Cohen สาธิตโปรแกรมคล้ายไวรัสบนระบบ VAX11/750 ที่มหาวิทยาลัย Lehigh ซึ่งสามารถติดตั้งตัวเองหรือแพร่เชื้อสู่ระบบอื่น ๆ ได้

- 1984 Ken Thompson ตีพิมพ์เอกสารสำคัญของเขาชื่อ Reflections on Trusting Trust ซึ่งอธิบายถึงวิธีที่เขาแก้ไขคอมไพเลอร์ภาษา C เพื่อใช้คอมไพล์ระบบปฏิบัติการ Unix เวอร์ชันพิเศษ ที่จะมีประตูลับในคำสั่งล็อกอิน

- 1986 ไวรัส Brain อาศัยการซ่อนตัวใน boot sector ถือเป็นไวรัสบน IBM PC compatible ตัวแรก ถูกสร้างขึ้นในประเทศปากีสถานโดยโปรแกรมเมอร์ชาวปากีสถานวัย 19 ปี

- 1987 เริ่มพบไวรัสที่ติดเชื้อทางไฟล์โปรแกรม

1. ไวรัส Veinna ไวรัส Lehigh และไวรัส Cascade ซึ่งเป็นไวรัสที่ติดเชื้อทางไฟล์แบบเข้ารหัสตัวแรก (แพร่สู่สำนักงานของ IBM ทำให้ IBM ออกผลิตภัณฑ์ป้องกันไวรัสของตัวเอง)

2. ไวรัส Jerusalem ทำลายทุกไฟล์ที่มีนามสกุล .EXE ทุกวันศุกร์ที่ 13

3. ไวรัส SCA และ Byte Bandit บนเครื่อง Amiga

4. Christmas Tree EXEC เป็นมัลแวร์ที่สำเนาตัวเองผ่านเครือข่ายเป็นวงกว้างตัวแรก

- 1988 Morris worm สร้างโดย Robert Tappan Morris ติดเชื้อสู่เครื่อง DEC VAX และเครื่อง Sun ที่ใช้ BSD UNIX ที่เชื่อมต่อกับอินเทอร์เน็ตและกลายเป็น worm ตัวแรกที่แพร่กระจายอย่างกว้างขวาง และเป็นหนึ่งในโปรแกรมที่รู้จักกันดีโปรแกรมแรกที่อาศัยช่องโหว่ buffer overrun

- 1989 ฟล็อปปี้ดิสก์หลายพันแผ่นที่มีโทรจัน AIDS ซึ่งถือเป็น ransomware ตัวแรกจะถูกส่งไปยังสมาชิกของนิตยสาร PC Business World และผู้เข้าร่วมประชุม WHO AIDS โทรจันบน DOS ตัวนี้เมื่อติดแล้วจะไม่ทำงานจนเมื่อระบบผ่านการบูตไป 90 รอบ จากนั้นจะเข้ารหัสเฉพาะชื่อไฟล์ทั้งหมดในระบบแล้วแสดงประกาศขอเงิน 189 ดอลลาร์ส่งไปยังตู้ไปรษณีย์ในปานามาเพื่อรับโปรแกรมถอดรหัส

ค.ศ. 1990–1999

- 1990 เกิด Polymorphic Virus ตัวแรกชื่อ “The Chameleon family”

- 1993 Leandro แพร่กระจายผ่าน BBS และ shareware

- 1994 OneHalf เป็น polymorphic computer virus บน DOS ตัวแรก ๆ ที่ใช้เทคนิค “patchy infection”

- 1995 Macro virus ตัวแรกชื่อ “Concept” ถูกสร้างขึ้นเพื่อติดเชื้อผ่านไฟล์เอกสาร Microsoft Word

- 1996 Boza ไวรัสตัวแรกที่ออกแบบมาเฉพาะสำหรับไฟล์บน Windows 95 Laroux Excel macro virus ตัวแรก และ Staog ไวรัสบนระบบปฏิบัติการ Linux ตัวแรก

- 1998 ไวรัส CIH เป็นไวรัสตัวแรกที่สามารถลบข้อมูลโดยแฟลช ROM BIOS ได้

- 1999 เกิดอีเมลไวรัสที่เรียกว่า Happy99 และ Melissa Worm

ค.ศ. 2000–2009

- 2000 ILOVEYOU worm (Love Letter หรือ Love Bug) ถูกเขียนด้วย VB Script เขียนทับไฟล์แบบสุ่มบนระบบจากนั้นจะส่งต่อตัวเองไปยังอีเมลทั้งหมดในรายชื่อผู้ติดต่อ สร้างโดยชาวฟิลิปปินส์ คาดว่าน่าจะสร้างความเสียหายถึง 5.5-8.7 พันล้านเหรียญสหรัฐ

- 2001 มีการระบาดของเวิร์ม (worm) Code Red ที่โจมตี Index Server ISAPI Extension ในซอฟต์แวร์แม่ข่ายเว็บของไมโครซอฟต์ (Microsoft Internet Information Services) และพัฒนาต่อเป็น Code Red II ซึ่งมีการสร้างประตูลับทิ้งไว้และถูกใช้โดย Nimda worm ในเวลาต่อมา

- 2002 เกิด Simile virus เป็น metamorphic computer virus (กลายพันธุ์โดยการเปลี่ยนโค้ดโปรแกรมของตัวเองเพื่อเลี่ยงการตรวจจับ) ถูกเขียนด้วยภาษาแอสเซมบลีและม้าโทรจัน Beast บน Windows หรือที่เรียกกันทั่วไปว่า RAT--Remote Administration Tool

- 2003 เวิร์ม SQL Slammer โจมตีช่องโหว่ใน Microsoft SQL Server และ MSDE กลายเป็นเวิร์มที่แพร่กระจายเร็วที่สุดตลอดกาล ทำให้อินเทอร์เน็ตหยุดชะงักทั่วโลกเพียงสิบห้านาทีหลังจากแพร่เชื้อเหยื่อรายแรก ตามด้วยเวิร์ม Blaster Welchia Sobig Sober Agobot ฯลฯ ที่ล้วนแต่โจมตีช่องโหว่ของวินโดวส์

- 2004 เกิดเวิร์ม Witty Sasser Rugrat Rugrat.B Nuclear และ Bifrost ซึ่งล้วนแต่เป็นเวิร์มที่โจมตีช่องโหว่ของวินโดวส์ และยังเกิดเวิร์ม Santy ซึ่งเป็น webworm ตัวแรก โดยใช้ช่องโหว่ใน phpBB และใช้ Google เพื่อค้นหาเป้าหมายใหม่

- 2007 เป็นปีแห่ง botnet ซึ่งเป็นอุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ตจำนวนมากที่โปรแกรม bot อยู่ เกิด Storm worm ที่เป็นจุดเริ่มต้นของ Storm botnet และ Zeus ซึ่งเป็นโทรจันที่ขโมยข้อมูลธนาคารโดยใช้การแอบบันทึกการกดแป้นพิมพ์ (keylogger) และยังเป็น botnet ด้วย

- 2008 เกิด Koobface worm มีเป้าหมายที่ผู้ใช้ Facebook และ Myspace และยังเกิด Conficker worm ที่ใช้เทคนิคใหม่ๆ มาโจมตี Windows 2000 ถึง Windows 7

ค.ศ. 2010–ปัจจุบัน

- 2010 มีการตรวจพบ Stuxnet ซึ่งเป็น Windows Trojan ตัวแรกที่โจมตีระบบสกาดา (SCADA) และเชื่อกันว่าได้รับการออกแบบมาเพื่อมุ่งเป้าหมายที่โรงงานนิวเคลียร์ของอิหร่าน ในตัวมันยังพบว่ามีลายเซ็นดิจิทัลจากใบรับรองที่ถูกต้องอีกด้วย

- 2013 เกิด CryptoLocker มัลแวร์ที่เป็นต้นแบบของแรนซัมแวร์ยุคใหม่

จากประวัติที่กล่าวมาจะเห็นพัฒนาการที่สำคัญของมัลแวร์ในรอบหลายปีที่ผ่านมา เช่น มีการเปลี่ยนรูปแบบจาก ไวรัสเป็นโทรจันและเวิร์ม ใช้เทคนิคใหม่ ๆ เพื่อหลบเลี่ยงการถูกตรวจจับ เช่น Polymorphic หรือ Metamorphic และเปลี่ยนรูปแบบการแพร่กระจายไปเรื่อย ๆ ตามเทคโนโลยี เช่น จากไฟล์เป็นอีเมล เครือข่าย และเว็บเป็นต้น

ต้นกำเนิดของแรนซัมแวร์ยุคใหม่

ในปีค.ศ. 1996 Adam L. Young และ Yung (Young & Yung, 1996) ได้บัญญัติคำว่า cryptovirology เพื่อแสดงถึงการใช้การเข้ารหัสเป็นอาวุธโจมตีผ่านไวรัสคอมพิวเตอร์และมัลแวร์อื่น ๆ ซึ่งตรงกันข้ามกับบทบาทของการเข้ารหัสแบบดั้งเดิมที่มักใช้เป็นเครื่องมือในการป้องกันสารสนเทศ (Whitman & Mattord, 2018) โดยเฉพาะอย่างยิ่งพวกเขาได้สาธิตต้นแบบของแรนซัมแวร์ที่ใช้การเข้ารหัสแบบ Public-key cryptography โดยสรุปขั้นตอนการทำงานตามภาพ 1 ดังนี้

1. แฮกเกอร์ทำการสร้าง public กับ private key คู่กันขึ้น

2. เอา public key ที่สร้างขึ้นแนบไปกับมัลแวร์และแพร่มัลแวร์สู่เหยื่อ

3. เมื่อเหยื่อติดมัลแวร์มันจะสร้าง symmetric key เดี่ยวขึ้นมา

4. นำ symmetric key นั้นมาเข้ารหัสไฟล์ของเหยื่อ

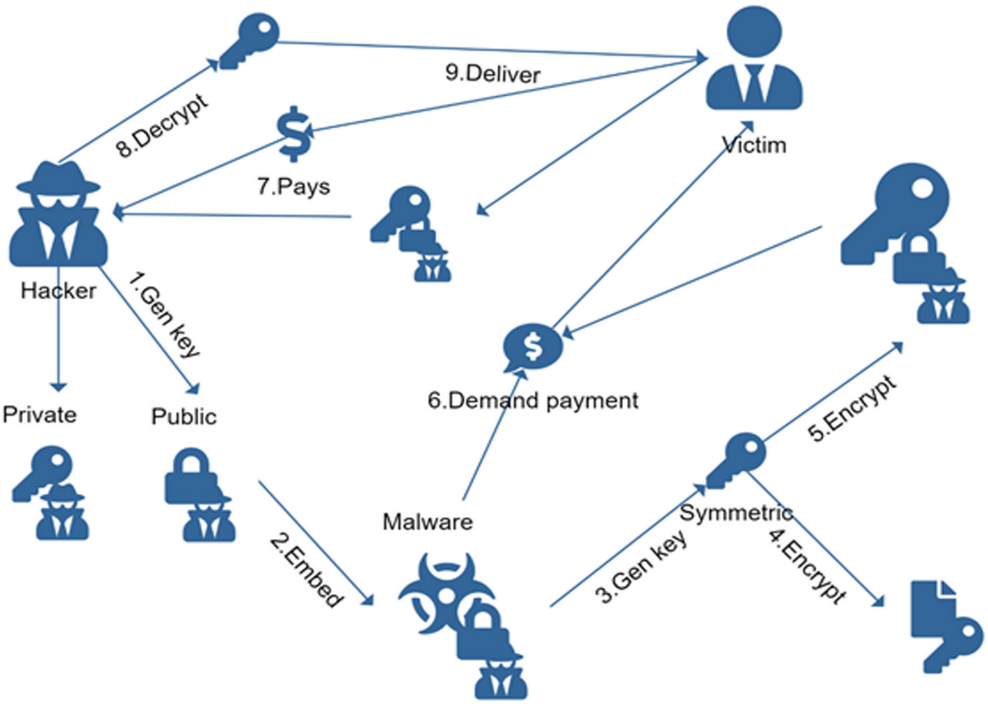
5. เข้ารหัส symmetric key ที่ใช้เข้ารหัสไฟล์ของเหยื่อด้วย public key ของแฮกเกอร์ที่แนบมากับตัวมัลแวร์

6. แจ้งข้อความเรียกค่าไถ่ให้เหยื่อส่งเงินและ symmetric key ที่ถูกเข้ารหัสกลับไปหาแฮกเกอร์

7. หากเหยื่อส่งค่าไถ่และ symmetric key ที่ถูกเข้ารหัสกลับไปหาแฮกเกอร์

8. แฮกเกอร์จะถอดรหัส symmetric key ที่ถูกเข้ารหัสด้วย private key จากขั้นตอนแรก

9. ส่ง symmetric key ที่ถอดรหัสแล้วกลับไปให้เหยื่อใช้ถอดรหัสไฟล์ของตน



ภาพ 1 ต้นแบบของแรนซัมแวร์ที่ใช้การเข้ารหัสแบบ Public-key cryptography

แม้ว่าแนวคิดนี้จะถูกนำเสนอตั้งแต่ปีค.ศ. 1996 แต่ด้วยข้อจำกัดด้านการจ่ายเงินในช่วงเวลานั้นที่ยังไม่มีวิธีจ่ายเงินที่สะดวกแพร่หลายเพียงพอที่จะให้จ่ายจากที่ไหนในโลกก็ได้ และการจ่ายเงินค่าไถ่นั้นยากที่จะทำการปกปิดผู้รับจนไม่อาจตามรอยเพื่อดำเนินคดีได้ ทำให้แรนซัมแวร์ยุคนั้นยังไม่ประสบความสำเร็จมากนัก จนกระทั่งในปีค.ศ. 2009 เริ่มมีการใช้บิตคอยน์ซึ่งเป็นเงินตราแบบดิจิทัล (cryptocurrency) ซึ่งต่อมากลายเป็นระบบการชำระเงินที่ใช้กันแพร่หลายทั่วโลกและยังตามรอยได้ยากด้วย

แรนซัมแวร์ CryptoLocker

แรนซัมแวร์ CryptoLocker ถูกพบในเดือนกันยายน ค.ศ. 2013 มุ่งเป้าโจมตีระบบที่ใช้วินโดวส์ แพร่กระจายผ่านการแนบไปกับอีเมลและ botnets (ZeuS) เมื่อติดที่เครื่องเหยื่อจะมีขั้นตอนการทำงานตามภาพ 2 ดังนี้

1. แก้ไข registry ของวินโดวส์ เพื่อให้ถูกรันทุกครั้งที่เครื่องบูทใหม่ และจะทำการสร้างไอดีเพื่อแยกแยะเหยื่อที่ติดเชื้อ

2. เชื่อมต่อกลับไปหาเครื่องแม่ข่ายของแฮกเกอร์เพื่อส่งไอดีของเหยื่อ

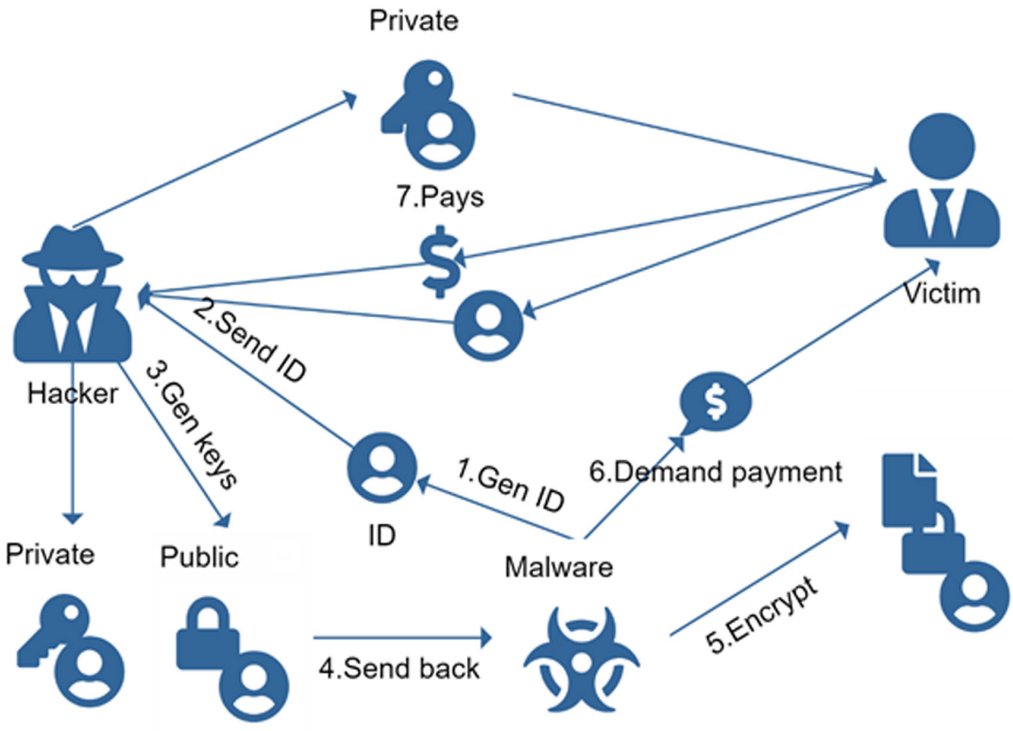
3. แฮกเกอร์จะทำการสร้าง public และ private key สำหรับเหยื่อแต่ละราย

4. ทำการส่ง public key กลับไปให้ CryptoLocker ที่เครื่องเหยื่อ

5. CryptoLocker ที่เครื่องเหยื่อจะเอา public key ที่ได้มาเข้ารหัสไฟล์ต่าง ๆ ของเหยื่อ

6. แจ้งข้อความเรียกค่าไถ่ให้เหยื่อส่งเงินไอดีของเหยื่อกลับไปหาแฮกเกอร์

7. เมื่อได้ค่าไถ่แล้ว แฮกเกอร์จะส่ง private key ของเหยื่อเพื่อให้ใช้ถอดรหัสไฟล์ที่โดนเข้ารหัสด้วย public key ของเหยื่อที่สร้างมาคู่กัน



ภาพ 2 ขั้นตอนการทำงานของ CryptoLocker

จะเห็นได้ว่าขั้นตอนวิธีเข้ารหัสของ CryptoLocker เมื่อเทียบกับของ Young และ Yung (Young & Yung, 1996) ยังมีข้อด้อยกว่าตรงที่ใช้ public key มาเข้ารหัสแทน ซึ่งจะทำงานได้ช้ากว่าการใช้ symmetric key ทำให้ต้องใช้เวลานานกว่าจะเข้ารหัสไฟล์ของเหยื่อได้หมด จึงมีโอกาสที่เหยื่อจะรู้ตัวได้ก่อนและอาจหยุดความเสียหายจากการโดนเข้ารหัสไฟล์ทั้งหมดได้ทันจนไม่จำเป็นต้องจ่ายค่าไถ่

แรนซัมแวร์ WannaCry

แรนซัมแวร์ WannaCry ถูกพบในเดือนพฤษภาคม ค.ศ. 2017 อาจถูกจัดว่าเป็นเวิร์มเพราะมุ่งโจมตีระบบที่ใช้วินโดวส์ โดยแพร่ผ่านการโจมตีแบบ EternalBlue ซึ่งคิดค้นโดยสำนักงานความมั่นคงแห่งชาติ (National Security Agency) ของประเทศสหรัฐอเมริกา ที่อาศัยช่องโหว่ซึ่งไมโครซอฟท์ได้ออกตัวแก้ไขมาก่อนการระบาดแล้ว แต่องค์การจำนวนมากก็ไม่สามารถแก้ไขช่องโหว่นั้นได้ทัน มีการประมาณการว่ามีจำนวนเครื่องที่ถูกโจมตีด้วย WannaCry มากกว่าสองแสนเครื่องใน 150 ประเทศ

แรนซัมแวร์ WannaCry มีขั้นตอนการทำงานตามภาพ 3 ดังต่อไปนี้

1. แฮกเกอร์ทำการสร้าง public กับ private key คู่กันขึ้น

2. เอา public key ที่สร้างขึ้นแนบไปกับมัลแวร์และแพร่มัลแวร์สู่เหยื่อ

3. เมื่อเหยื่อติดมัลแวร์มันจะสร้าง public และ private key สำหรับเหยื่อแต่ละรายขึ้นมา

4. เข้ารหัส private key ของเหยื่อด้วย public key ของแฮกเกอร์ที่แนบมากับมัลแวร์

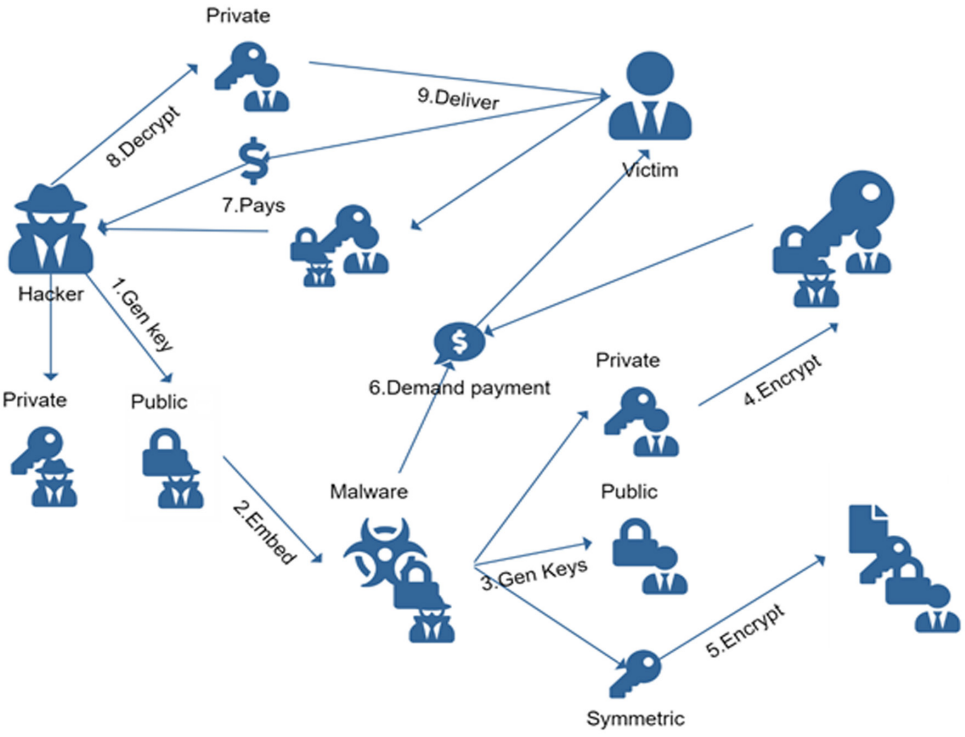
5. สร้าง symmetric key ขึ้นมาใหม่ทุกครั้งเพื่อเข้ารหัสเฉพาะแต่ละไฟล์ของเหยื่อ แล้วเข้ารหัส symmetric key นั้นด้วย public key ของเหยื่อ

6. แจ้งข้อความเรียกค่าไถ่ให้เหยื่อส่งเงินและ private key ของเหยื่อที่ถูกเข้ารหัสกลับไปหาแฮกเกอร์

7. หากเหยื่อส่งค่าไถ่และ private key ของเหยื่อที่ถูกเข้ารหัสกลับไปหาแฮกเกอร์

8. แฮกเกอร์ถอดรหัส private key ของเหยื่อที่ถูกเข้ารหัสด้วย private key ของแฮกเกอร์จากขั้นตอนแรก

9. ส่ง private key ของเหยื่อที่ถอดรหัสแล้วกลับไปให้เหยื่อใช้ถอดรหัส symmetric key แต่ละอันเพื่อถอดรหัสไฟล์ของตน



ภาพ 3 ขั้นตอนการทำงานของ WannaCry

จากภาพ 3 จะเห็นว่า นอกจากขั้นตอนการทำงานงานเป็นไปตามที่ Young และ Yung เสนอไว้แล้ว ยังมีการปรับปรุงให้ดีขึ้นโดยแทนที่จะใช้ symmetric key เพียงตัวเดียวเข้ารหัสไฟล์จำนวนมากของเหยื่อทั้งหมด key นั้นอาจจะถูกตรวจพบได้ในหน่วยความจำหลักในระหว่างที่การเข้ารหัสยังไม่เสร็จสิ้น ทำให้เอามาถอดรหัสไฟล์คืนได้โดยไม่ต้องจ่ายค่าไถ่ แต่ WannaCry ใช้วิธีสร้าง symmetric key ขึ้นใหม่เฉพาะแต่ละไฟล์ เมื่อเข้ารหัสแต่ไฟล์เสร็จแล้ว key ของแต่ละไฟล์จะถูกเข้ารหัสด้วย public key ที่ถูกสร้างขึ้นใหม่สำหรับเหยื่อแต่ละราย และเข้ารหัส private key ที่ใช้ถอดรหัสคู่กันทันทีด้วย public key ของแฮกเกอร์ที่แนบมากับตัว WannaCry จะเห็นได้ว่าไม่มี key ที่ใช้ถอดรหัสตัวใด ๆ คงค้างอยู่ในเครื่องเหยื่อเป็นเวลานานโดยไม่ถูกเข้ารหัส ทำให้ลดความเสี่ยงที่จะถูกตรวจพบ key ที่จะใช้ถอดรหัสได้ก่อนที่จะเข้ารหัสไฟล์ทั้งหมดเสร็จ

อย่างไรก็ตาม เนื่องจาก WannaCry เรียกใช้ library ของวินโดวส์ซึ่งบังเอิญมีข้อผิดพลาดในการสร้าง public และ private ของเหยื่อ ทำให้สามารถสร้าง private key ของเหยื่อขึ้นมาใหม่จากข้อมูลในหน่วยความจำที่หลงเหลืออยู่ได้แม้ key นั้นจะถูกเข้ารหัสไปแล้วถ้ายังไม่บูทเครื่องใหม่ ทำให้มีผู้ที่อาศัยข้อผิดพลาดนี้พัฒนาเครื่องมือสำหรับถอดรหัสไฟล์ที่ถูกเข้ารหัสโดย WannaCry ออกมาได้โดยไม่ต้องจ่ายค่าไถ่

นอกจากนั้น WannaCry ยังแนบที่อยู่ในการจ่ายค่าไถ่ด้วยบิตคอยน์มาแค่สามที่อยู่ ทำให้การตรวจสอบว่าเหยื่อคนไหนยอมจ่ายเพื่อจะได้ถอดรหัส key คืนมาให้อาจทำได้ล่าช้าหากมีการจ่ายค่าไถ่เข้ามาจำนวนมาก ส่งผลต่อความเชื่อมั่นของเหยื่อรายใหม่ว่าจะได้ไฟล์คืนหรือไม่หากยอมจ่ายค่าไถ่ ถึงกระนั้นจากการตรวจสอบที่อยู่ทั้งสามพบว่า มีการจ่ายเงินรวมถึงกว่าสามร้อยธุรกรรม เป็นเงินประมาณ 50 BTC หรือประมาณสี่ล้านห้าแสนบาทในเวลาแค่หนึ่งเดือน

แรนซัมแวร์แบบใช้คนสั่งการ (human-operated ransomware)

พฤติกรรมการโจมตีของแรนซัมแวร์แบบใช้คนสั่งการ (human-operated ransomware) นั้นจะแตกต่างจากแรนซัมแวร์แบบแพร่กระจายอัตโนมัติ (auto-spreading ransomware) อย่าง WannaCry โดยรูปแบบจะใกล้เคียงกับการโจมตีประเภทมีเป้าหมาย (targeted attack) จากแฮกเกอร์ของรัฐ (nation-state actors) ซึ่งผู้โจมตีจะมุ่งเป้าไปที่องค์กรขนาดใหญ่โดยจะเข้ามารวบรวมข้อมูลของระบบก่อน จากนั้นค่อยขยายไปยังเครื่องอื่น ๆ ในเครือข่าย สร้างช่องทางเชื่อมต่อทิ้งไว้ แล้วสุดท้ายค่อยสั่งติดตั้งแรนซัมแวร์ ทั้งนี้นอกจากผู้โจมตีจะเจาะระบบเข้ามาเพื่อแพร่กระจายแรนซัมแวร์แล้วอาจมีการโจมตีอย่างอื่นเพิ่มเติมด้วย เช่น ขโมยข้อมูลสำหรับยืนยันตัวตน ขโมยข้อมูลความลับทางการค้า หรือข้อมูลของลูกค้าเพื่อเรียกค่าไถ่ (Microsoft, 2020a) ถ้าหากไม่ยอมจ่ายข้อมูลเหล่านี้ก็จะถูกเผยแพร่สู่สาธารณะซึ่งนอกจากจะทำให้องค์กรเสียชื่อเสียงแล้ว ยังอาจถูกลูกค้าฟ้องร้องเรียกค่าเสียหายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกด้วย (Pokudom, 2020)

Maze เป็นตัวอย่างหนึ่งของแรนซัมแวร์แบบใช้คนสั่งการที่สร้างความเสียหายให้องค์กรชั้นนำต่าง ๆ ในระดับโลกรวมถึงรัฐวิสาหกิจและองค์กรธุรกิจขนาดใหญ่ของประเทศไทย ไมโครซอฟท์ (Microsoft, 2020b) ได้อธิบายพฤติกรรมของ Maze สามารถสรุปโดยสังเขปได้ดังนี้

- นอกจากการแพร่กระจายทางอีเมลแล้ว Maze มักจะเข้าถึงระบบที่มีความเสี่ยงด้วยการโจมตีผ่านการเดารหัสผ่านบริการควบคุมระยะไกล (remote desktop) ซึ่งตั้งค่าไว้อย่างไม่ปลอดภัย ในขณะที่มัลแวร์กลุ่มอื่นมีการโจมตีช่องโหว่ซึ่งเป็นที่มีการเปิดเผยมาก่อนแล้ว อาทิ ช่องโหว่ใน Citrix Application Delivery Controller (CVE-2019-19781) ที่จะช่วยอำนวยความสะดวกในการเข้าถึงทุก Application หรือช่องโหว่ใน VPN ของบริษัท Pulse Secure (CVE-2019-11510) และยังมีการระบุว่าเป้าหมายหลักของ Maze คือ การโจมตีกลุ่มผู้ให้บริการ (managed service provider) เพื่อใช้เป็นช่องทางในการเข้าถึงผู้ใช้บริการในกลุ่มธุรกิจนี้ด้วย

- Maze ใช้โปรแกรม Mimikatz ในการระบุหาข้อมูลสำหรับยืนยันตัวตนในระบบ ข้อมูลสำหรับยืนยันตัวตนนี้จะถูกใช้เพื่อเข้าถึงระบบอื่น ๆ

- กระบวนการเคลื่อนย้ายตัวเองในระบบภายในขององค์กรมักเกิดขึ้นผ่านการใช้โปรแกรม Cobalt Strike ซึ่งเป็นเครื่องมือสำหรับการทดสอบเจาะระบบ ทั้งนี้เทคนิคและวิธีการที่ Cobalt Strike รองรับนั้นโดยส่วนใหญ่เป็นเทคนิคซึ่งเป็นที่รู้จักกันอยู่แล้ว อาทิ การโจมตีแบบ Pass-the-Hash, WinRM หรือการใช้ PsExec ในการเข้าถึงด้วยข้อมูลสำหรับยืนยันตัวตนที่ได้มา

- กระบวนการฝังตัวของ Maze มีการปรากฏการใช้ Task Scheduler ร่วมกับการใช้คำสั่ง PowerShell ซึ่งทำให้ผู้โจมตีสามารถเข้าถึงระบบที่ถูกโจมตีไปแล้วได้ Maze ยังมีการใช้ฟีเจอร์ WinRM ในการควบคุมระบบเมื่อได้บัญชีซึ่งมีสิทธิ์ของผู้ดูแลโดเมน (Domain admin) ด้วย

- Maze มีการแก้ไขการตั้งค่าใน Group Policy หลายรายการเพื่อช่วยอำนวยความสะดวกในการโจมตี

การโจมตีเพื่อติดตั้งแรนซัมแวร์ในกรณีที่ใช้คนเป็นผู้สั่งการมักจะมีลักษณะคล้าย ๆ กัน คือ ผู้โจมตีจะเข้ามาอยู่ในระบบเพื่อรวบรวมข้อมูลรวมถึงสร้างช่องทางเพื่อให้สามารถกลับเข้ามาโจมตีซ้ำได้อีก ดังนั้นถึงแม้จะมีการจ่ายเงินค่าไถ่ (ซึ่งก็อาจไม่สามารถรับประกันว่าจะได้ข้อมูลกลับคืนจริง ๆ) หรือการกู้คืนระบบจากข้อมูล สำรอง หากไม่มีกระบวนการตรวจสอบ แก้ไขช่องโหว่ และกำจัดช่องทางที่ผู้โจมตีได้สร้างไว้ ก็มีสิทธิ์ที่จะติดแรนซัมแวร์ซ้ำได้อีกเรื่อย ๆ ยังไม่รวมปัญหาข้อมูลถูกขโมยซึ่งอาจส่งผลกระทบได้ไม่น้อยไปกว่าปัญหาแรนซัมแวร์ ซึ่งสามารถสรุปรูปแบบการโจมตีได้ ดังนี้

- ช่องทางการโจมตีส่วนใหญ่มักอาศัยข้อผิดพลาดของการตั้งค่าระบบ เช่น เปิดให้เชื่อมต่อ Remote Desktop--RDP ได้ผ่านอินเทอร์เน็ต หรือตั้งรหัสผ่านผู้ดูแลระบบที่สามารถคาดเดาได้ง่าย โจมตีช่องโหว่ที่มีแพตช์หรือซอฟต์แวร์ที่แก้ไขข้อผิดพลาดแล้วแต่ยังไม่ได้ติดตั้ง หรือมีเครื่องมือด้านความมั่นคงปลอดภัยอยู่แล้วแต่ไม่ได้ถูกเปิดใช้งาน

- ช่องทางแรกสุดของการโจมตีโดยมากมาจากมัลแวร์ที่สามารถรวบรวมข้อมูลสำหรับยืนยันตัวตน หรือข้อมูลของระบบเครือข่ายได้ ซึ่งข้อมูลเหล่านี้จะถูกใช้ขยายขอบเขตต่อไปยังเครื่องอื่นในเครือข่ายเพื่อแพร่กระจายแรนซัมแวร์ในภายหลัง

- หลังจากที่โจมตีสำเร็จแล้ว หากไม่มีกระบวนการแก้ไขปัญหาที่ดีพอก็มีโอกาสที่จะถูกโจมตีซ้ำอีกได้เรื่อย ๆ การมุ่งความสนใจแค่เรื่องของการกู้คืนระบบจากแรนซัมแวร์เพียงอย่างเดียวนั้นไม่เพียงพอ จำเป็นต้องค้นหาสาเหตุและกำจัดช่องทางการเชื่อมต่อที่ถูกสร้างไว้ด้วย

จากรูปแบบการโจมตีข้างต้นสามารถสรุปข้อแนะนำในการป้องกันได้ ดังนี้

- ระบบใด ๆ ที่เปิดให้สามารถเข้าถึงได้จากอินเทอร์เน็ตจำเป็นต้องได้รับการป้องกันและเฝ้าระวังการโจมตีเป็นพิเศษ

- ควรเปิดใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (multi-factor authentication) หรือให้ผู้ใช้ยืนยันตัวตนก่อนเชื่อมต่อ (network-level authentication) เพื่อลดผลกระทบจากกรณีรหัสผ่านถูกขโมย

- ใช้หลักการการให้สิทธิ์เฉพาะที่จำเป็นต้องใช้เท่านั้น (least-privilege) เพื่อป้องกันไม่ให้มีบัญชีที่มีสิทธิ์ระดับสูงโดยไม่จำเป็น

- เฝ้าระวังการโจมตีแบบ brute force (Windows Event ID 4625)

- เฝ้าระวังการเคลียร์ Windows Security Log (Windows Event ID 1102) หรือการรัน PowerShell

- เฝ้าระวังการล็อกอินโดยใช้บัญชีของผู้ดูแลระบบ (Window Event ID 4624) โดยเฉพาะอย่างยิ่งบัญชีของผู้ดูแลโดเมน (domain admin) ซึ่งบัญชีดังกล่าวไม่ควรถูกนำมาล็อกอินบนเครื่องของผู้ใช้ทั่วไป

- ใช้ Windows Defender ATP ซึ่งจะมีการแจ้งเตือนการรันโปรแกรมหรือคำสั่งที่น่าสงสัย เช่น PsExec WMI หรือ Office macro

บทสรุป

แรนซัมแวร์เป็นมัลแวร์ที่มีการพัฒนาด้วยเทคโนโลยีขั้นสูงขึ้น เนื่องจากมันได้กลายเป็นช่องทางหนึ่งในการหารายได้ให้กับแฮกเกอร์ จากการโจมตีเหยื่อเป็นรายบุคคล เปลี่ยนมาเป็นการโจมตีเป้าหมายระดับองค์การโดยใช้รูปแบบที่ซับซ้อนขึ้นเพราะมีโอกาสที่จะได้ผลประโยชน์ที่มากขึ้น อย่างไรก็ตาม จากข้อแนะนำในบทความนี้ก็อาจใช้เป็นแนวทางป้องกันหรือลดความเสียหายจากการโจมตีของแรนซัมแวร์ลงได้

References

Microsoft. (2020 a). *Human-operated ransomware attacks: A preventable disaster*. Retrieved from https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Microsoft. (2020 b). *Ransomware groups continue to target healthcare, critical services; here's how to reduce risk*. Retrieved from https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

Pokudom, N. (2020). Data privacy in the digital age. *EAU Heritage Journal Science and Technology, 14*(2), 59-69. (in Thai).

Spadafora, A. (2020). *FBI: Over $140 million handed over to ransomware attackers*. Retrieved from https://www.techradar.com/news/fbi-over-dollar140-million-handed-over-to-ransomware-attackers

Vanderlee, K. (2020). *They come in the night: Ransomware deployment trends*. Retrieved from https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security*. Boston: Cengage Learning.

Wikipedia. (2020). *Timeline of computer viruses and worms*. Retrieved from https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

Young , A. L., & Yung, M. (1996). Cryptovirology: Extortion-based security threats and countermeasures. *IEEE Symposium on Security & Privacy* (pp. 129–141). Oakland: IEEE.