แนวทางการรับมือและการรับแจ้งเหตุของตำรวจต่อกรณีมัลแวร์เรียกค่าไถ่

อัศว์ณุต แสงทองดี[1]
ญาณพล ยั่งยืน[2]

บทคัดย่อ

มัลแวร์เรียกค่าไถ่เป็นเครื่องมือของคนร้ายไซเบอร์ที่ต้องการขู่กรรโชกทรัพย์เพื่อให้ได้ผลประโยชน์ที่เป็นตัวเงิน แฮกเกอร์สร้างซอฟท์แวร์ประสงค์ร้ายโดยอาศัยเทคโนโลยีรหัสลับผสมผสานกับเทคนิควิธีวิศวกรรมซอฟท์แวร์ วันนาครายและเพทย่าเป็นมัลแวร์ที่สร้างความเสียหายทั่วโลกในช่วงหลายปีที่ผ่านมา มัลแวร์สเปดเพิ่งถูกตรวจพบเมื่อไม่มานานนี้และได้สร้างความเสียหายให้กับโรงพยาบาลสระบุรี สิ่งสำคัญอันดับแรกของการรับมือกับภัยคุกคามเช่นนี้คือการปฏิเสธการจ่ายเงินและเจรจาต่อรองกับคนร้ายทุกช่องทาง โครงการยกเลิกค่าไถ่เป็นทางเลือกหนึ่งให้เหยื่อได้รับคำแนะนำและเครื่องมือถอดถอนมัลแวร์ วันนาคราย เพทย่าและสเปดยังคงถูกจัดอยู่ในกลุ่มภัยคุกคามที่น่าจับตาช่วงทศวรรษนี้ การรับมือเชิงรุกด้วยการปฏิเสธการจ่ายเงินเป็นสิ่งที่ผู้เชี่ยวชาญแนะนำ ตลอดจนการตัดการเชื่อมต่อทันทีเมื่อเกิดเหตุเพื่อลดการแพร่ระบาดในวงกว้าง ส่วนการรับมือเชิงตั้งรับคือการสำรองข้อมูลและปรับปรุงซอฟท์แวร์ระบบปฏิบัติการและโปรแกรมป้องกันไวรัสเป็นประจำ ช่องทางรับแจ้งเหตุร้ายไซเบอร์เป็นที่สิ่งตำรวจทุกประเทศต้องให้ความสำคัญ การเชื่อมโยงข้อมูลจากเหยื่อในฐานะผู้แจ้งเป็นประโยชน์อย่างยิ่งต่อการสืบสวนเพื่อรวบรวมพยานหลักฐานนำไปสู่การพิสูจน์การกระทำผิดของคนร้าย

คำสำคัญ: มัลแวร์เรียกค่าไถ่, วันนาคราย, เพทย่า, วอยด์คริปท์และสเปด, ระบบรับแจ้งเหตุของตำรวจ

[1] คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
[2] สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

Guidelines of Countermeasures and Police Reporting for Ransomware Cases

Usanut Sangtongdee[1]
Yanaphon Youngyuen[2]

Abstract

Cybercriminals apply ransomware for extortion with an ability in locking data assets for monetary purposes. Hackers create malicious software based on cryptographic technologies combined with software engineering techniques. WannaCry and Petya are malware that has damaged vast numbers of computer machines around the world over the years. Spade ransomware has recently defined as an infectious attack at the Saraburi Hospital. The priority in dealing with these extortion threats is denying payments and stopping a negotiation with criminals at all stages. No More Ransom project is an initiative to provide victims with advice and decryption tools. WannaCry, Petya and Spade remain among the top cyber threats this decade. Dealing with aggressive denial of payment is what the experts recommend. Terminating immediately when the incident occurs should also be put in place to reduce the widespread infection. A defensive response is to regularly back up and update operating systems and antivirus programs. Channels for filing a crime report are a top priority for all police countries. Connecting information from a victim as an informant is vital in an investigation to obtain intelligence, leading to the culprit.

Keywords: Ransomware, WannaCry, Petya, VoidCrypt and Spade, police report service

[1] Faculty of Forensic Science, Royal Police Cadet Academy (RPCA)

[2] Thailand Information Security Association (TISA)

1. บทนำ

การบริโภคข้อมูลดิจิทัลผ่านระบบเทคโนโลยีสารสนเทศในปัจจุบันได้รับความนิยมทั้งผ่านโทรศัพท์มือถือและคอมพิวเตอร์ แต่ความกังวลต่อการต่อการถูกบุกรุกและยึดครองเครื่องเพื่อหาผลประโยชน์จากช่องโหว่ทีเกิดขึ้นมีมากขึ้นเช่นกัน มัลแวร์เรียกค่าไถ่ (ransomware) ยังคงได้รับความนิยมของผู้ไม่หวังดีใช้โจมตีผ่านทางเครือข่ายระบบคอมพิวเตอร์ ส่วนหนึ่งเกิดจากความนิยมที่เพิ่มขึ้นอย่างต่อเนื่องของการใช้สกุลเงินดิจิทัล ภายหลังซอฟท์แวร์ประสงค์ร้ายหลายประเภทถูกนักพัฒนาเสริมความแข็งแกร่งด้วยเทคโนโลยีการเข้ารหัส โปรแกรมไม่พึงประ สงค์ที่มาพร้อมคำขู่เป็นหนึ่งในตัวเลือกที่ถูกเสริมความสามารถแบบนี้ได้เช่นกัน จุดเด่นการพัฒนาคุณลักษณะสำคัญในระยะหลังได้แก่ การรนับเวลาถอยหลัง การเรียกค่าไถ่เพิ่มขึ้นเมื่อไม่ได้รับการตอบสนอง และการแพร่กระจายความเสียหายด้วยการกระจายไวรัส เหล่านี้ล้วนเป็นส่วนประกอบสำคัญของมัลแวร์แบบนี้สมัยใหม่ที่ทำให้เกิดอุปสรรคการควบคุมความเสียหายเมื่อเกิดการโจมตีขึ้นมาแล้ว

วันนาคราย (WannaCry) เป็นหนึ่งในโปรแกรมประสงค์ร้าย (Malware) ที่สร้างความเสียหายต่อภาคธุรกิจและภาครัฐทั่วโลกให้เกิดความสูญเสียมหาศาล เมื่อปี พ.ศ.2560 ไทยเซิร์ต (ThaiCERT) รายงานจำนวนคอมพิวเตอร์ที่ติดมัลแวร์นี้มีไม่น้อยกว่า 250 เครื่องทั่วประเทศ (Thailand Computer Emergency Response Team, 2018) รูปแบบการโจมตีคือการเข้ารหัสลับข้อมูลที่จัดเก็บในคอมพิวเตอร์เป้าหมาย คนร้ายมีวัตถุประสงค์ข่มขู่ให้จ่ายเงินตามที่ต้องการ หากปฏิเสธหรือเพิกเฉยจะส่งผลให้ผู้ใช้คอมพิวเตอร์เหล่านั้นไม่อาจเข้าใช้งานระบบหรือไฟล์ได้อีกต่อไป แม้ตัวเลขจำนวนคอมพิวเตอร์ที่ติดเชื้อไวรัสนี้จะมีน้อยก็ตาม สิ่งหนึ่งที่สาธารณชนต้องรับรู้ไว้คือการรายงานการถูกโจมตีที่กล่าวมานั้นเป็นการดำเนินงานทางเทคนิค ผู้รายงานต้องลงทะเบียนกับองค์กรไทยเซิร์ตไว้อยู่ก่อนหน้าแล้วและจะมีการตรวจสอบข้อมูลการโจมตีย้อนหลัง ด้วยเหตุนี้ทำให้ปริมาณความเสียหายในภาพรวมของประเทศไทยไม่สอดคล้องกับความเป็นจริง องค์กรภาคธุรกิจและภาครัฐหลายแห่งอาจไม่ได้ตรวจสอบและรายงานไปยังไทยเซิร์ตอย่างต่อเนื่อง

ประเทศไทยติดอันดับหนึ่งในสี่ร่วมกับอินโดนีเซีย ฟิลิปปินส์ และเวียดนาม ซึ่งเป็นสมาชิกของอาเซียนที่ถูกก่อเหตุอาชญากรรมไซเบอร์เกี่ยวกับสกุลเงินดิจิทัล (INTERPOL Global Complex for Innovation, 2020) ด้วยสถานการณ์เช่นนี้ทำให้ภาครัฐและภาคเอกชนต่างตื่นตัวกับภัยคุกคามที่มากับการใช้งานอินเตอร์เน็ต แต่การสืบสวนสอบสวนทางคดีอาญาในกรณีถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่นั้นยังเป็นไปด้วยความยากลำบาก ทั้งนี้ขึ้นอยู่กับชนิดมัลแวร์และความซับซ้อนของการโจมตี ความเสียหายอาจไม่ได้เกี่ยวข้องเงินเพียงเท่านั้น เมื่อเดือนกันยายน พ.ศ.2563 พบว่าคนร้ายฝังไวรัสไปกับโปรแกรมเรียกค่าไถ่อีกครั้งโดยเลือกเป้าหมายเป็นโรงพยาบาลรัฐในจังหวัดสระบุรี ฐานข้อมูลคนไข้จำนวนมหาศาลถูกเข้ารหัสและล็อคข้อมูลพร้อมกับไฟล์สำคัญจำนวนมาก ถูกปกปิดการ

เข้าถึง ตำรวจดำเนินการสืบสวนหาสาเหตุและรวบรวมพยานหลักฐานอย่างเต็มที่ แต่จวบจนปัจจุบันเจ้าหน้าที่ยังไม่สามารถยืนยันตัวคนร้ายและสถานที่ต้นทางที่ใช้ก่อเหตุ

เจ้าของคอมพิวเตอร์ไม่ว่าเป็นองค์กรหรือผู้ใช้ตามบ้านมักเลือกจ่ายเงินค่าไถ่ตามคำขู่ แต่ความเป็นจริงมีโอกาสน้อยมากที่ได้ข้อมูลและสิทธิการควบคุมเครื่องกลับมาเหมือนเดิม เมื่อพิจารณาการรับมือต่อเหตุการณ์นี้ของหน่วยงานในประเทศ ตำรวจระดับท้องถิ่นไม่อาจเริ่มต้นการสืบสวนได้ด้วยตนเองเนื่องจากข้อจำกัดด้านบุคลากรและเครื่องมือ สำนักงานตำรวจแห่งชาติได้มอบหมายให้กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยีเป็นหน่วยงานหลักในการสืบสวน อย่างไรก็ตามข้อจำกัดส่วนหนึ่งของการสืบสวนมัลแวร์เรียกค่าไถ่เกิดจากการจัดวางระบบเครือข่ายคอมพิวเตอร์ขององค์กรที่ไม่ได้รับปรับปรุงและรองรับภัยคุกคามสมัยใหม่ ดังนั้นเมื่อเกิดเหตุขึ้น การเข้ามาแสวงหาหลักฐานเพื่อพิสูจน์การกระทำผิดเป็นไปด้วยความยากลำบาก

ดังนั้น บทความนี้มีวัตถุประสงค์เพื่อศึกษาสถานการณ์ภัยคุกคามออนไลน์ที่มาในรูปแบบโปรแกรมประสงค์ร้ายและการใช้เทคนิคเรียกค่าไถ่จากการปิดกั้นการเข้าถึงข้อมูล นอกจากนั้นแนวทางการปฏิบัติงานด้านการสืบสวนเพื่อแสวงหาหลักฐานจะถูกกล่าวถึง ตลอดจนการสร้างเครือข่ายความร่วมมือระหว่างองค์กรตำรวจและภาคธุรกิจในระดับสากล ส่วนสุดท้ายเป็นข้อเสนอแนะสำหรับรับมือกับการโจมตีแบบเข้ารหัสและส่งเสริมความตระหนักรับรู้ต่อภัยคุกคามออนไลน์ของสังคมไทยยุคดิจิทัล

2. วัตถุประสงค์

เพื่อศึกษาสภาพปัญหาและความรุนแรงของมัลแวร์เรียกค่าไถ่ และนำเสนอแนวทางการรับมือด้วยการรับแจ้งเหตุผ่านระบบการให้บริการของหน่วยงานตำรวจ

3. ทบทวนวรรณกรรม

3.1 โปรแกรมประสงค์ร้าย (Malicious Software)

ในยุคที่สังคมเต็มไปด้วยการทำธุรกรรมผ่านข้อมูลดิจิทัลส่งผลให้คนร้ายอาศัยช่องโหว่ของเครื่องคอมพิวเตอร์ทำการรุกล้ำโดยเจตนาแสวงหาประโยชน์ทางทรัพย์สินของเหยื่อ ชุดคำสั่งคอมพิวเตอร์ที่ถูกสร้างมาเพื่อประโยชน์นอกเหนือจากการใช้งานปกติจึงมักถูกใช้เป็นเครื่องมือในการล้วงข้อมูลของเป้าหมาย มัลแวร์ที่มีชุดคำสั่งประสงค์ร้ายแฝงเอาไว้จะถูกซ่อนเร้นมาซอฟท์แวร์หรือแอพพลิเคชั่นปกติ บางทีคนร้ายใช้เทคนิคปรับแต่งให้ตัวมัลแวร์คล้ายคลึงกับซอฟท์แวร์ที่ถูกต้อง รูปแบบการทำการงานของมัลแวร์คือการแพร่กระจายตัวเองไปยังคอมพิวเตอร์หลายเครื่องให้ครอบคลุมทั้งระบบเครือข่าย บางกรณีมีการควบคุมจากภายนอกให้เข้าถึงการใช้อีเมล์ขององค์กรของเหยื่อในปริมาณมหาศาลโดยหวังให้เกิดความเสียหายของระบบเครือข่าย (Liangboonprakong,

2012) ทั้งนี้รูปแบบการโจมตีทางไซเบอร์ด้วยมัลแวร์ที่ได้รับความนิยมของคนร้าย ได้แก่ จุดช่องโหว่ของโปรแกรม (Backdoor), ม้าโทรจัน (Trojan Horse), โปรแกรมไวรัส (Virus) และหนอน (Worm)

มัลแวร์เรียกค่าไถ่หรือแรนซั่มแวร์เป็นเพียงชื่อเรียกมัลแวร์ชนิดหนึ่งที่ต้องการเน้นคุณสมบัติเฉพาะ สิ่งนั้นคือการข่มขู่เรียกร้องเงินจากเหยื่อโดยตรง สาเหตุที่คนร้ายนิยมใช้โปรแกรมประยุกต์หรือซอฟแวร์แบบนี้คือความสามารถในการกำหนดสิ่งตอบแทนตามต้องการได้อิสระ มัลแวร์ลักษณะแบบนี้ถูกจัดให้อยู่ในภัยคุกคามประเภทการบุกรุก (intrusion) ในอดีตมัลแวร์ชนิดนี้ถูกเขียนโค๊ดโปรแกรมในแบบไฟล์โค๊ดเดอร์ (filecoder) แต่เนื่องจากเทคโนโลยีรหัสลับได้รับการพัฒนาสร้างความแข็งแกร่งต่อการเข้าถึงข้อมูลมากยิ่งขึ้นในช่วยหลายทศวรรษที่ผ่านมา ผู้เขียนโปรแกรมประสงค์ร้ายจึงปรับใช้เทคโนโลยีนี้ให้เป็นแบบคริปโตล็อคเกอร์ (cryptolocker) ที่จำเป็นต้องมีกุญแจสำหรับการถอดรหัสลับที่ปกป้องข้อมูล

3.2 มัลแวร์เรียกค่าไถ่ (Ransomware)

เราทราบกันดีกว่ารูปแบบการแพร่กระจายมัลแวร์เรียกค่าไถ่มีจุดประสงค์เพื่อหลอกล่อให้เหยื่อยอมรับการเข้าสู่ระบบเครือข่ายผ่านช่องทางการสื่อสารตามปกติ คนร้ายอาศัยการแฝงสิ่งผิดปกติไปกับเนื้อหาข้อความด้วยเทคนิคจำนวนสามแบบ (Teelawittayakul, 2019) ได้แก่ การแฝงกับเอกสารแนบในอีเมล การแฝงกับโฆษณาและการสร้างเว็บไซต์หลอกลวง ในส่วนของเว็บไซต์ที่ถูกสร้างมีวัตถุประสงค์เป็นศูนย์กลางของไฟล์โปรแกรมประสงค์ร้ายที่ล่อลวงให้เหยื่อเรียกไปติดตั้งทั้งแบบอัตโนมัติและแบบผู้ใช้เผลอติดตั้งเอง

ภัยคุกคามที่อาศัยการแพร่กระจายเช่นนี้อาศัยช่องโหว่การให้บริการเว็บแอพพลิเคชั่น ช่องโหว่ของสถาปัตยกรรมเว็บที่มีความเสี่ยงสูงต่อการดำเนินการของคนร้ายมีสองประการ อันดับแรกคือซีเคียลอินเจ็คชั่น (SQL Injection) มีความเสี่ยงมากถึงร้อยละ 55 รองลงมาที่เป็นอันดับสองคือรีโมทโค๊ดเอ็กซ์คิวชั่นมีสัดส่วนอยู่ที่ร้อยละ 22 ส่วนช่องโหว่ที่เกิดจากตัวซอฟท์แวร์มักจะพบกับซอฟท์แวร์บริหารจัดการเนื้อหาบนเว็บ (Content Management System) หรือซีเอ็มเอส (CMS) ที่มีโอกาสถูกเจาะระบบง่ายกว่าชนิดอื่นโดยเฉพาะจุมล่า (Joomla) ส่วนซอฟท์แวร์จัดการเว็บชนิดอีคอมเมิร์ซโดยเฉพาะแม็กเจนโต (Magento) มีความเสี่ยงอยู่เช่นกัน (Umnoiy-Pol et.al., 2018) มาถึงตรงนี้จะเห็นได้ว่าการแพร่กระจายมัลแวร์เรียกค่าไถ่เกิดขึ้นได้ง่ายยิ่งขึ้นผ่านเครือข่ายอินเตอร์เน็ตที่ต้องใช้งานการบริการผ่านเว็บแอพพลิเคชั่น

นักวิชาการด้านความปลอดภัยไซเบอร์ต่างยอมรับว่าม้าโทรจันเอดส์ (AIDS Trojan Horse) เป็นจุดเริ่มต้นของมัลแวร์เรียกค่าไถ่ โทรจันนี้เริ่มรู้จักเมื่อปี พ.ศ.2522 เรียกว่า พีซีไซบอร์ก (PC Cyborg) สร้างโดยโจเฟซ ปอป (Joseph Popp) เหตุการณ์ขณะนั้นเกิดขึ้นระหว่างการประชุมองค์กรอนามัยโลก โจเฟซสร้างแผ่นดิสก์กว่าหมื่นแผ่นสำหรับแจกจ่ายให้ผู้เข้าร่วม เมื่อการประชุมเสร็จสิ้นผู้ที่ได้รับแผ่นดิสก์กลับพบว่าภายในมีไฟล์ที่เป็นไวรัส

คอมพิวเตอร์ รูปแบบการทำงานของโปรแกรมไวรัสนั้นทำให้เครื่องต้องเริ่มต้นระบบ (reboot) ซ้ำกว่าร้อยครั้ง อีกส่วนหนึ่งมีการใช้เทคนิคเข้ารหัสไฟล์และซ่อนเส้นทางหรือไดเรกทอรีของโฟลเดอร์ที่เก็บไฟล์ ยิ่งไปกว่านั้นสิ่งสำคัญที่เกิดขึ้นคือมีการแสดงข้อความขึ้นหลังไวรัสได้ทำงานไปแล้ว โดยระบุว่าผู้ใช้ต้องส่งเงินจำนวนเกือบสองร้อยดอลล่าร์สหรัฐไปยังตู้จดหมายในประเทศปานามาเพื่อปลดล็อกระบบให้เป็นปกติ

เวลาต่อมาเหตุแบบเดียวกันเกิดขึ้นอีกครั้งเมื่อปี พ.ศ.2548 โทรจันจีพีโค๊ด (GPCode) ถูกนำไปใช้ก่อเหตุรบกวนระบบปฏิบัติการวินโดวส์โดยจะทำการคัดลอกไฟล์แบบเข้ารหัสและทำการลบตัวไฟล์ต้นฉบับออกจากระบบ เหตุนี้ทำให้ไฟล์ที่สร้างใหม่ไม่สามารถอ่านและใช้งานได้ รูปแบบการเข้ารหัสลับเป็นแบบ RSA-1024 คำว่า RSA มาจาก Rivest–Shamir–Adleman เป็นชื่อเรียกชนิดกุญแจสาธารณะ (public key) ที่ใช้สำหรับปกปิดข้อมูลให้มีความปลอดภัยทั้งนี้ความซับซ้อนอยู่ที่ตัวเลขต่อท้าย

เมื่อปี พ.ศ.2554 หนอนมัลแวร์เรียกค่าไถ่ถูกตรวจพบในการสร้างความเสียหายต่อการลอกเลียนแบบรหัสผลิตภัณฑ์วินโดว์สที่ใช้สำหรับการเปิดใช้งานซอฟท์แวร์ของบริษัทไมโครซอฟท์ ถัดจากนั้นในช่วงปลายปี พ.ศ.2556 มัลแวร์เรียกค่าไถ่ถูกพัฒนาโดยเครื่องมือ Stamp.EK exploit kit ได้ทำการเจาะระบบปฏิบัติการแม็คอินทอช (Mac OS X) จากนั้นใช้โปรแกรม CryptoLocker สำหรับเข้ารหัสไฟล์เอาไว้เพื่อเรียกค่าไถ่สูงถึง 5ล้านดอลลาร์สหรัฐ ตั้งแต่นั้นเรื่อยมาจนถึงปี พ.ศ.2558 การโจมตีด้วยมัลแวร์เรียกค่าไถ่เกิดความนิยมในหมู่คนร้ายไซเบอร์เป็นอย่างมาก มีการตรวจพบการโจมตีเกิดขึ้นหลากหลายแพลตฟอร์มไม่ใช่แค่วินโดว์สและแม็คอีกต่อไป และการสร้างความเสียหายมีความรุนแรงมากขึ้นอย่างต่อเนื่อง

3.3 ประเภทของมัลแวร์เรียกค่าไถ่

3.3.1 *มัลแวร์แบบเข้ารหัส* การโจมตีเหยื่อด้วยรูปแบบนี้เป็นการเข้ารหัสไฟล์และโฟลเดอร์ส่วนบุคคล อาทิ เอกสาร ไฟล์ตาราง รูปภาพ และวิดีโอ ผลที่เกิดขึ้นทำให้ไฟล์เหล่านั้นถูกลบทันทีเมื่อถูกเข้ารหัสสำเร็จ ต่อจากนั้นผู้ใช้งานจะได้รับไฟล์ข้อความแสดงขั้นตอนจ่ายค่าไถ่ซึ่งอยู่ภายในโฟลเดอร์เดิมที่ไฟล์ของตนถูกลบทิ้งไป เนื้อหาข้อความจะแจ้งวิธีการเข้าถึงเว็บไซต์สำหรับชำระเงิน โดยส่วนมากจะต้องเข้าถึงผ่านบราวเซอร์พิเศษ ได้แก่ ทอร์บราวเซอร์ (TOR browser) เพื่อพาไปยังหน้าเว็บที่กำหนดไว้ จากนั้นคนร้ายจะแจ้งข้อความที่เป็นตัวอักษรและตัวเลขซึ่งเป็นกุญแจสาธารณะสำหรับนำไปยืนยันเมื่อชำระเงินผ่านระบบของคนร้าย

3.3.2 *มัลแวร์แบบล็อคหน้าจอ* เรียกอีกอย่างว่า WinLocker โดยจะทำการล็อคหน้าจอคอมพิวเตอร์ของเหยื่อที่กำลังใช้งานอยู่ จากนั้นจะปรากฏข้อความเกี่ยวกับค่าไถ่และวิธีการชำระเงิน โดยภาพหน้าจอจะเป็นแบบเต็มที่ผู้ใช้ไม่สามารถเปิดหน้าต่างอื่นได้อีก แต่ไม่พบว่าไฟล์ส่วนบุคคลถูกเข้ารหัสด้วยมัลแวร์ชนิดนี้

3.3.3 *มัลแวร์แบบมาสเตอร์บูตเร็คคอร์ด* Master Boot Record (MBR) เป็นองค์ประกอบส่วนหนึ่งที่สำคัญของฮาร์ดไดร์ฟในระบบคอมพิวเตอร์ซึ่งมีหน้าที่สนับสนุนการทำงานของระบบปฏิบัติการประ จำเครื่องให้สามารถเริ่มเข้าระบบได้ มัลแวร์ชนิดนี้จะรบกวนการทำงานของ MBR โดยเฉพาะซึ่งหน้าจอเมื่อเข้าระบบจะถูกขัดจังหวะ และปรากฏข้อความว่าคอมพิวเตอร์ถูกล็อคไว้แล้วต้องชำระค่าไถ่เสียก่อนจึงจะได้รหัสผ่านที่ถูกต้องสำหรับเข้าระบบได้

3.3.4 *มัลแวร์แบบเข้ารหัสเว็บเซิฟเวอร์* เป้าหมายของมัลแวร์ชนิดนี้เป็นตัวเครื่องแม่ข่ายหรือเซิฟเวอร์ที่ให้บริการผ่านเว็บ ไฟล์จำนวนมากที่จำเป็นในการให้บริการจะถูกรบกวนและเข้ารหัสทำให้เมื่อผู้ใช้เรียกหน้าเว็บจะเกิดขัดข้องทันที ส่วนมากเว็บไซต์ที่ถูกโจมตีมากที่สุดจะเป็นเว็บที่พัฒนาหรือสร้างขึ้นแบบระบบบริหารจัดการเนื้อหา (Content Mangement Ssytem) ทั้งนี้มาจากเครื่องมือสร้างเว็บแบบนี้มักมีช่องโหว่เกิดขึ้นเสมอและผู้พัฒนาไม่สามารถอัพเดทหรือปรับปรุงความปลอดภัยได้ทันท่วงที

3.3.5 *มัลแวร์สำหรับอุปกรณ์โมบาย* ปัจจุบันนี้การโจมตีต่ออุปกรณ์พกพาหรือโมบายนั้นเกิดขึ้นกับระบบปฏิบัติการแอนดรอยด์เป็นส่วนใหญ่ โดยมักเกิดจากการดาวน์โหลดไฟล์ต้องสงสัยมาไว้บนเครื่องโดยตรง เรียกว่า drive-by downloads เหตุนี้ทำให้เกิดการสร้างหน้าแอพปลอมขึ้นใช้สำหรับหลอกลวงผู้ใช้งาน แอพที่หลอกลวงมักจะเป็นโปรแกรมป้องกันไวรัสหรือแอพอื่นที่ทำงานด้วยการอาศัยอโดบีแฟลช (Adobe Flash) ในการประมวลผล

3.4 การรับมือการมัลแวร์เรียกค่าไถ่

การปกป้องตนเองจากการตกเป็นเหยื่อมีหลากหลายวิธีขึ้นอยู่กับความพร้อมของผู้ใช้หรือเจ้าของคอมพิวเตอร์แต่ละราย ศูนย์ต่อต้านหลอกลวงและอาชญากรรมไซเบอร์ที่กำกับดูแลโดยตำรวจสหราชอาณาจักรได้แนะนำขั้นตอนสำหรับตรวจตราระบบให้ปลอดภัย (National Fraud & Cyber Crime Centre, 2018) ได้แก่ การติดตั้งโปรแกรมป้องกันไวรัส, การปรับปรุงซอฟท์แวร์และโปรแกรมประยุกต์ให้เป็นปัจจุบัน, การสำรองข้อมูล และการใช้อีเมล์อย่างระมัดระวัง

เมื่อเกิดตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่แล้วสิ่งที่ต้องพิจารณาเป็นลำดับแรกคือระงับการจ่ายเงิน การตอบสนองต่อคำขู่ของคนร้ายเป็นสิ่งที่ต้องหลีกเลี่ยงมากที่สุด (National Fraud & Cyber Crime Centre, 2018) เนื่องจากเมื่อคนร้ายได้รับเงินแล้วไม่เคยมีข้อยืนยันใดที่รับประกันได้ว่าผู้ใช้จะได้สิทธิการเข้าถึงไฟล์หรืออุปกรณ์กลับมาอย่างสมบูรณ์ นอกจากนั้นแล้วกลุ่มผู้กระทำผิดเหล่านี้มีการแบ่งปันข้อมูลเหยื่อและแลกเปลี่ยนพฤติกรรมตอบสนองของเหยื่อระหว่างกัน ตัวอย่างเช่น หากนาย ก.ตกลงจ่ายค่าไถ่เมื่อเดือนที่แล้วหลังจากโดนโจมตี เมื่อเวลาผ่านไปนาย ก.มักจะตกเป็นเหยื่อซ้ำ (re-targeted victim) จากการก่อเหตุแบบนี้

กรณีตัวอย่างที่กล่าวถึงเปรียบได้กับเป็นการเปิดช่องโหว่ระบบของนาย ก.ว่าสามารถใช้เทคนิคแบบเดิมโจมตีได้เสมอแม้จะเหยื่อจะเป็นลูกจ้างภายในองค์กร อย่างไรก็ตามการจ่ายเงินตามคำขู่ในบางครั้งอาจเกิดความสำเร็จโดยได้สิทธิของไฟล์และเครื่องกลับคืนมาปกติ แต่คนร้ายมักจะแอบติดตั้งช่องโหว่ที่เป็นแบบทางเข้าหลังบ้าน (backdoor) เอาไว้เสมอเพื่อเปิดโอกาสให้กลับมาโจมตีในอนาคต

ประตูหลังบ้านหรือแบ็คดอร์ (backdoor/ trapdoor) เป็นเทคนิคหนึ่งที่คนร้ายนิยมในการเปิดจุดช่องโหว่ในโปรแกรม จุดโหว่นี้ใช้สำหรับขยายโอกาสสำหรับการเข้าควบคุมเครื่องและจัดการข้อมูลในระดับผู้ใช้งานสูงสุด สิทธิการเข้าถึงตัวโปรแกรมเป็นสิ่งที่คนร้ายปรารถนามากที่สุดโดยเมื่อมีการปรับแก้ไขในระดับโค้ดไว้แล้วสามารถทำให้รอดพ้นการตรวจจับโดยปกติของระบบคอมพิวเตอร์ได้ (Liangbunprakong, 2012) กล่าวโดยสรุปช่องโหว่ที่ตั้งใจทำไว้จะคอยเอื้อประโยชน์ต่อแฮกเกอร์ (hacker) ควบคุมเครื่องจากระยะไกล ส่วนมากจะใช้การฝังโค้ดไว้ที่ส่วนใดส่วนหนึ่งของระบบที่ต้องอาศัยโปรแกรมตรวจจับและป้องกันไวรัสโดยเฉพาะ

4. ระเบียบวิธีการศึกษา

บทความนี้เป็นการศึกษาเชิงเอกสารที่มีต่อสภาพปัญหาและการรับมือภัยคุกคามออนไลน์ที่เรียกว่ามัลแวร์เรียกค่าไถ่ ข้อมูลที่ใช้ในการศึกษาเป็นชนิดทุติยภูมิที่ผู้เขียนได้รวบรวมไว้ในช่วงหลายปีที่ผ่านมา ขอบเขตของการศึกษามุ่งไปที่สถานการณ์การแพร่ระบาดของมัลแวร์และความเสียหายที่เกิดขึ้นในประเทศไทย ตลอดจนผู้เขียนได้กล่าวถึงแนวทางการรับมือโดยหน่วยงานตำรวจทั้งในประเทศไทยและระดับสากล อย่างไรก็ตามข้อจำกัดของการศึกษานี้กล่าวคือการจัดเก็บข้อมูลรับแจ้งเหตุและความเสียหายที่เกิดขึ้นในประเทศไทยมีจำกัด ข้อมูลที่ปรากฏสาธารณะเกิดจากสื่อสารมวลชนเป็นส่วนใหญ่ สิ่งนี้ทำให้การนำข้อมูลดังกล่าวมาใช้ในการศึกษาจำเป็นต้องมีการพิจารณาและคัดเลือกอย่างเหมาะสมเพื่อให้เกิดความน่าเชื่อถือทางวิชาการ

5.ผลการศึกษา

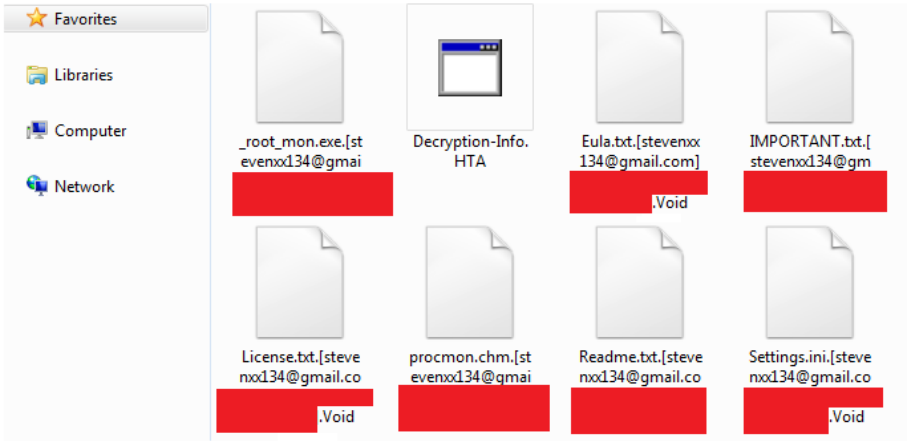
5.1 สถานการณ์การแพร่ระบาดของมัลแวร์เรียกค่าไถ่ที่น่าสนใจในปัจจุบัน

5.1.1 วันนาคราย (WannaCry) เป็นมัลแวร์เรียกค่าไถ่ที่มาพร้อมกับความสามารถในการแพร่กระจายด้วยตนเองจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งผ่านระบบเครือข่ายเดียวกัน การดำเนินการอาศัยช่องโหว่ของโปรโตคอลระบบที่ชื่อเอสเอ็มบี (Server Message Block: SMB) ข้อกำหนดการสื่อสารระหว่างคอมพิวเตอร์หรือโปรโตคอล (protocol) ชนิดนี้ใช้สำหรับการแชร์ไฟล์ ปรินเตอร์ การเชื่อมต่อแบบอนุกรม ตลอดจนการสื่อสารที่อาศัยพอร์ตของคอมพิวเตอร์วินโดว์ส ช่องโหว่ชนิดนี้ถูกเปิดเผยให้รับรู้ทางสาธารณะเพียงหนึ่งเดือนก่อนหน้าการระบาดครั้งใหญ่เมื่อเดือนพฤษภาคม พ.ศ.2560 หน่วยงานในระบบสาธารณสุขของสหราชอาณาจักรถูกโจมตีมากที่สุด

(Thailand Computer Emergency Response Team, 2017) ส่วนในประเทศไทยมีการตรวจพบเครื่องคอมพิวเตอร์ติดมัลแวร์นี้อยู่จำนวนหนึ่งแต่ยังไม่แพร่กระจายในวงกว้าง คำแนะนำเบื้องต้นเมื่อพบว่าถูกโจมตีด้วยมัลแวร์วันนาคราย ผู้ใช้ต้องรีบตัดการเชื่อมต่อกับเครือข่ายและปิดเครื่องโดยทันที จากนั้นอัพเดทฐานข้อมูลล่าสุดของโปรแกรมป้องกันไวรัสบนเครื่องที่ไม่ถูกโจมตี แล้วนำฐานข้อมูลดังกล่าวไปปรับปรุงกับโปรแกรมป้องกันไวรัสบนเครื่องที่เสียหายผ่านการเริ่มต้นระบบแบบปลอดภัย (safe mode) จากนั้นให้ดำเนินตรวจสอบหรือสแกนหามัลแวร์โดยละเอียด การดำเนินการดังกล่าวเป็นเพียงยับยั้งความเสียหายไม่ให้ลุกลาม การศึกษาในปัจจุบันยังไม่ปรากฏวิธีการใดที่กู้คืนไฟล์หลังจากถูกเข้ารหัสด้วยวันนาครายอย่างสมบูรณ์แบบโดยไม่จ่ายเงิน

5.1.2 เพทย่า (Petya) เป็นมัลแวร์เรียกค่าไถ่ชนิดหนึ่งที่ตรวจพบการแพร่ระบาดครั้งแรกเมื่อกลางปี พ.ศ. 2560 คุณลักษณะการแพร่กระจายมีความคล้ายคลึงกับวันนาครายที่อาศัยช่องโหว่ของโปรโตคอลเอสเอ็มบีเวอร์ชั่นแรก เวลาปกติคอมพิวเตอร์จะมีการตรวจสอบสิทธิทั้งเครื่องลูกและเครื่องแม่ แต่เมื่อแฮกเกอร์นำช่องโหว่จากโปรโตคอลเอสเอ็มบีไปพัฒนาเพื่อโจมตีจะเป็นการรบกวนการทำงานปกติทำให้เกิดความเสียหาย แม้จะไม่ได้เข้ารหัสลับกับไฟล์ส่วนตัวทั่วไปแต่เพทย่าจะใช้การเข้ารหัสลับกับไฟล์สำคัญคือมาสเตอร์ไฟล์เทเบิล (Master File Table: MFT) ของพาร์ทิชั่นในระบบคอมพิวเตอร์แทน ตารางนี้คอยทำหน้าที่ระบุตำแหน่งไฟล์และเนื้อหาเมื่อถูกเรียกจากระบบหรือผู้ใช้งาน เมื่อเกิดการทำงานผิดพลาดจะส่งผลให้ไม่สามารถระบุตำแหน่งไฟล์อย่างถูกต้องบนฮาร์ดดิสอีกต่อไปได้ ความเสียหายทั่วโลกจากมัลแวร์นี้เกิดขึ้นไม่น้อยกว่าสามแสนเครื่องภายในสามวัน (Thailand Computer Emergency Response Team, 2017) ประเทศรัสเซีย ยูเครน และอินเดียเป็นสามเป้าหมายหลักที่ถูกโจมตีมากที่สุด สถาบันการเงิน โรงงานไฟฟ้า และสนามบินเป็นโครงสร้างพื้นฐานที่ตกเป็นเป้าของการคุกคาม

5.1.3 สเปด (Spade) เป็นมัลแวร์รูปแบบหนึ่งที่ถูกระบุใช้เป็นเครื่องมือโจมตีโรงพยาบาลสระบุรีเมื่อเดือนกันยายนปี พ.ศ.2563 (Mahidol University, Nakhonsawan Campus Project, 2020) มัลแวร์สเปดเป็นหนึ่งในรูปแบบการติดเชื้อของคอมพิวเตอร์ที่จะสร้างกลไกลล็อคการเข้าถึงข้อมูล มัลแวร์เรียกค่าไถ่นี้ถูกจัดให้อยู่กับกลุ่มของมัลแวร์ทั่วไปที่ชื่อวอยด์คริปท์ (VoidCrypt) (Cyber Security Plan, 2020) โดยที่การโจมตีด้วยสเปดมีการตรวจพบครั้งแรกราวเดือนเมษายน พ.ศ.2563 จุดผิดสังเกตที่ทำให้ได้ชัดเจนอย่างหนึ่งคือไฟล์แปลกปลอมที่ลงท้ายด้วย .Void หรือ .Spade โดยจะมาพร้อมกับอีเมลหลอกลวง เนื้อหาอีเมล์อาจไม่ปรากฏชัดแจ้งให้เห็นสิ่งแปลกปลอมเน่องจากมีการเข้ารหัสอีเมล์ป้องกันเอาไว้ชั้นหนึ่ง รูปแบบการเข้ารหัสใช้สถาปัตยกรรมการเข้ารหัสเป็นบล็อกแบบสมมาตรหรือแบบเออีเอส (Advance Encryption Standard :AES) ผสมผสานกับอัลกอริทึมการเข้ารหัสแบบอาร์เอสเอ (Rivest-Shamir-Adleman cryptosystem: RSA) ส่งผลให้การล็อคข้อมูลของผู้ใช้เป็นไปโดยปลอดภัยเปรียบเสมือนผู้ใช้งานงานปกป้องจากผู้ใช้คนอื่น



รูปภาพที่ 1: ไฟล์ถูกเข้ารหัสลงท้ายด้วย .Void และไฟล์แนะนำการกู้คืน .HTA (Sonic Wall, 2020)

ปัจจุบันยังไม่พบขั้นตอนการถอดรหัสไฟล์ที่ติดไวรัสแบบ .spade นี้โดยปราศจากการสำรองข้อมูล (backup) ไว้ก่อนหน้า นอกจากเข้ารหัสไฟล์ไว้แล้วตัวมัลแวร์ยังคงทิ้งข้อความให้ผู้ใช้รู้ถึงวิธีการถอดรหัส (Read-For-Decrypt) ด้วยไฟล์ข้อความชนิด .HTA (HTML Application) (Sonic Wall, 2020) คำขู่จะให้ชำระเงินเป็นบิตคอยน์หรือสกุลเงินดิจิทัลอื่นซึ่งจะได้รับเครื่องมือสำหรับถอดรหัสกลับมา บัญชีอีเมลที่มักจะพบมาพร้อมกับมัลแวร์สเปดได้แก่ rsaencrypt@tutanota. com, rsaencrypt@protonmail. ch, VoidDeceryptor @tutanota. com, หรือ VoidDeceryptor@protonmail.com

5.2 แนวทางปฏิบัติในระดับสากลต่อการควบคุมสถานการณ์การแพร่ระบาดของมัลแวร์เรียกค่าไถ่

การถอดถอน (removal) มัลแวร์เรียกค่าไถ่เป็นอีกวิธีที่ได้รับความนิยมเช่นกัน แม้อดีตเคยเชื่อกันว่าเมื่อติดไวรัสเรียกค่าไถ่แล้วไม่สามารถที่จะกู้คืนหรือถอดถอนมัลแวร์ได้ ปัจจุบันมีโครงการความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายและบริษัทผู้ให้บริการความปลอดภัยทางระบบสารสนเทศได้ร่วมมือระดมทุนจัดตั้งโครงการยกเลิกค่าไถ่หรือโนมอร์แรนซั่ม (No More Ransom) โครงการนี้ได้รับการสนับสนุนจากหน่วยงานภาครัฐและเอกชน อาทิ หน่วยงานอาชญากรรมทางเทคโนโลยีของตำรวจเนเธอร์แลนด์ (National High Tech Crime of Netherlands Police), ศูนย์ต่อต้านอาชญากรรมไซเบอร์ของตำรวจยุโรป (EUROPOL’s European Cybercrime Centre), บริษัทแมกกาฟี (McAfee) บริษัทแคสเปอสกี (Kaspersky) เป็นต้น โดยโครงการดังกล่าวดำเนินการบนระบบประมวลผลคลาวด์บนแพลตฟอร์มอะเมซอนเว็บเซอร์วิส (Amazon Web Services) และบาร์ราคิวดา (Barracuda)

วัตถุประสงค์ของโครงการยกเลิกค่าไถ่ คือ การช่วยเหลือสังคมออนไลน์ให้ตระหนักถึงการรับมือเมื่อตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่แล้วห้ามจ่ายเงินคืนคนร้าย การดำเนินงานโครงการเป็นไปลักษณะการสร้างความตระหนักรับรู้ผ่านการถ่ายทอดและการช่วยเหลือเมื่อเกิดเหตุ แม้จะเป็นโครงการที่ก่อตั้งในพื้นที่ภาคพื้นยุโรปก็ตาม แต่เว็บไซต์ของโครงการรองรับการแสดงผลหลายภาษามากถึง 36 ภาษา (No More Ransom, n.d.) ซึ่งมีภาษาไทยเปิดให้บริการด้วยเช่นกัน

5.3 เครือข่ายความร่วมมือขององค์กรตำรวจระหว่างประเทศสำหรับติดตามและตรวจสอบการแจ้งเหตุมัลแวร์เรียกค่าไถ่

ตารางที่ 1 : หน่วยงานตำรวจที่ร่วมสนับสนุนและตรวจสอบการรับแจ้งเหตุมัลแวร์เรียกค่าไถ่

Country	Police's contribution	
	Partner	Report
Australia	✔	✔
Austria	✔	✔
Belgium	Europol	✔
Bosnia & Herzagovina	✔	
Bulgaria	✔	✔
Croatia	✔	✔
Cyprus	✔	✔
Czech Republic	✔	✔
Denmark	✔	✔
Estonia	✔	✔
Finland	✔	✔
France	Europol	✔
Germany	✔	✔
Greece	✔	✔
Hong Kong	✔	✔
Hungary	✔	✔
Iran	✔	✔
Ireland	✔	✔
Israel	✔	✔
Italy	✔	✔
Japan	✔	✔
Latvia	✔	✔
Lithuania	✔	✔
Luxembourg	Europol	✔
Malta	✔	✔
Netherlands	Founder of No More Ransom project	✔
New Zealand	✔	
Poland	✔	
Portugal	✔	✔
Romania	Europol	✔
Russia	✔	✔
Scotland	✔	✔
Singapore	✔	✔
Slovakia	✔	✔
Slovenia	✔	✔
South Korea	✔	✔
Spain	✔	✔
Sweden	✔	✔
Switzerland	✔	
Taiwan	✔	
Ukraine	✔	✔
United Kingdom	✔	✔
United States	Interpol	✔
GCC POL	✔	
Interpol	✔	
Europol	Founder of No More Ransom project	

ที่มา: List of supporting partners and police report service (No More Ransom, n.d.)

จำนวนองค์กรตำรวจที่เข้าร่วมเป็นส่วนหนึ่งกับโครงการยกเลิกค่าไถ่ (No More Ransom) มีจำนวนมากขึ้นอย่างต่อเนื่องซึ่งเห็นได้จากตารางข้างต้น รูปแบบการมีส่วนร่วมนั้นประกอบไปด้วยการสนับสนุนทรัพยากรและการติดตามตรวจสอบการรับแจ้งเหตุ ทรัพยากรที่ได้รับการสนับสนุนนั้นนอกจากอยู่ในรูปเงินทุนแล้วยังรวมไปถึงทรัพยากรด้านอื่น ได้แก่ กำลังพล อุปกรณ์ และความรู้ ปัจจุบันมีหน่วยงานตำรวจ 41 แห่งจากทั่วโลกที่เข้าร่วม

โครงการ ตำรวจสิงคโปร์เป็นเพียงประเทศเดียวจากภูมิภาคอาเซียน (ข้อมูลเมื่อวันที่ 6 ตุลาคม 2563) ที่เป็นส่วนหนึ่งในการใช้งานโครงการยกเลิกค่าไถ่ ลักษณะของการดำเนินการเป็นการเชื่อมโยงช่องทางรับแจ้งเหตุมัลแวร์ไปยังระบบรายงานของตำรวจ (police report) โดยตรง ทั้งนี้การรับแจ้งมัลแวร์นี้สามารถส่งผ่านข้อมูลไปยังระบบบริการภายในประเทศที่มีไว้อยู่แล้วเพื่อลดความซ้ำซ้อน

ตารางที่ 2 : รายการมัลแวร์เรียกค่าไถ่ที่ถูกถอดรหัสสำเร็จ

777 Ransom	Bitcryptor	Cyborg	GlobeImposter	LambdaLocker	Muhstik	Pylocky	TurkStatic
AES_NI	CERBER	DXXD	GoGoogle	Linux.Encoder	Nemty	Rakhni	VCRYPTOR
Agent.iih	CheckMail	Damage	Gomasom	Loocipher	Nemucod	Rannoh	WannaCryFake
Alcatraz	Chernolocker	Democry	HKCrypt	Lortok	NemucodAES	Ransomwared	Wildfire
Alpha	Chimera	Derialock	Hakbit	MacRansom	Nmoreira	RedRum	XData
Amnesia	Coinvault	Dharma	HiddenTear	Magniber	Noobcrypt	Rotor	XORBAT
Annabelle	Cry	DragonCyber	HildaCrypt	Mapo	Ouroboros	SNSLocker	XORIST
Aura	CryCryptor	ElvisPresley	Iams00rry	Marlboro	Ozozalocker	Shade	Yatron
Aurora	CrySIS	EncrypTile	InsaneCrypt	Marsjoke	PHP	SimpleLocker	ZQ
AutoIt	Cryakl	Everbe 1.0	Iwanttits	MegaLocker	Paradise	SpartCrypt	ZeroFucks
AutoLocky	Crybola	FenixLocker	JSWorm	GetCrypt	Pewcrypt	Stampado	Zorab
Avest	Crypt32	FilesLocker	Jaff	Globe	Philadelphia	Syrk	djvu
BTCWare	Crypt888	FortuneCrypt	JavaLocker	Globe/Purge	Planetary	Teamxrat/Xpan	
BadBlock	CryptON	Fury	Jigsaw	Merry X-Mas	Pletor	TeslaCrypt	
BarRax	CryptXXX	GalactiCryper	Kokokrypt	MirCop	Popcorn	Thanatos	
Bart	CryptoMix	GandCrab	Lamer	Mira	Professeur	ThunderX	
BigBobRoss	Cryptokluchen	Globe3	LECHIFFRE	Mole	Puma	Trustezeb	

ที่มา : Decryption Tools (No More Ransom, n.d.)

ตารางข้างต้นเป็นบัญชีรายชื่อมัลแวร์ที่โครงการยกเลิกค่าไถ่ได้เปิดให้ผู้ใช้ทั่วไปสามารถดาวน์โหลดเครื่องมือถอดรหัสมาใช้ได้อย่างอิสระ ยกตัวอย่างเช่นมัลแวร์ชื่อ WannaCryFake ที่ปรากฏอยู่ในบัญชีเครื่องมือถอดรหัส ผู้ใช้ที่ต้องการถอดถอนตัวนี้สามารถเข้าไปดาวน์โหลดเครื่องมือและศึกษาขั้นตอนการดำเนินการด้วยตนเอง ผู้พัฒนาเครื่องมือสำหรับถอดรหัส (decryptor) ชื่อเอมซิสซอฟท์ (Emsisoft) ได้เผยแพร่แหล่งดาวน์โหลดข้อมูลสำหรับแก้ไขปัญหามัลแวร์เรียกค่าไถ่หลากหลายชนิด แม้ WannaCryFake จะมีความแตกต่างกับ WannaCry ที่เคยสร้างความเสียไปทั่วโลกช่วงปี พ.ศ.2560 ก็ตาม เหยื่อทั่วไปยังพอมีตัวเลือกในการแก้ไขปัญหาเบื้องต้นกับมัลแวร์ชื่อคล้ายกัน เนื่องจากผู้ใช้ทั่วไปอาจสับสนระหว่างมัลแวร์ทั้งสองแต่เมื่อได้ลองใช้เครื่องมือที่จัดการปัญหาได้อาจจะประสบผลสำเร็จในถอดถอนมัลแวร์หรือลดทอนความเสียหายลงได้บ้าง

นอกเหนือไปจากการระงับจ่ายค่าไถ่และการพยายามถอนมัลแวร์แล้ว การรายงานเหตุไปยังหน่วยงาน ที่เปิดให้รับแจ้งถือว่าเป็นสิ่งที่พึงกระทำ หน่วยงานตำรวจในหลายประเทศได้เข้าร่วมเป็นส่วนหนึ่งของโครงการ

ยกเลิกค่าไถ่และเปิดให้เหยื่อผู้เสียหายสามารถแจ้งเหตุผ่านระบบรับแจ้งออนไลน์ ทุกรายงานการแจ้งเหตุมัลแวร์เรียกค่าไถ่ส่งผลให้เจ้าหน้าที่และนักวิเคราะห์ความมั่นคงไซเบอร์ได้เข้าใจในรายละเอียดและพฤติการณ์ก่อเหตุที่เกิดขึ้นจากคนร้าย ยิ่งไปกว่าหลักฐานดิจิทัลหรือร่องรอยที่คนร้ายหลงเหลือไว้จะเป็นประโยชน์ต่อการสืบสวนของตำรวจและหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง

5.4 ระบบรับแจ้งเหตุฉ้อโกงออนไลน์ (Report Online Fraud)

มัลแวร์เรียกค่าไถ่เป็นอาชญากรรมดิจิทัลชนิดการหลอกลวงหรือฉ้อโกง เมื่อมีเหตุเกิดขึ้นผู้ใช้งานทั่วไปสามารถเข้าไปเริ่มกระบวนการรายงานเหตุร้ายด้วยตนเองผ่านระบบรับแจ้งที่หน่วยงานในประเทศที่เกิดเหตุ โดยทั่วไปการแจ้งเหตุฉ้อโกงถูกแบ่งระดับการตอบสนองออกเป็นสองส่วน ได้แก่ แบบเร่งด่วน และแบบปกติ โดยทั้งสองแบบแตกต่างกันที่มีความเสียหายต่อทรัพย์สินที่เป็นเงินหรือไม่เพียงเท่านั้น

รายงานแจ้งเหตุที่ต้องตอบสนองแบบเร่งด่วนนั้น ผู้แจ้งต้องระบุถึงความสูญเสียทรัพย์สินอาจเป็นเงินในบัญชีธนาคารหรือเงินสกุลดิจิทัลพร้อมทั้งระบุรายละเอียดเกี่ยวกับสถาบันการเงินที่ใช้บริการเมื่อเกิดเหตุ ภายหลังกรอกข้อมูลส่วนบุคคลแล้ว ขั้นต่อไปเป็นพฤติการณ์หลอกลวงที่สูญเงินไป ข้อมูลที่ต้องแจ้งประกอบไปด้วย สกุลเงิน จำนวนเงินที่เสีย จำนวนเงินที่ได้คืน ชนิดหลักฐาน และช่องทางอื่นที่เคยแจ้งไว้ ในส่วนของหลักฐานที่เป็นประโยชน์ต่อการตั้งต้นคดีของตำรวจ ได้แก่ สำเนาการติดต่อสื่อสารทางอีเมล์ จดหมาย แฟ็กซ์ บันทึกการโทรเข้าออก ประวัติการรับส่งข้อความ รูปภาพ การบันทึกของกล้องวงจรปิด เอกสารสัญญา บันทึกยินยอม เอกสารทางกฎหมายอื่นและ/หรือหลักฐานอย่างอื่นที่อาจเป็นประโยชน์

ขั้นต่อไปเป็นการระบุรายละเอียดผู้ต้องสงสัย ระบบจะจำแนกรูปแบบก่อเหตุของคนร้ายเป็นแบบบุคคลและแบบองค์กรหรือบริษัท หากในกรณีที่เหยื่อรู้ข้อมูลคนร้ายมาบ้างสามารถแจ้งรายละเอียดเท่าที่ทราบได้ เช่น วัน เดือนปีที่เริ่มพูดคุย หมายเลขโทรศัพท์ อีเมล์ บัญชีสื่อสังคมออนไลน์ (social media) ชื่อและนามสกุล ชื่อเรียก ที่อยู่ การพบเจอหน้าคนร้าย ยานพาหนะ เป็นต้น แต่หากผู้ต้องสงสัยกระทำเป็นกลุ่มคณะหรือองค์กร ผู้แจ้งสามารถเพิ่มเติมรายละเอียดที่เป็นชื่อองค์กร และเว็บไซต์ที่อาจเชื่อมโยงไปยังบริษัทห้างร้านของคนร้าย นอกจากนั้นการระบุรายละเอียดการชำระเงินเป็นสิ่งที่ต้องระบุไว้เช่นกัน โดยปกติจะต้องแจ้งรูปแบบการจ่ายเงินที่ถูกหลอกลวงไป อาทิ บัญชีธนาคาร บัตรเครดิตหรือเดบิต เช็ค บริการการเงินอิเล็กทรอนิกส์ เงินสด เป็นต้น

ก่อนที่จะสิ้นสุดกระบวนการแจ้งเหตุผ่านระบบบริการออนไลน์นั้น โดยทั่วไปผู้แจ้งสามารถระบุรายละเอียดเพิ่มเติมในช่องการกรอกข้อมูลที่เป็นอิสระ ส่วนนี้จะเป็นประโยชน์อย่างยิ่งต่อการปะติดปะต่อพฤติการณ์ก่อเหตุ รวมทั้งอาจนำไปเชื่อมโยงกับรายงานการแจ้งคดีอื่นที่คล้ายคลึงกัน อย่างไรก็ตามผู้แจ้งต้องพึงระลึกเสมอว่าการแจ้งข้อมูลอันเป็นเท็จหรือคลาดเคลื่อนทั้งที่เกิดจากความไม่ตั้งใจก็ตามอาจนำไปสู่การตรวจสอบย้อนกลับในภายหลัง

ด้วยเทคโนโลยีระบบรับแจ้งเหตุออนไลน์ในปัจจุบันหลายองค์กรได้พัฒนาระบบที่ใช้การวิเคราะห์ความเชื่อมโยงรายละเอียดจากฐานข้อมูลหลายแหล่ง

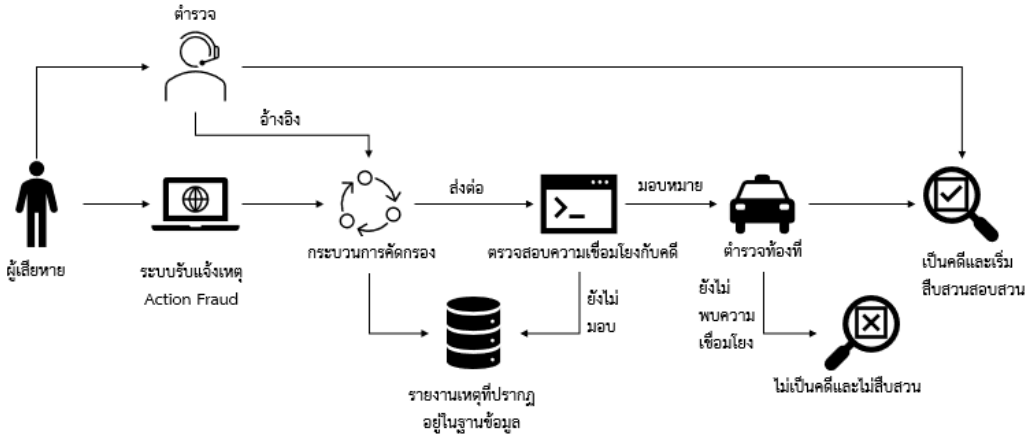
5.5 การรับมือมัลแวร์เรียกค่าไถ่ในประเทศไทย

เมื่อปี พ.ศ.2560 มัลแวร์เรียกค่าไถ่ชื่อวันนาคราย (WannaCry) ถูกตรวจพบการแพร่ระบาดในประเทศอย่างกว้างขวาง สำนักงานพัฒนาธุรกิจทางอิเล็กทรอนิกส์เคยรายงานไว้ว่าจำนวนรายงานเหตุภัยคุกคามเพิ่มขึ้นหลายเท่าตัวระหว่างปี พ.ศ.2554 ถึง 2559 เรื่อยจนมาถึงครึ่งปีแรกของปี พ.ศ.2560 ช่วงเวลานั้นมัลแวร์เรียกค่าไถ่และบ็อทเน็ต (botnet) ถูกใช้เจาะระบบเครือข่ายคอมพิวเตอร์ของภาครัฐและเอกชนอย่างต่อเนื่อง (Umnoiy-Pol et.al., 2018) ตัวอย่างเหตุการณ์โจมตีด้วยวันนาครายที่น่าสนใจเกิดขึ้นกับศูนย์รับแจ้งเหตุ 191 ของตำรวจภูธรจังหวัดศรีสะเกษและฉะเชิงเทรา เหตุการณ์เกิดเมื่อปี พ.ศ.2560 โดยที่ความเสียหายนั้นทำให้ระบบรับแจ้งเหตุหยุดชะงักภายในพื้นที่ทั้งสองจังหวัด (Thairath Online, 2017) การกู้คืนระบบอาศัยผู้เชี่ยวชาญภายนอกร่วมกับเจ้าหน้าที่เทคนิคของตำรวจจากส่วนกลางมาร่วมกู้คืนระบบให้กลับมาใช้งานเป็นปกติ มัลแวร์วันนาครายถูกใช้ล้วงข้อมูลบัญชีธนาคารที่ร่วมกับบริการออนไลน์ โดยมีผู้ใช้งานโทรศัพท์มือถือเป็นกลุ่มเป้าหมายหลัก

การโจมตีหน่วยงานสาธารณสุขปลายปีที่ผ่านมาถือเป็นปรากฏการณ์ที่เกิดขึ้นน้อยมากในประเทศไทย มัลแวร์สเปดเริ่มแพร่ระบาดตั้งแต่กลางปี พ.ศ.2563 ผ่านการตรวจพบของสถาบันวิจับความปลอดภัยไซเบอร์ในหลายประเทศ โรงพยาบาลในสระบุรีมาถูกโจมตีช่วงเดือนกันยายน ความเสียหายที่เกิดขึ้นแม้จะไม่เปิดเผยถึงการสูญเสียทางการเงิน แต่สื่อมวลชนรายงานว่าข้อมูลทะเบียนผู้ป่วยของโรงพยาบาลถูกเข้ารหัสและปิดกั้นการเข้าถึง การให้บริการทางการแพทย์ต้องหยุดชะงักทันที ระบบสารสนเทศภายในและภายนอกต้องถูกหยุดการให้บริการเป็นการชั่วคราวซึ่งเป็นการปฏิบัติตามคำแนะนำมาตรฐานโดยหน่วยงานไทยเซิร์ต

5.6 การแจ้งเหตุภัยคุกคามไซเบอร์ภายในประเทศ

ช่องทางรับแจ้งเหตุเมื่อเกิดภัยคุกคามทางไซเบอร์ของประเทสไทยมีอยู่สองแห่ง ได้แก่ 1) ศูนย์แจ้งเรื่องร้องเรียน 1212 OCC Service (1212 Online Complaint Center, n.d.) และ 2)ระบบรับแจ้งเหตุออนไลน์ของตำรวจปราบปรามอาชญากรรมทางเทคโนโลยี (Technology Crime Suppression Division, n.d.) โดยทั้งสองช่องทางนี้มีความแตกต่างด้านหน่วยงานผู้รับหน้าที่ดำเนินเรื่อง และคุณลักษณะของเหตุที่เปิดให้แจ้ง ศูนย์ 1212 เปิดให้แจ้งเหตุเกี่ยวกับคำร้องเรียนที่มุ่งไปที่การบริโภคและการทำธุรกรรมออนไลน์เป็นหลัก ส่วนศูนย์รับแจ้งของตำรวจจะเน้นไปที่เหตุร้ายหรืออาชญากรรมที่ใช้คอมพิวเตอร์หรือเกี่ยวข้องกับหลักฐานดิจิทัล



รูปภาพที่ 2: กระบวนการแจ้งเหตุฉ้อโกงผ่านระบบ Action Fraud (Lipson, 2019)

ศูนย์รับแจ้งเหตุคุกคามไซเบอร์ของประเทศไทยทั้งสองแห่งเมื่อนำไปเปรียบเทียบกับศูนย์รับแจ้งของตำรวจต่างประเทศในโครงการยกเลิกค่าไถ่ (No More Ransom Project) พบว่ามีความแตกต่างหลายจุด สิ่งแรกคือการลงทะเบียนผู้แจ้งเหตุ ศูนย์ 1212 และศูนย์ตำรวจไม่พบระบบการลงทะเบียนผู้ใช้งาน ทั้งสองแห่งเริ่มต้นกระบวนการรับแจ้งผ่านหน้าเว็บไซต์ด้วยการให้ผู้ใช้เยี่ยมชม (visitor) สามารถกรอกข้อมูลได้ทันที ตัวเลือกการแจ้งเหตุแบ่งเป็นการเลือกเหตุร้ายหรือเรื่องร้องเรียน ต่อจากนั้นผู้แจ้งต้องกรอกข้อมูลให้ครบถ้วนกล่องข้อความบางส่วนถูกตั้งค่าบังคับให้กรอกเป็นอย่างน้อยแล้วจึงสามารถกดส่งเพื่อบันทึกเข้าระบบ แม้จะมีการเปิดให้อัพโหลดไฟล์มัลติมีเดียเพิ่มเติมและระบุวันเดือนปีที่เกิดเหตุได้ก็ตาม แต่ในท้ายที่สุด กระบวนการให้ผู้รับแจ้งติดตามย้อนกลับผ่านระบบออนไลน์อาจเกิดความลำบาก ทั้งสองศูนย์รับแจ้งไม่มีช่องสำหรับบันทึกข้อมูลส่วนบุคคลไม่ว่าจะเป็นชื่อ นามสกุล หมายเลขโทรศัพท์ อีเมล์ สื่อสังคมออนไลน์ เป็นต้น ในส่วนนี้แตกต่างจากศูนย์รับแจ้งเหตุของตำรวจสหราชอาณาจักรที่เรียกว่าระบบ Action Fraud ที่ผู้ใช้ต้องระบุรายละเอียดแบบเจาะจงของสถานะผู้แจ้งเสียก่อน นอกจากนั้นรายละเอียดเกี่ยวกับความสูญเสียทางการเงินไม่ได้มีกล่องข้อความให้ระบุไว้โดยเฉพาะ อย่างไรก็ตามผู้แจ้งอาจจะกรอกข้อมูลผ่านกล่องข้อความสำหรับข้อมูลเพิ่มเติมที่เตรียมไว้แล้วได้เช่นกัน

6. สรุปและข้อเสนอแนะ

จากการศึกษาคุณลักษณะของโปรแกรมเรียกค่าไถ่และรูปแบบการสร้างความเสียหาย ตลอดจนแนวทางการรับมือกับภัยคุกคามที่ข่มขู่เรียกร้องทรัพย์สินในลักษณะเช่นที่กล่าวมานี้ ผู้เขียนขอสรุปให้เกิดความเข้าใจอย่างกระชับดังต่อไปนี้

6.1 ความซับซ้อนทางเทคโนโลยีที่เพิ่มมากขึ้นทำให้คนร้ายไซเบอร์ (cybercriminal) สามารถเข้าควบคุมเครื่องคอมพิวเตอร์จากระยะไกลหรือเข้ารหัสลับไฟล์ที่ถูกเก็บไว้ในเครื่อง แรงจูงใจหลักของคนร้ายคือการขู่กรรโชกเอาเงินจากค่าไถ่โดยแลกกับการคืนสิทธิให้เจ้าของเครื่อง มัลแวร์ชนิดนี้เกิดขึ้นจากการสื่อสารได้หลายช่องทาง แต่ที่นิยมจะเป็นในแบบไฟล์แนบมาอีเมล์ที่ดูเป็นปกติโดยมักจะใช้หลอกล่อให้เหยื่อหลงเชื่อว่าเป็นการติดต่อสื่อสารประจำวันตามปกติตามสภาพแวดล้อมของที่ทำงาน ดังนั้นเมื่อพิจารณาถึงสิทธิที่จะได้คืนมาหลังจากปฏิบัติตามคำขู่อาจจะไม่ได้กลับคืนมาโดยสมบูรณ์

6.2 แม้การหลอกลวงด้วยมัลแวร์เรียกค่าไถ่ที่มากับการสื่อสารประจำวันกลับพบว่าผู้ใช้ในภาคธุรกิจยังขาดความระมัดระวังในการตรวจสอบผู้ส่งและเนื้อหาในข้อความ การรับมือกับเหตุการณ์เมื่อไฟล์ถูกเข้ารหัสที่เกิดจากความพลั้งเผลอของผู้ใช้ทั่วไปทำให้ไม่ได้รับการแก้ไขโดยผู้เชี่ยวชาญในทันที หลายครั้งมักจบลงด้วยการยินยอมชำระเงินเป็นค่าไถ่เพื่อหวังให้คนร้ายคืนสิทธิกลับมา ในทางตรงกันข้ามคนร้ายเรียนรู้ทุกครั้งจากปฏิกิริยาตอบสนองของเหยื่อที่มีต่อข้อความข่มขู่ หากได้รับเงินครบถ้วนปราศจากการต่อรองยิ่งทำให้เกิดความมั่นใจในการลงมือซ้ำ แต่หากถูกเพิกเฉยแม้ความเป็นจริงเหยื่อจะต้องสูญเสียไฟล์ก็ตาม แต่เป็นการสะท้อนให้คนร้ายได้รับรู้ถึงการปฏิเสธต่อการยินยอมตามคำขู่

6.3 โครงการยกเลิกค่าไถ่ถือเป็นศูนย์กลางการต่อต้านมัลแวร์ในระดับสากล โครงการนี้เปิดให้บริการถอดถอนมัลแวร์แบบไม่มีค่าใช้จ่ายผ่านการดำเนินการด้วยตนเอง หากเกินความสามารถของผู้ใช้ทั่วไปองค์กรธุรกิจภายใต้โครงการดังกล่าวยินดีให้คำปรึกษาในฐานะผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ซึ่งอาจมีการเรียกเก็บค่าใช้จ่ายในบางกรณี แม้ท้ายที่สุดข้อมูลไม่อาจกู้คืนครบถ้วน แต่ทำให้ผู้ใช้ได้ตระหนักถึงการรักษาความปลอดภัยเมื่อต้องเชื่อมต่อระบบสื่อสารจากภายนอกองค์กร

6.4 การรับแจ้งเหตุออนไลน์ผ่านระบบการให้บริการที่ดูแลโดยตำรวจเป็นสิ่งจำเป็นสำหรับสังคมดิจิทัล แม้การหลอกลวงหรือโจมตีด้วยมัลแวร์เรียกค่าไถ่เป็นสิ่งซับซ้อน แต่ข้อมูลพื้นฐานทั้งส่วนบุคคล การชำระเงิน และการติดต่อสื่อสารกับคนร้ายล้วนแล้วแต่เป็นองค์ประกอบสำคัญ สิ่งเล็กน้อยเหล่านี้จะช่วยปะติดปะต่อเรื่องราวนำไปสู่การตีกรอบแนวทางการสืบสวนจนนำไปสู่ตัวคนร้ายได้ในที่สุด

เมื่อผู้เขียนได้ศึกษาเนื้อหาทั้งสภาพปัญหาและแนวทางปฏิบัติที่ดีต่อการรับมือมัลแวร์เรียกค่าไถ่แล้ว มีข้อเสนอแนะ ดังต่อไปนี้

1) การจัดทำระบบรับแจ้งเหตุฉ้อโกงทางอินเตอร์เน็ตจำต้องกระทำอย่างเร่งด่วน ระบบนี้ต้องเกิดจากหน่วยงานภาครัฐร่วมกับภาคเอกชนในการสอดส่องธุรกรรมทางอินเตอร์เน็ต หน่วยงานตำรวจต้องเป็นกลไกพื้นฐานสำหรับขับเคลื่อน ข้อมูลที่ได้จากภาคปฏิบัติต้องถูกนำมาวิเคราะห์และเชื่อมโยงกับฐานข้อมูลอาชญากรรมของประเทศ ประโยชน์ที่ได้จะทำให้สถานีตำรวจสามารถเริ่มดำเนินการตั้งต้นคดีด้วยข้อมูลครบถ้วนและรวดเร็ว

ผู้เสียหายในฐานะผู้แจ้งได้นำข้อมูลเข้าสู่ระบบในทันทีซึ่งจะถูกนำไปวิเคราะห์หากความเชื่อมโยงกับคดีที่คล้ายคลึงกันที่ปรากฏในฐานข้อมูล

2) การให้ความรู้ถึงความตระหนักในการใช้สื่อสังคมออนไลน์และระบบบริการทางอินเตอร์เน็ต เริ่มต้นที่ชื่ออีเมล์ติดต่อสื่อสารงานธุรกิจและธุรกรรมออนไลน์ต้องใช้ความระมัดระวังในการแบ่งปันข้อมูลที่เป็นส่วนบุคคล การสร้างความตระหนักรับรู้นี้ต้องได้รับการถ่ายทอดไปสู่ประชาชนทุกเพศทุกวัย การคิดวิเคราะห์เสมอเมื่อต้องใช้งานระบบสื่อสารทั้งทางอีเมล์และทางสื่อสังคมออนไลน์ต้องระมัดระวังสิ่งแปลกปลอมที่แฝงมา

3) หน่วยงานที่มีหน้าที่กำกับดูแลการรักษาความปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายต้องเร่งกำหนดกรอบแนวทางปฏิบัติที่ได้มาตรฐาน ผลิตภัณฑ์และบริการด้านความปลอดภัยต้องคำนึงถึงภาระต้นทุนของธุรกิจขนาดย่อม การเข้าถึงบริการรักษาความปลอดภัยด้านระบบคอมพิวเตอร์ต้องสร้างความหลากหลายให้ผู้ขอใช้บริการมีตัวเลือกที่เหมาะสม

4) ผู้ให้บริการธุรกิจดิจิทัลต้องตระหนักไว้เสมอว่าเว็บไซต์และโมบายแอพพลิเคชั่นเป็นเป้าหมายหลักของคนร้าย รูปแบบของการโจมตีไซเบอร์มักจะล่อลวงผู้ใช้ให้ตกหลุมพรางและนำไปสู่การติดตั้งมัลแวร์ ดังนั้นระบบตรวจจับและคัดกรองสิ่งแปลกปลอมที่ดีบนสภาพแวดล้อมของผู้ให้บริการจึงเป็นสิ่งสำคัญต่อการลดความเสียหายที่เกิดขึ้นได้

บรรณานุกรม

Thailand Computer Emergency Response Team. (2018). ThaiCERT Annual Report 2017-2018. Bangkok, Thailand: Electronic Transactions Development Agency (ETDA). (In Thai)

INTERPOL Global Complex for Innovation. (2020). ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk. Singapore: INTERPOL.

Teelawittayakul, S. (2019). *Ransomware Detection Using Machine Learning Techniques with Ransomware Attack Samples*. Thesis of the Degree of Master of Science in Data Communication and Networking, King Mongkut’s University of Technology North Bangkok. (in Thai)

National Fraud & Cyber Crime Reporting Centre. (2018, January 19). RansomAware. ActionFraud. Retrieved October 1, 2020 from https://www.actionfraud. police.uk/campaign/ransomaware

No More Ransom. (n.d). About the Project. Retrieved 1 October 2020 from https://www.nomoreransom.org/en/about-the-project.html

Unnoiy-Pol, C., Kulnites, N., & Wongsongja, N. (2018*). The study’s framework for the significant impacts of cybercrime towards national security, public safety, national economic security, and infrastructure serving public interest*. Paper presented at the Proceeding of Graduate School Conference 2018, Suan Sunandha Rajabhat University, Bangkok, Thailand. (in Thai)

Liangbunprokong, C. (2012). *Classification of malware families based on N-grams sequential pattern features.* Thesis of the Degree of Master of Science in Information Technology Management, National Institute of Development Administration, Bangkok. (in Thai)

Thailand Computer Emergency Response Team. (2017, June 27). Ransomware Alert: Petya a new specie of malware which spreads the same way as WannaCry by encrypting an entire disk. Retrieved October 1, 2020, from https://www.thaicert.or.th/alerts/user/2017/al2017us002.ht ml (in Thai)

Thailand Computer Emergency Response Team. (2017, May 13). Watch out: WannaCry Ransomware ransomware spreads through Windows vulnerabilities, update immediately. Retrieved October 1, 2020, from https://www.thaicert.or.th/alerts/user/2017/al2017us001.html (in Thai)

Mahidol University, Nakhonsawan Campus Project. (2020, September 11). Watch out! Ransomware a Severe Cyber Attack. Retrieved October 1, 2020, from https://na.mahidol.ac.th/medical center/2020/09/11/ransomware/ (in Thai)

Cyber Security Plan. (2020, September 14). Spade Ransomware. Retrieved October 2, 2020, from https://webcache.googleusercontent.com/search?q=cache:1_ui7jHCTEYJ:https://www.cybersecurityplan.org/spade-ransomware/+&cd=4&hl=en&ct=clnk&gl=th

Sonic Wall. (2020, August 14). VoidCrypt Ransomware Actively Spreading in the Wild. Retrieved October 2, 2020, from https://securitynews.sonicwall.com/xmlpost/voidcrypt-ransomware-actively-spreading-in-the-wild/

Thairath Online. (2017, May 20). Alert! The 191 Centre was attacked by 'ransomware', many people could not report. *Thairath.* Retrieved from https://www.thairath.co.th/news/crime/947410 (in Thai)

Technology Crime Suppression Division. (n.d.). Report a Lead/Crime. Retrieved October 1, 2020 from https://tcsd.go.th/report-a-lead-2/?lang=en

1212 Online Complaint Center. (n.d.). Report a Complaint. Retrieved October 1, 2020 from https://tcsd.go.th/report-a-lead-2/?lang=en

Lipson, F. (2019, September 27). Exclusive: scam victims ignored by police fraud reporting system. In Which. Retrieved October 2, 2020, from https://www.which.co.uk/news/2019/09/ exclusive-scam-victims-ignored-by-police-fraud-reporting-system/