แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรีอยุธยา กรณีศึกษาคริปโตล็อคเกอร์แรนซัมแวร์

โดย
พิทยา นครไทย

มหาวิทยาลัยรังสิต Rangsit University

วิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี

บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต
ปีการศึกษา 2567

A GUIDELINE FOR RANSOMWARE DETECTION AND PREVENTION ON INDUSTRIAL CONTROL SYSTEMS IN THE FACTORIES PHRANAKORN SRI AYUTTHAYA A CASE STUDY CRYPTOLOCKER RANSOMWARE

BY

PHITAYA NAKHONTHAI

มหาวิทยาลัยรังสิต Rangsit University

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR

THE DEGREE OF MASTER OF SCIENCE IN INFORMATION MANAGEMENT TECHNOLOGY

COLLEGE OF DIGITAL INNOVATION TECHNOLOGY

GRADUATE SCHOOL, RANGSIT UNIVERSITY

ACADEMIC YEAR 2024

วิทยานิพนธ์เรื่อง

แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุม
อุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรีอยุธยา
กรณีศึกษาคริปโตล็อคเกอร์แรนซัมแวร์

โดย

พิทยา นครไทย

ได้รับการพิจารณาให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ

มหาวิทยาลัยรังสิต
ปีการศึกษา 2567

รศ. ดร.ปริญญา สงวนสัตย์
ประธานกรรมการสอบ

ผศ. ดร.ชุติมา พิศาลย์
กรรมการ

รศ. ดร.คริชณะ ฉิมมณี
กรรมการและอาจารย์ที่ปรึกษา

บัณฑิตวิทยาลัยรับรองแล้ว

(ศ. ดร.สื่อจิตต์ เพ็ชร์ประสาน)
คณบดีบัณฑิตวิทยาลัย
24 กุมภาพันธ์ 2568

มหาวิทยาลัยรังสิต Rangsit University

Thesis entitled

A GUIDELINE FOR RANSOMWARE DETECTION AND PREVENTION ON INDUSTRIAL CONTROL SYSTEMS IN THE FACTORIES PHRANAKORN SRI AYUTTHAYA A CASE STUDY CRYPTOLOCKER RANSOMWARE

by

PHITAYA NAKHONTHAI

was submitted in partial fulfillment of the requirements

for the degree of Master of Science in Information Management Technology

Rangsit University

Academic Year 2024

Prof. Parinya Sanguansat, Ph.D.
Examination Committee Chairperson

Asst. Prof. Chutima Pisan, Ph.D.
Member

Assoc. Prof. Krishna Chimmanee, Ph.D.
Member and Advisor

Approved by Graduate School

(Prof. Suejit Pechprasarn, Ph.D.)
Dean of Graduate School
February 24, 2025

มหาวิทยาลัยรังสิต Rangsit University

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลุล่วงได้ด้วยความกรุณาอย่างสูงจาก รองศาสตราจารย์ ดร.ศริชณะ ฉิมมณี อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่สละเวลาอันมีค่าให้คำแนะนำปรึกษาตลอดระยะเวลาที่ผ่านมา รวมทั้ง ผู้ช่วยศาสตราจารย์ ดร.ชุติมา พิศาลย์ และ รองศาสตราจารย์ ดร.ปริญญา สงวนสัตย์ คณะกรรมการสอบ ที่ได้ให้คำแนะแนวทางปรับปรุงแก้ไขทำวิทยานิพนธ์ให้มีความถูกต้องและสมบูรณ์มากยิ่งขึ้น ซึ่งผู้วิจัยรู้สึกซาบซึ้งในความกรุณาเป็นอย่างยิ่ง และขอขอบคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ผู้วิจัยขอขอบคุณคณาจารย์ผู้สอน คณาจารย์ประจำหลักสูตรหลักสูตรวิทยาศาตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต ทุกท่านที่ได้อบรมสั่งสอนให้ความรู้เป็นอย่างดี และให้ความช่วยเหลือและให้คำแนะนำต่าง ๆ ในการทำวิทยานิพนธ์นี้จนสำเร็จลุล่วงไปด้วยดี

ผู้วิจัยขอกราบบูชาพระคุณ บิดา มารดา ผู้ให้กำเนิดและเลี้ยงดูและอบรมสั่งสอนให้ข้าพเจ้าได้ตระหนักถึงคุณธรรมและศีลธรรมอันดี ตระหนักถึงคุณค่าของความรู้และเป็นผู้ให้การศึกษาและคำนึงถึงความสำคัญในการศึกษาของข้าพเจ้า จนทำให้ประสบผลสำเร็จในการศึกษาครั้งนี้

คุณความดีและคุณค่าจากการสร้างสรรค์องค์ความรู้อันพึงมีจากการทำวิทยานิพนธ์ฉบับนี้ ขอมอบเป็นเครื่องบูชาพระคุณ แด่ บุพการี ทุกท่าน และผู้มีพระคุณทุกท่าน

พิทยา นครไทย

ผู้วิจัย

มหาวิทยาลัยรังสิต Rangsit University

6406778 : พิทยา นครไทย

ชื่อวิทยานิพนธ์ : แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรีอยุธยา กรณีศึกษา คริปโตล็อคเกอร์แรนซัมแวร์

หลักสูตร : วิทยาศาตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษา : รศ. ดร.คริชณะ ฉิมมณี

บทคัดย่อ

ปัจจุบันการปฏิวัติอุตสาหกรรมครั้งที่ 5 ระบบควบคุมในโรงงานอุตสาหกรรม เชื่อมต่อผ่านอินเตอร์เฟสเครือข่ายที่หลากหลายในการเชื่อมต่อระหว่างคอมพิวเตอร์ควบคุมเครื่องจักรเพื่อสื่อสารข้อมูลการผลิต ซึ่งได้นำระบบอัจฉริยะ และหุ่นยนต์ร่วมปฏิบัติช่วยพัฒนากระบวนการผลิตให้มีประสิทธิภาพ และมีความแม่นยำสูงมากขึ้น ถือเป็นปัจจัยสำคัญในการขับเคลื่อนให้เกิดประสิทธิภาพ และส่งผลให้การผลิตมีข้อผิดพลาดที่ลดลง ด้วยเหตุนี้ระบบควบคุมในโรงงานอุตสาหกรรมจึงกลายเป็นหนึ่งในเป้าหมายหลัก จากการโจมตีจากมัลแวร์เรียกค่าไถ่ ซึ่งเพิ่มขึ้นเป็นจำนวนมากในปัจจุบัน ทำให้การดำเนินงานหลายองค์กรในส่วนสายการผลิตในระบบควบคุมในโรงงานอุตสาหกรรมได้รับผลกระทบต้องหยุดชะงักลง

ดังนั้น บทความวิจัยฉบับนี้เป็นงานวิจัยเชิงผสานวิธี ทั้งการวิจัยเชิงคุณภาพ และการวิจัยเชิงปริมาณ โดยใช้ 1) การวิจัยเอกสาร 2) การวิจัยเชิงทดลองจริง เพื่อวิเคราะห์ขั้นตอนการโจมตีในระบบควบคุมในโรงงานอุตสาหกรรม ของมัลแวร์เรียกค่าไถ่ โดยใช้กรอบแนวคิดไมโครซอฟท์ และไมเตอร์แอทแทค และ 3) การจัดกลุ่มสนทนาเฉพาะประเด็น โดยใช้กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์จากแนวทางของ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกา เพื่อหาแนวทางป้องกันตลอดจนข้อปฏิบัติในการรับมือในกรณีที่ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรม

(วิทยานิพนธ์มีจำนวนทั้งสิ้น 125 หน้า)

คำสำคัญ: ระบบควบคุมอุตสาหกรรม, มัลแวร์เรียกค่าไถ่, เอ็นไอเอสที

ลายมือชื่อนักศึกษา ..... ลายมือชื่ออาจารย์ที่ปรึกษา.....

6406778 : Phitaya Nakhonthai

Thesis Title : A Guideline for Ransomware Detection and Prevention on Industrial Control Systems in the Factories Phranakorn Sri Ayutthaya a Case Study CryptoLocker Ransomware

Program : Master of Science in Information Management Technology, College of Digital Innovation Technology

Thesis Advisor : Assoc. Prof. Krishna Chimmanee, Ph.D.

Abstract

In the current era of the Fifth Industrial Revolution, industrial control systems in factories are interconnected via diverse network interfaces, enabling seamless communication between control computers and machinery for the exchange of production data. These systems integrate advanced intelligent technologies and collaborative robots, which optimize production processes by enhancing efficiency and precision. Such innovations have become pivotal in boosting productivity while minimizing production errors. As a result, industrial control systems have emerged as prime targets for ransomware attacks, which have seen a significant increase in recent years. These attacks have disrupted the operations of numerous organizations within the manufacturing sector, often bringing production control systems to a standstill.

This research article employed a mixed-methods approach, incorporating both qualitative and quantitative research methods. The methodology consisted of three main components: 1) Documentary Research, 2) a True Experiment for analyzing the stages of ransomware attacks within industrial control systems using the Microsoft and MITRE ATT&CK frameworks, and 3) a Focus Group, applying a cybersecurity framework based on guidelines from the National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce. In this context, this study aimed to identify preventive measures and response strategies for industrial control systems in the event of ransomware attacks.

(Total 125 pages)

Keywords: Industrial Control Systems, Ransomware, NIST

Student's Signature ..... Thesis Advisor's Signature .....

สารบัญ

มหาวิทยาลัยรังสิต Rangsit University

สารบัญ (ต่อ)

มหาวิทยาลัยรังสิต Rangsit University

สารบัญ (ต่อ)

สารบัญตาราง

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป (ต่อ)

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology: IT) และอินเทอร์เน็ตนับว่าเป็นเครื่องมือเข้ามามีบทบาทสำคัญอย่างยิ่งในการขับเคลื่อนภารกิจหลักขององค์กรต่าง ๆ ทั่วโลก โดยเฉพาะอย่างยิ่งองค์กรที่เป็นผู้นำในอุตสาหกรรมต่าง ๆ รวมถึงหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ตามที่ อนาวิล แก้วสอาด และณัฐวี อุตกฤษฎ์ (2564) ได้ศึกษาไว้ว่าในองค์กรด้านการรักษาความปลอดภัยเป็นสิ่งสำคัญอย่างยิ่งในส่วนของระบบเครือข่าย (Network) เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์ (Computer) ภายในสำนักงาน และเครื่องจักรที่ใช้ในการควบคุมจากเครื่องคอมพิวเตอร์ (Computer-Controlled Machine) ในกระบวนการเทคโนโลยีและอุปกรณ์ด้านการผลิต (Operational Technology: OT) ในระบบควบคุมในโรงงานอุตสาหกรรมผลิตชิ้นส่วนอิเล็กทรอนิกส์ จากรายงานการวิเคราะห์สถิติการโจมตีด้วย ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) ในระบบควบคุมในอุตสาหกรรม (Industrial Control Systems: ICS) หรือเทคโนโลยีด้านการปฏิบัติการ โดย Alamri (2022) จากเว็บไซต์ดาร์กอต (Dragos) ได้รายงานสถิติการโจมตีจากมัลแวร์ (Malware) เรียกค่าไถ่ในไตรมาสที่ 2 ของ พ.ศ. 2565 พบว่า ร้อยละ 86 มุ่งเป้าโจมตีไปที่ภาคการผลิตในโรงงานอุตสาหกรรม ซึ่งเพิ่มขึ้นเป็นจำนวนมากเมื่อเทียบกับปีที่ผ่านมา ซึ่งแสดงให้เห็นว่ากลุ่มซอฟต์แวร์เรียกค่าไถ่มีแนวโน้มที่อาจก่อให้เกิดความเสี่ยงต่อการหยุดชะงักในการปฏิบัติงานของสายการผลิตในระบบควบคุมในโรงงานอุตสาหกรรม เห็นได้ชัดว่าการโจมตีของซอฟต์แวร์เรียกค่าไถ่ในหลายครั้งที่ผ่านมา ทำให้การดำเนินงานหลายองค์กรในส่วนสายการผลิตในระบบควบคุมในโรงงานอุตสาหกรรมได้รับผลกระทบต้องหยุดชะงักลง

จากสถานการณ์การแพร่ระบาดของเชื้อไวรัสโคโรน่า COVID-19 ส่งผลให้บริษัทผู้ผลิตชิ้นส่วนอิเล็กทรอนิกส์ ได้ปรับเปลี่ยนให้บุคลากรขององค์กรสามารถทำงานจากที่พักได้ ด้วยการเชื่อมต่อระยะไกลผ่านระบบเครือข่ายส่วนบุคคลเสมือน (VPN) ในการเข้าถึงข้อมูลสำคัญภายใน

ระบบเครือข่ายขององค์กร ผู้ดูแลระบบเครือข่ายมีการอนุญาตจำนวนผู้ใช้งานเพิ่มขึ้นจากรายงานสถิติประจำเดือน การรับส่งรายงานผ่านอีเมล (Email) จากภายนอกเครือข่ายเพิ่มมากขึ้น ผู้ใช้งานบางส่วนได้ทำการเข้าถึงเครื่องคอมพิวเตอร์ด้วยการเชื่อมต่อผ่านรีโมทเดสท็อปคอนเนคชั่น (Remote Desktop Connection) หรือ เรียกย่อว่า อาร์ดีพี (RDP) ซึ่งจากมาตรการตามแผนการป้องกันในสถานการณ์โควิดในส่วนของแผนงานติดตั้งเครื่องจักร องค์กรจะต้องนำส่งคอมพิวเตอร์ระบบควบคุมเครื่องจักรไปยังผู้ขายเพื่อทำการติดตั้งโปรแกรม พร้อมให้บริการบำรุงรักษาคอมพิวเตอร์ระบบควบคุมเครื่องจักร จากบริการหลังการขายโดยให้บริการสนับสนุนผ่านการเข้าถึงเครือข่ายจากระยะไกลเป็นจำนวนเพิ่มขึ้น ซึ่งจากปีที่ผ่านมาตรวจพบว่า มีเครื่องคอมพิวเตอร์คอมพิวเตอร์ระบบควบคุมที่เชื่อมต่อกับเครื่องจักร ได้ถูกโจมตีจากซอฟต์แวร์ประสงค์ร้าย (Malicious Software: Malware) ประเภทหนึ่งที่โจมตีด้วยการเข้ารหัสข้อมูล เพื่อเรียกค่าไถ่ในการปลดล็อคข้อมูล ซึ่งจากการตรวจสอบเบื้องต้นพบว่าไฟล์ข้อมูลเกิดความเสียหายจนไม่สามารถกู้คืนสภาพไฟล์ได้ จากรายงานของผู้ดูแลความมั่นคงปลอดภัยระบบสารสนเทศในองค์กร พบว่าเป็นการโจมตีในรูปแบบประมวลผลโปรแกรมแบบอัตโนมัติตามตารางเวลาที่กำหนด (Schedule Task) บนระบบปฏิบัติการวินโดวส์ และมีการแสดงป๊อบอับ (Pop-up) เรียกค่าไถ่ จากค้นหาข้อมูลพบว่าเป็นมัลแวร์เรียกค่าไถ่ ที่ชื่อว่า คริปโตล็อคเกอร์ (Cryptolocker) ดังนั้น ผู้วิจัยจึงมีความสนใจที่จะศึกษาเพื่อหาแนวทางรักษาความมั่นคงปลอดภัยเพื่อป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมของอุตสาหกรรม กรณีศึกษาในโรงงานอุตสาหกรรมผลิตชิ้นส่วนอิเล็กทรอนิกส์ในเขตพื้นที่จังหวัดอยุธยาแห่งหนึ่งที่ได้ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่

งานวิจัยฉบับนี้เป็นงานวิจัยเชิงผสานวิธี (Mixed Method Research) ทั้งการวิจัยเชิงคุณภาพ (Qualitative Research) และการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้ 1) การวิจัยเอกสาร (Documentary Research) 2) การวิจัยเชิงทดลองจริง (True Experiment) และ 3) การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group เป็นเครื่องมือการวิจัย ในการวิเคราะห์การโจมตีจากโปรแกรมประสงค์ร้าย ประเภทเรียกค่าไถ่ ด้วยกรอบแนวทางของไมโครซอฟท์ (Microsoft Framework) และ ไมเตอร์แอทแทค (MITRE ATT&CK Framework) โดยใช้กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์จากแนวทางของ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกา (NIST) ซึ่งเป็นที่นิยมใช้อ้างอิงเป็นมาตรฐานสากลในปัจจุบัน เพื่อหาแนวทางป้องกันมัลแวร์เรียกค่าไถ่ตลอดจนข้อปฏิบัติในการรับมือในกรณีที่ถูกโจมตี

มหาวิทยาลัยรังสิต Rangsit University

จากมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรม และเพื่อเป็นโยชน์และเติมเต็มแนวทางการป้องกันให้กับผู้ดูแลระบบรักษาความมั่นคงปลอดภัย

1.2 วัตถุประสงค์การวิจัย

1.2.1 ศึกษาภัยคุมคามจากมัลแวร์เรียกค่าไถ่ในภาคอุตสาหกรรมการผลิต (Manufacturing) ในระบบควบคุมในโรงงานอุตสาหกรรม โดยใช้ข้อมูลจากการวิจัยเชิงเอกสาร จำนวน 3 กรณีศึกษา

1.2.2 ศึกษาภัยคุมคามจากมัลแวร์เรียกค่าไถ่ในภาคอุตสาหกรรมการผลิต (Manufacturing) ในระบบควบคุมในโรงงานอุตสาหกรรม โดยใช้ข้อมูลจากการวิจัยเชิงทดลอง จำนวน 1 กรณีศึกษา

1.2.3 วิเคราะห์ขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่ในระบบควบคุมในอุตสาหกรรม โดยใช้กรอบแนวคิดไมโครซอฟท์ และไมเตอร์แอทแทค (MITRE ATT&CK)

1.2.4 เพื่อศึกษาหาแนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่เหมาะสมของระบบควบคุมในอุตสาหกรรม จากแนวทางของนิสต์ (NIST) โดยใช้ข้อมูลจากการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

1.3 ขอบเขตของการวิจัย

1.3.1 ขอบเขตด้านเนื้อหา

1.3.1.1 ศึกษาลักษณะการโจมตีไวรัสเรียกค่าไถ่คริปโตล็อคเกอร์จากเหตุการณ์ที่เกิดจริง โดยใช้การวิเคราะห์ทางนิติวิทยาศาสตร์ทางดิจิทัลของการโจมตีในระบบควบคุมของอุตสาหกรรมจากกรอบแนวทางของไมโครซอฟท์ เปรียบเทียบกับ กลยุทธ์ เทคนิค และกระบวนการทำงานของแฮกเกอร์ด้วยไมเตอร์แอทแทค (MITRE ATT&CK)

1.3.1.2 ใช้กรอบแนวทางจากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ สหรัฐฯ (NIST) ในการป้องกันมัลแวร์เรียกค่าไถ่ ประกอบด้วย 5 ขั้นตอนหลัก ซึ่งได้แก่ (1) การกำหนดมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ (2) การปกป้องทรัพย์สินสารสนเทศ (3) การตรวจจับภัยคุกคามไซเบอร์ (4) การวางแผนรับมือกับภัยคุกคาม และ (5) การกู้คืนข้อมูลหลังเกิดเหตุภัยคุกคามไซเบอร์

มหาวิทยาลัยรังสิต Rangsit University

1.3.1.3 การวิจัยในครั้งนี้เป็นการวิจัยเชิงผสานวิธี (Mixed Methods Research) โดยใช้

1) การวิจัยเชิงเอกสาร (Documentary Research)

2) การวิจัยเชิงทดลอง (True Experiment)

3) การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

1.3.2 ขอบเขตด้านเวลา

ระยะเวลาที่ใช้ในการทำการวิจัยตั้งแต่เดือนพฤษภาคม พ.ศ. 2565 ถึง เดือนพฤษภาคม พ.ศ. 2566 รวม ระยะเวลา 12 เดือน

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 สร้างความตระหนักรู้ถึงภัยคุกคามจากมัลแวร์เรียกค่าไถ่

1.4.2 วิเคราะห์ขั้นตอนการโจมตีมัลแวร์เรียกค่าไถ่

1.4.3 แนวทางการรักษาความมั่นคงปลอดภัยของระบบให้กับผู้ดูแลระบบเครือข่ายทางไซเบอร์ในระบบควบคุมในอุตสาหกรรม

1.5 นิยามศัพท์

ระบบควบคุมในอุตสาหกรรม (Industrial Control Systems: ICS) เป็นระบบที่ใช้ควบคุมเครื่องจักรในโรงงานอุตสาหกรรมเปรียบเสมือนสมองของโรงงานที่คอยสั่งการเครื่องจักรต่าง ๆ เพื่อให้สามารถดำเนินงานต่อไปได้ ปัจจุบันได้ถูกทำให้มีการใช้งานง่ายมากขึ้น มีความเป็นอัตโนมัติมากขึ้น รวมถึงสามารถควบคุมจากที่ไหนก็ได้และคาดว่าในอนาคตจะมีการพัฒนาไปอย่างก้าวกระโดดด้วยการประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) และระบบการทำงานอัติโนมัติ (Automation) ที่ดียิ่งขึ้น (Kamalanathan, Sethuraman, Krishanshree, & Venkat , 2022)

การวิเคราะห์ทางนิติวิทยาศาสตร์ทางดิจิทัล (Digital Forensic Analysis) การพิสูจน์หลักฐานทางคอมพิวเตอร์ การเก็บหลักฐาน, การค้นหา, วิเคราะห์ และการนำเสนอหลักฐานทาง

ดิจิทัลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์ การวิเคราะห์ทางนิติวิทยาศาสตร์ทางดิจิทัล เป็นการจัดเก็บรวบรวม และวิเคราะห์หลักฐานทางดิจิตอล ด้วยกระบวนการที่น่าเชื่อถือเพื่อให้สามารถนำข้อเท็จจริงจากการวิเคราะห์หลักฐานนำไปใช้เป็นหลักฐานได้ (Andrew, 2023)

มัลแวร์ (Malware: Malicious Software) คือ โปรแกรมหรือไฟล์ใด ๆ เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อประสงค์ร้ายต่อคอมพิวเตอร์,เครือข่ายและเซิร์ฟเวอร์ ไม่ว่าจะเป็น ไวรัส (Virus), วอร์ม (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น (สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย, 2566)

การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) หมายถึง ความสามารถของระบบองค์กร หรือบุคคล ในการเตรียมพร้อม รับมือ ปรับตัว และฟื้นฟูจากภัยคุกคามทางไซเบอร์ เพื่อให้สามารถดำเนินงานต่อไปได้อย่างต่อเนื่อง การคืนสภาพให้ระบบกลับมาใช้งานได้ปกติอย่างรวดเร็วและมีประสิทธิภาพตามแผนปฏิบัติงานในกรณีที่เกิดภัยคุกคามทางไซเบอร์ โดยให้ความสำคัญกับการเตรียมพร้อมรับมือทุกส่วนงานที่เกี่ยวข้องกับสถานการณ์ที่อาจเกิดขึ้นตลอดเวลา ซึ่งดังกล่าวมีความแตกต่างจาก "ความมั่นคงปลอดภัยทางไซเบอร์" ที่ได้มุ่งเน้นในด้านการป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ ตั้งแต่แรก (จันทกานต์ ผลพล, 2563)

National Institute of Standards and Technology (NIST) **หรือ นิสต์** เป็นสถาบันมาตรฐาน และ เทคโนโลยีแห่งชาติ เป็นหน่วยงานหนึ่งของกระทรวงพาณิชย์แห่งสหรัฐอเมริกา (คริชณะ ฉิมมณี และมณีสุข โชติรุ่งรัตน์, 2564)

กลยุทธ์ เทคนิคและกระบวนการทำงานของแฮกเกอร์ด้วยไมเตอร์แอทแทค (MITRE ATT&CK) ไมเตอร์แอทแทค (Adversarial Tactics, Techniques, and Common Knowledge : MITRE ATT&CK) เป็นฐานข้อมูลความรู้และแบบจำลองที่รวบรวมกลยุทธ์ เทคนิคและกระบวนการ (TTPs) ที่แฮกเกอร์ใช้ในการโจมตีระบบต่าง ๆ ฐานข้อมูลนี้จัดทำโดย MITRE Corporation องค์กรไม่แสวงหาผลกำไรที่มุ่งเน้นการวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (MITRE ATT&CK, 2022)

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 2

ทบทวนวรรณกรรมที่เกี่ยวข้อง

ในบทนี้จะทำการศึกษาเกี่ยวกับแนวคิด ทฤษฎี งานวิจัยที่เกี่ยวข้องของของมัลแวร์เรียกค่าไถ่วิวัฒนาการ วิธีการโจมตี วิธีการป้องกัน แนวโน้มการพัฒนามัลแวร์เรียกค่าไถ่ในอนาคตและบทความที่เกี่ยวข้องในประเทศและต่างประเทศ โดยแบ่งออกเป็นจำนวน 10 หัวข้อได้แก่

2.1 ทฤษฎีมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์

2.2 มัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021

2.3 มัลแวร์เรียกค่าไถ่การโจมตีในระบบควบคุมอุตสาหกรรมที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021

2.4 แอคทีฟไดเรกทอรี่ (Active Directory)

2.5 รีโมทเดสท็อปคอนเนคชั่น (Remote Desktop Connection)

2.6 กรอบแนวคิดของไมโครซอฟท์การโจมตีของมัลแวร์เรียกค่าไถ่

2.7 กลยุทธ์ เทคนิค และกระบวนการทำงานของแฮกเกอร์ด้วยไมเตอร์แอทแทค (MITRE ATT&CK)

2.8 สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกา (NIST)

2.9 งานวิจัยที่เกี่ยวข้อง

2.9.1 บทความวิจัยจากต่างประเทศ

2.9.2 บทความจากเว็บไซต์ต่างประเทศ

2.10 ตารางสรุปบทความที่เกี่ยวข้อง

2.1 ทฤษฎีมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์

Nagaraja and Rubia (2020) ได้กล่าวว่า มัลแวร์เรียกค่าไถ่ (Ransomware) หรือ Malicious Software คือ โปรแกรมอันตรายประเภทหนึ่งที่ออกแบบมาเพื่อสร้างความเสียหาย หรือก่อให้เกิดอันตรายต่ออุปกรณ์ไอที ซึ่งสามารถเข้ารหัสข้อมูลที่เก็บไว้ในเครือข่ายคอมพิวเตอร์โดยมีจุดประสงค์เพื่อเรียกรับเงินจากกลุ่มเป้าหมาย การโจมตรีของมัลแวร์เรียกค่าไถ่เพิ่มขึ้นทุกวัน

เช่นเดียวกันกับมัลแวร์เรียกค่าไถ่ที่มีความหลากหลายจากจำนวนเหตุการณ์จากรายงานในปีที่ผ่านมาได้เพิ่มขึ้นเป็นจำนวนมาก โครงข่ายการเชื่อต่อที่เพิ่มขึ้น การเปลี่ยนแปลงดิจิทัลได้อำนวยความสะดวกให้อาชญากรทางไซเบอร์ได้ออกแบบ เปิดการโจมตีทางทางไซเบอร์ขนาดใหญ่ที่กำหนดเป้าหมายบุคคลและองค์กรทั่วโลก ในขณะที่บุคลลากรขาดความรู้และองค์กรขาดความตระหนักทำให้การโจมตีเหล่านี้สามารถหลีกเลี่ยงการรักษาความปลอดภัยขั้นพื้นฐานได้

HelpRansomware (2022) คริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่ในปี พ.ศ. 2556 ได้พบการโจมตีทั้งระบบซึ่งได้รับผลกระทบหลายบริษัทถูกโจมตีแล้ว และการใช้อัลกอริทึม (Algorithm) การเข้ารหัสที่หลากหลาย มัลแวร์เรียกค่าไถ่ได้รับการพัฒนาโดยบิสสิเนสคลับ (Business Club) ซึ่งใช้บ็อตเน็ต Game over Zeus ขนาดใหญ่ที่มีการโจมตรีแล้วแพร่กระจายกว่าล้านรายการ กลุ่มนี้ใช้ประโยชน์จากบ็อตเน็ตเป็นหลักในโจมตี และการฉ้อโกงที่เกี่ยวข้องกับธนาคาร คริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่เป็นมัลแวร์ประเภทหนึ่งที่พบการแพร่ระบาดในวงกว้าง และทำให้เกิดมัลแวร์เรียกค่าไถ่สายพันธุ์อื่น ๆ แพร่ระบาดตามมาเป็นจำนวนมากตั้งแต่ช่วงปลายปี พ.ศ. 2556 เป็นมัลแวร์เรียกค่าไถ่ที่กำหนดเป้าหมายระบบปฏิบัติการ ไมโครซอฟท์วินโดวส์ (Microsoft Windows) มัลแวร์จะเลือกเข้ารหัสข้อมูล ใช้การเข้ารหัสคีย์สาธารณะอาร์เอสเอ (RSA) เพื่อล็อคไฟล์ ซึ่งเป็นหนึ่งในไวรัสที่กระจายอย่างมีประสิทธิภาพมากที่สุด แฮกเกอร์ (Hackers) ได้ผสมผสานเทคนิคต่าง ๆ เข้าด้วยกันเพื่อเผยแพร่ พบว่าคริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่มี 12 เวอร์ชัน (Versions) ได้แก่ CryptoLocker Virus, CryptoLocker- v3 , Cryptographic Locker, PCLock Ransomware, CryptoTorLocker2 0 1 5 , Crypt0 Ransomware, Cryptolocker Infected Your Computer! Ransomware, CryptoLocker 5.1 Ransomware virus, Cryptolocker3 Ransomware Virus, MNS Cryptolocker, CryptoLockerEU Ransomware Virus, และ CryptON ผู้สร้างมัลแวร์ได้รวมเทคนิคต่าง ๆ เพื่อเผยแพร่ มัลแวร์เรียกค่าไถ่ประเภทนี้ มีการสร้างเวอร์ชันใหม่โดยที่ไม่จำเป็นต้องเกี่ยวข้องกับต้นฉบับ คริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่สามารถโจมตีเข้าสู่เครือข่ายที่มีการป้องกันผ่านเวกเตอร์ต่าง ๆ รวมถึงอีเมล แชร์ไฟล์ และการดาวน์โหลด ตัวแปรใหม่ประสบความสำเร็จในการโจมตีจากการหลีกเลี่ยงของเทคโนโลยีป้องกันไวรัสและไฟร์วอลล์

คริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่พบว่ามีการสร้างเวอร์ชันใหม่โดยที่ไม่จำเป็นต้องเกี่ยวข้องกับต้นฉบับ ในการโจมตีสามารถโจมตีเข้าสู่เครือข่ายที่มีการป้องกันผ่านเวกเตอร์ต่าง ๆ ได้แก่ อีเมล แชร์ไฟล์ และการดาวน์โหลด จะทำการเข้ารหัสไฟล์หรือข้อมูลเพื่อล็อคไฟล์ ของเหยื่อ

เพื่อไม่ให้เข้าถึงได้เว้นแต่เหยื่อจะจ่ายค่าไถ่ที่เรียกร้อง ตามทฤษฎีแล้ว เมื่อเหยื่อชำระเงินจะได้รับคีย์การเข้ารหัสเพื่อเข้าถึงไฟล์หรือข้อมูลที่ผู้โจมตีเข้ารหัสไว้ ในการโจมตีโดยคริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่เหยื่อจะถูกล็อกออกจากอุปกรณ์ของตนและไม่สามารถเข้าสู่ระบบได้ เหยื่อจะได้รับข้อความเรียกค่าไถ่บนหน้าจอแจ้งว่าพวกเขาถูกล็อกและรวมถึงคำแนะนำสำหรับวิธีจ่ายค่าไถ่เพื่อให้สามารถเข้าถึงระบบได้อีกครั้ง

2.2 มัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021

จากตารางที่ 2.1ได้แสดงถึงมัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021

ตารางที่ 2.1 แสดงมัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021

ชื่อมัลแวร์ / ปี ค.ศ.	เป้าหมายการโจมตีหรือผลกระทบ
Bit Cryptor and Coin Vault, 2015	มัลแวร์เรียกค่าไถ่ทั้งสองนี้ได้มีการโจมตีและแพร่ไปยังหลายพันเครื่อง ก่อนที่ผู้เขียนสองคนที่ถูกกล่าวหาจะถูกจับกุมที่ประเทศเนเธอร์แลนด์ในปี ค.ศ. 2015 ในระหว่างการสืบสวน บริษัทแอนตี้มัลแวร์ของรัสเซีย Kaspersky สามารถจับคีย์ถอดรหัสทั้งหมด 14,000 คีย์ ที่ซึ่งจำเป็นในการถอดรหัสไฟล์ของเหยื่อ ภายหลัง Kaspersky ได้สร้างเครื่องมือที่สามารถดาวน์โหลดได้ฟรี เพื่อยกเลิกความเสียหายที่เกิดขึ้นจากทั้ง Bit Cryptor และ Coin Vault (Christiaan, 2018)
TeslaCrypt, 2015	เทสล่าเครปต์ (TeslaCrypt) ปรากฏขึ้นในปี ค.ศ. 2015 โดยเริ่มแรกมุ่งเป้าไปที่การเข้ารหัสข้อมูลบันทึกและไฟล์ต่าง ๆ ที่สร้างโดยเกมคอมพิวเตอร์ยอดนิยม เช่น Call of Duty และ World of Warcraft ซึ่งผู้โจมตีจะเรียกค่าไถ่เป็นเงินสกุลดิจิทัล Bitcoin มูลค่ากว่า 500 ดอลลาร์สหรัฐ TeslaCrypt รุ่นแรกใช้การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) ซึ่งนักวิจัยด้านความปลอดภัยสามารถสร้างเครื่องมือถอดรหัสได้ อย่างไรก็ตาม รุ่นต่อ ๆ มาได้ใช้การเข้ารหัสที่ซับซ้อนมากขึ้น ทำให้เครื่องมือดังกล่าวไม่สามารถถอดรหัสได้ (Loana, 2019)
Locky, 2017	ล็อกกี้ (Locky) ซึ่งปรากฏตัวครั้งแรกในปี ค.ศ. 2017 เป็นมัลแวร์เรียกค่าไถ่ที่มีรูปแบบการทำงานที่ซับซ้อน โดยทั่วไปจะแพร่กระจายผ่านไฟล์แนบไมโครซอฟท์

ตารางที่ 2.1 แสดงมัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021 (ต่อ)

ชื่อมัลแวร์ / ปี ค.ศ.	เป้าหมายการโจมตีหรือผลกระทบ
	ออฟฟิศ (Microsoft Office) ที่ฝังมากับอีเมล เมื่อผู้ใช้เปิดไฟล์ดังกล่าวและคลิกเปิดใช้งานมาโคร (Macro) โดยหลงเชื่อว่าเป็นการแสดงผลเอกสารที่ถูกต้อง ก็เท่ากับเป็นการอนุญาตให้มัลแวร์เริ่มทำงาน จากนั้น Locky จะทำการเข้ารหัสไฟล์ (Loana, 2019)
WannaCry, 2017	วานนาไครย์ (WannaCry) ได้แพร่กระจายไปยังคอมพิวเตอร์มากกว่า 100,000 เครื่อง ในเดือนพฤษภาคม ค.ศ. 2017 ด้วยการใช้ประโยชน์จากช่องโหว่ของวินโดวส์ ที่ออกมา (MS17-010) WannaCry (หรือ WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor) จะทำการเข้ารหัสไฟล์ของคุณ และเก็บไว้เพื่อเรียกค่าไถ่ เป็นเวลาหลายวัน โดยเงินค่าไถ่จะอยู่ที่ประมาณ 0.17 BTC (ประมาณ 300 เหรียญสหรัฐ) ซึ่งเงินค่าไถ่จะเพิ่มขึ้นตามระยะเวลาที่ปล่อยเอาไว้ หลังจากนั้นหนึ่งสัปดาห์ไฟล์ที่ถูกเข้ารหัสจะถูกลบ ไฟล์ที่เข้ารหัสจะมีนามสกุล .WCRY พบว่ามัลแวร์ได้อธิบาย “kill switch functionality” นอกจากนี้ยังมี Wannacry รุ่นใหม่กว่าที่สามารถเห็นได้ทั่วไปในวันอาทิตย์ พร้อมโดเมน kill switch แบบใหม่ (Loana, 2019)
GandCrab, 2018	มัลแวร์เรียกค่าไถ่ GandCrab เป็นกลุ่มไวรัสเข้ารหัสข้อมูล เปิดตัวครั้งแรกในช่วงต้นปี ค.ศ. 2018 และภายในเวลาเพียงหนึ่งปี ก็กลายเป็นภัยคุกคามไซเบอร์ที่อันตรายที่สุดในโลก GandCrab มีหลายเวอร์ชัน เช่น GDCB, KRAB, CRAB virus, GandCrab 2, 3, 4 และ 5 โดยทุกเวอร์ชันใช้การเข้ารหัสแบบ RSA 2048 และ AES 256 โดยจะเปลี่ยนชื่อไฟล์ของเหยื่อด้วยนามสกุลแบบสุ่ม ณ ปัจจุบัน เวอร์ชันที่อันตรายที่สุดคือ GandCrab 5.0.4 และ 5.1 การแพร่กระจายของมัลแวร์นี้ใช้วิธีการที่หลากหลาย เช่น ผ่านชุดโปรแกรม RIG, GradSoft, Magnitude และ Fallout exploit รวมถึง cracks, keygens แม้จะเป็นภัยคุกคามที่ร้ายแรง แต่ทีมวิจัย Bitdefender ร่วมกับตำรวจสากลและตำรวจโรมาเนีย ได้พัฒนาเครื่องมือถอดรหัส GandCrab เวอร์ชันที่ 3 ซึ่งสามารถใช้งานได้กับเวอร์ชัน 1, 4 และ 5.0.1 ถึง 5.1 (Loana, 2019)

ตารางที่ 2.1 แสดงมัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021 (ต่อ)

ชื่อมัลแวร์ / ปี ค.ศ.	เป้าหมายการโจมตีหรือผลกระทบ
Ryuk, 2018	อายิว (Ryuk) ถือเป็นหนึ่งในมัลแวร์เรียกค่าไถ่ยุคแรก ๆ ที่ใช้กลยุทธ์การโจมตีแบบกำหนดเป้าหมาย ถูกค้นพบครั้งแรกในปี ค.ศ. 2018 และได้สร้างมาตรฐานใหม่ให้กับมัลแวร์เรียกค่าไถ่รุ่นต่อ ๆ มา "อายิว" มีชื่อเสียงโด่งดังจากการเลือกโจมตีเป้าหมายระดับสูง ซึ่งรวมถึงอุตสาหกรรมการดูแลสุขภาพที่มีมาตรฐานความปลอดภัยต่ำในปี ค.ศ. 2020 ต่อมาในปี ค.ศ. 2021 "คอนติ" (Conti) ซึ่งเป็นมัลแวร์เรียกค่าไถ่ที่พบมากที่สุดในปีนั้น มีรายงานว่าพัฒนามาจาก "อายิว" (Jackson, 2023)
REvil, 2019	รีอวิล (Revil) เป็นหนึ่งในตระกูล มัลแวร์เรียกค่าไถ่ที่รู้จักกันดีที่สุดในเน็ตกลุ่มมัลแวร์เรียกค่าไถ่ ซึ่งดำเนินการโดยกลุ่ม REvil ที่พูดภาษารัสเซียมาตั้งแต่ปี ค.ศ. 2019 ได้รับผิดชอบต่อการละเมิดครั้งใหญ่มากมาย เช่น Kaseya และ JBS ใช้เทคนิค Double Extortion เพื่อขโมยข้อมูลจากธุรกิจในขณะที่เข้ารหัสไฟล์ด้วย ซึ่งหมายความว่านอกเหนือจากการเรียกค่าไถ่เพื่อถอดรหัสข้อมูลแล้ว ผู้โจมตีอาจขู่ว่าจะเปิดเผยข้อมูลที่ถูกขโมยหากไม่มีการชำระเงินครั้งที่สอง (Jackson, 2023)
DarkSide, 2020	ดาร์กไซด์ (DarkSide) คือมัลแวร์เรียกค่าไถ่ที่ให้บริการในรูปแบบ RaaS (Ransomware-as-a-Service) ซึ่งเริ่มโจมตีองค์กรต่าง ๆ ทั่วโลกตั้งแต่เดือนสิงหาคม ค.ศ. 2020 มัลแวร์นี้ไม่ได้แค่เข้ารหัสข้อมูลของเหยื่อ แต่ยังขโมยข้อมูลจากเซิร์ฟเวอร์ที่ถูกโจมตีด้วย ซึ่งเป็นรูปแบบการโจมตีแบบกำหนดเป้าหมายที่พบได้ในภัยคุกคามไซเบอร์อื่น ๆ ที่คล้ายคลึงกัน (Trend Micro Research, 2021)
LockBit, 2021	ล็อกบิต (LockBit) เวอร์ชัน 2.0 ซึ่งปรากฏขึ้นในเดือนกรกฎาคม ค.ศ. 2021 มีความสามารถในการเข้ารหัสอุปกรณ์ต่าง ๆ ในเครือข่ายวินโดวส์ได้อย่างรวดเร็วโดยอาศัยช่องโหว่ของระบบ Active Directory (AD) ซึ่งทำให้ผู้พัฒนาโปรแกรมนี้กล่าวอ้างว่าเป็นหนึ่งในมัลแวร์เรียกค่าไถ่ที่เร็วที่สุดในขณะนั้น ต่อมาในเดือนตุลาคม ค.ศ. 2021 ได้มีการประกาศล็อกบิตเวอร์ชัน 1.0 ซึ่งแสดงให้เห็นถึงความพยายามในการขยายเป้าหมายการ

ตารางที่ 2.1 แสดงมัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. 2015 ถึง 2021 (ต่อ)

ชื่อมัลแวร์ / ปี ค.ศ.	เป้าหมายการโจมตีหรือผลกระทบ
	โจมตีไปยังระบบปฏิบัติการลีนุข (Linux) อีกด้วย (Megan, 2021)
DearCry, 2021	ไมโครซอฟท์ได้ออกแพตช์เพื่อแก้ไขช่องโหว่ 4 จุด บนเซิร์ฟเวอร์ (Microsoft Exchange) อย่างไรก็ตาม DearCry ซึ่งเป็นมัลแวร์เรียกค่าไถ่ชนิดใหม่ ถูกออกแบบมาเพื่อโจมตีช่องโหว่ดังกล่าวโดยเฉพาะ โดยมัลแวร์จะเข้ารหัสไฟล์บางประเภท หลังจากเข้ารหัสเสร็จสิ้น DearCry จะแสดงข้อความเรียกค่าไถ่ พร้อมแนะนำให้ผู้ใช้ติดต่อผู้โจมตีเพื่อขอวิธีการถอดรหัสไฟล์ (Abrams, 2021)

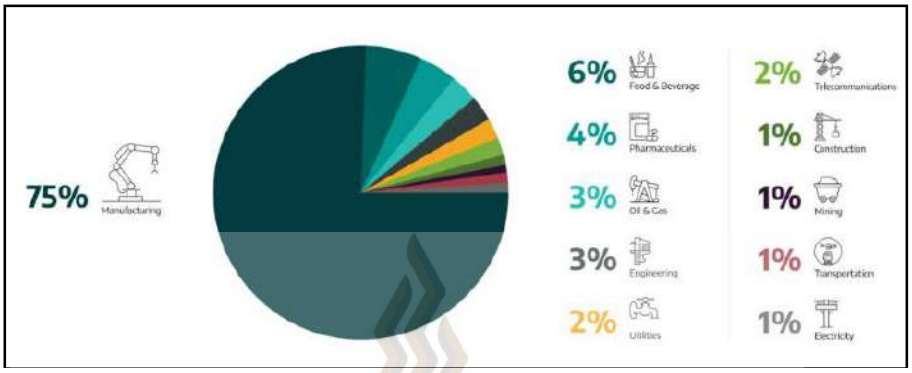
ที่มา: รวบรวมโดยผู้วิจัย, 2566

2.3 มัลแวร์เรียกค่าไถ่การโจมตีในระบบควบคุมอุตสาหกรรมที่สำคัญ ในช่วงปี ค.ศ. 2015 ถึง 2021

ระบบควบคุมในอุตสาหกรรม (Industrial Control Systems: ICS) เป็นระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรมเปรียบเสมือนสมองของโรงงานที่คอยสั่งการเครื่องจักรต่าง ๆ เพื่อให้สามารถดำเนินงานต่อไปได้ ปัจจุบันได้ถูกทำให้มีการใช้งานง่ายมากขึ้น มีความเป็นอัตโนมัติมากขึ้น รวมถึงสามารถควบคุมจากที่ไหนก็ได้ และคาดว่าในอนาคตจะมีการพัฒนาไปอย่างก้าวกระโดดได้อีกแน่นอนด้วยการประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) และระบบการทำงานอัตโนมัติ (Automation) ที่ดียิ่งขึ้น การรักษาความปลอดภัยของเทคโนโลยี (Operational Technology Security) ครอบคลุมระบบหรืออุปกรณ์ที่ตั้งโปรแกรมได้หลากหลายที่โต้ตอบกับสภาพแวดล้อมทางกายภาพ (หรือจัดการอุปกรณ์ที่โต้ตอบกับสภาพแวดล้อมทางกายภาพ) ระบบและอุปกรณ์เหล่านี้ตรวจจับหรือทำให้เกิดการเปลี่ยนแปลงโดยตรงผ่านการตรวจสอบและหรือการควบคุมอุปกรณ์ กระบวนการและเหตุการณ์ ตัวอย่าง ได้แก่ ระบบควบคุมอุตสาหกรรม, ระบบอัตโนมัติในอาคาร, ระบบขนส่ง, ระบบควบคุมการเข้าออกทางกายภาพ, ระบบตรวจสอบสภาพแวดล้อมทางกายภาพ และระบบการวัดสภาพแวดล้อมทางกายภาพมัลแวร์เรียกค่าไถ่การโจมตีในระบบควบคุมในอุตสาหกรรมที่สำคัญ ในช่วงปี ค.ศ. 2015 ถึงปี ค.ศ. 2021

จาก Alamri (2022) มัลแวร์เรียกค่าไถ่โจมตีเป้าหมายตามกลุ่มธุรกิจ ดังรูปที่ 2.1 แสดงให้เห็นว่าร้อยละ 75 ของการโจมตีด้วยมัลแวร์เรียกค่าไถ่ทั้งหมดที่จากเว็บไซต์ดาร์กอตได้ติดตามใน

ไตรมาสที่ 1 ปี 2565 มุ่งเป้าไปที่ภาคการผลิตจากรายงานในไตรมาสที่ 1 ปี 2565 มาพบว่าจำนวนเปอร์เซ็นต์การโจมตีของภาคการผลิตมากสุดดังรูปที่ 2.1



รูปที่ 2.1 แสดงประเภทของมัลแวร์เรียกค่าไถ่ล่าสุดโดยแบ่งการโจมตีเป้าหมายตามกลุ่มธุรกิจ
ที่มา: เว็บไซต์ดาร์กอต, 2565

จากตารางที่ 2.2 ได้แสดงถึงมัลแวร์เรียกค่าไถ่การโจมตีในระบบควบคุมในอุตสาหกรรมที่สำคัญ ในช่วงปี ค.ศ. 2015 ถึง 2021

ตารางที่ 2.2 แสดงมัลแวร์เรียกค่าไถ่การโจมตีในระบบควบคุมในอุตสาหกรรมที่สำคัญ ในช่วงปี ค.ศ. 2015 ถึง 2021

มัลแวร์เรียกค่าไถ่ ปี ค.ศ. ที่พบ	เป้าหมาย/วิธีการโจมตีหรือผลกระทบ
BlackEnergy, 2015	ในเดือนธันวาคม ค.ศ. 2015 ในภูมิภาค อีวาโนฟรังคีฟสค์ (Ivano-Frankivsk) ในยูเครนไม่มีไฟฟ้าใช้เป็นเวลาสองสามชั่วโมง ตามรายงานสาเหตุของไฟดับ คือเกิดจากการโจมตีทางไซเบอร์ที่ใช้มัลแวร์ ที่น่าสนใจคือ กรณีที่ได้รับรายงานไม่ใช่เหตุการณ์ที่เกิดขึ้นสถานที่เดียว เนื่องจากพบว่าบริษัทไฟฟ้าอื่น ๆ ในยูเครนตกเป็นเป้าหมายโจมตี ทั้งระบบ SCADA ที่ปิดสถานีย่อย ซึ่งจากโจมตีระยะไกลในรูปแบบ ฟิชชิ่ง เพื่อวางมัลแวร์ ปิดการใช้งาน ทำลาย UPS โมเด็ม RTU ฯลฯ พร้อมทั้งทำลายไฟล์บนเซิร์ฟเวอร์และเวิร์กสเตชัน (Miller, 2021)

ตารางที่ 2.2 แสดงมัลแวร์เรียกค่าไถ่การโจมตีในระบบควบคุมในอุตสาหกรรมที่สำคัญ ในช่วงปี ค.ศ. 2015 ถึง 2021 (ต่อ)

มัลแวร์เรียกค่าไถ่ ปี ค.ศ. ที่พบ	เป้าหมาย/วิธีการโจมตีหรือผลกระทบ
Shamoon 2, 2016	ผู้โจมตี Shamoon ได้โจมตีหน่วยงานการบินในซาอุดิอาระเบีย การหยุดชะงักและความเสียหาย กำหนดเป้าหมายบริษัทพลังงาน GCC การโจมตีด้วยการเข้าถึงระยะไกลด้วยข้อมูลประจำตัวที่ถูกขโมยจากมัลแวร์ ได้แพร่กระจายอย่างลับ ๆ ในคอมพิวเตอร์ด้วยการตั้งกำหนดเวลากระบวนการ เพื่อโจมตี และล้างข้อมูล (Robert, 2016)
WannaCry, 2018	ในปี 2561 บริษัท Taiwan Semiconductor Manufacturing Company (TSMC) ได้ถูกการโจมตีด้วยมัลแวร์เรียกค่าไถ่ครั้งใหญ่ โดย WannaCry ซึ่งเป็นกลุ่มที่ถูกกล่าวหาว่ามีความสัมพันธ์กับเกาหลีเหนือ ซึ่งทำให้บริษัท TSMต้องปิดโรงงานผลิตชิปหลายแห่ง การโจมตีส่งผลกระทบต่อเครื่องจักรมากกว่า 10,000 เครื่องในโรงงานที่ทันสมัยที่สุดข และทำให้การผลิต การผลิตที่คาดว่าจะใช้กับ iPhone ในอนาคตของ Apple ล่าช้า ซึ่งอาจส่งผลกระทบต่อรายได้ประมาณ 256 ล้านดอลลาร์ (Loana, 2019)
DoppelPaymer, 2019	บริษัท Visser Precision ผู้ผลิตชิ้นส่วนสั่งทำสำหรับอุตสาหกรรมต่าง ๆ รวมถึงยานยนต์และการบิน ได้แถลงการณ์บริษัทยืนยันว่าเป็น เป้าหมายล่าสุดของเหตุการณ์ความปลอดภัยทางไซเบอร์ได้ถูก DoppelPaymer Ransomware โจมตีซึ่งเป็นมัลแวร์ประเภทใหม่ที่เข้ารหัสไฟล์ซึ่งจะทำการกรองข้อมูลของบริษัทออกก่อน มัลแวร์เรียกค่าไถ่ได้ทำการข่มขู่ว่าจะเผยแพร่ไฟล์ที่ถูกขโมยหากไม่ได้รับการจ่ายค่าไถ่ในครั้งนี้ (Jackson, 2023)
RYUK, 2020	EMCOR Group ซึ่งมีชื่อเสียงในฐานะ EMCOR เป็นบริษัทที่ติดอันดับ Fortune 500 ได้เปิดเผยว่าได้ตกเป็นเหยื่อการโจมตี RYUK Ransomware ในเดือนกุมภาพันธ์ปีนี้ ตามรายละเอียดที่รายงาน Cybersecurity Insiders การโจมตีของมัลแวร์เข้ารหัสไฟล์เกิดขึ้นเมื่อวันที่ 15 กุมภาพันธ์ ค.ศ. 2020 (Jackson, 2023)

DarkSide, 2021	Colonial Pipeline ก่อตั้งขึ้นในปี ค.ศ. 1962 และมีสำนักงานใหญ่ในเมืองอัลฟาเรตตา รัฐจอร์เจีย โคโลเนียลไปป์ไลน์ซึ่งเป็นบริษัทเอกชนถือเป็นหนึ่งในผู้ให้บริการท่อส่งน้ำมันรายใหญ่ที่สุดในสหรัฐอเมริกา และให้บริการเชื้อเพลิงประมาณร้อยละ 45 เมื่อวันที่ 7 พฤษภาคม ค.ศ. 2021 บริษัทต้องปิดการดำเนินงานในเชิงรุกและหยุดระบบไอทีหลังจากตกเป็นเหยื่อของการโจมตีทางไซเบอร์กลุ่ม DarkSide ที่โจมตีระบบเครือข่าย (Trend Micro Research, 2021)
CryptoLocker, 2021	โรงงานในเขตพื้นที่จังหวัดอยุธยา พบการโจมตีทางไซเบอร์เริ่มที่เครื่องจักรที่ควบคุมด้วยคอมพิวเตอร์ 3 เครื่องบนระบบปฏิบัติการ Windows 10 รุ่น 1809 ซึ่งเป็นเครื่องจักรที่ควบคุมด้วยคอมพิวเตอร์ในสายการผลิตใน OT พบว่ามีเครื่องที่ควบคุมด้วยคอมพิวเตอร์เครื่องหนึ่งได้ทำการเข้ารหัสไฟล์ข้อมูล CryptoLocker ransomware สร้างโฟลเดอร์และไฟล์ในคอมพิวเตอร์ โฟลเดอร์พบไฟล์ดังต่อไปนี้ DeployTools, igfxEMNP, DeployTools.exe และตัวหลักของ CryptoLocker ransomware โจมตีเพย์โหลดที่รันบน Windows กำหนดเวลางานรัน “update.exe” ในเส้นทางโฟลเดอร์บน “C:\Users\Users\AppData\Roaming\\Microsoft \Windows \Start Menu\Programs\Startup\update.exe” (Nakhonthai & Chimmanee, 2022)

ที่มา: รวบรวมโดยผู้วิจัย, 2566

2.4 แอคทีฟไดเรกทอรี่ (Active Directory)

Suwaradee (2017) ในระบบไอทีขององค์กรแอคทีฟไดเรกทอรี่ (Active Directory) เป็นเครื่องมือสำคัญที่มีมากับวินโดวส์เซิร์ฟเวอร์โอเปอร์เรติ้งซิสเต็ม (Windows Server Operating System) โดยทำหน้าที่ช่วยจัดการทรัพยากรในระบบ ด้วยเครื่องมือของเซิร์ฟเวอร์โดเมนคอนโทลเลอร์ (Server Domain Controller) ถ้าองค์กรที่มียูสเซอร์ (User) หรือผู้ใช้จำนวนมาก ๆ สามารถนำแอคทีฟไดเรกทอรี่มาใช้งาน จะช่วยลดภาระค่าใช้จ่ายในการบริหารจัดการทรัพยากรของยูสเซอร์ อีกทั้งยังเพิ่มความปลอดภัยให้กับระบบโดยรวมโดยที่ไม่ต้องซื้อเครื่องมือเพิ่มเติม นอกจากจะช่วยจัดการทรัพยากรในระบบแล้วแอคทีฟไดเรกทอรี่ ทำหน้าที่จัดเก็บข้อมูลเกี่ยวกับออฟเจค

(object) ต่าง ๆ เช่น ยูสเซอร์ (User), กลุ่ม (Group) คอมพิวเตอร์ (Computer) หรือ นโยบายรักษาความปลอดภัย (Security Policy) และจี พีโอ (GPO : Group Policy Object) ของไมโครซอฟท์ คือ ชุดการตั้งค่านโยบายเพื่อควบคุมการทำงานของเครื่องคอมพิวเตอร์และผู้ใช้งาน เช่น กำหนดความมั่นคงปลอดภัยในเครือข่าย กำหนดปิดเซอร์วิสอาร์ดีพีป้องกันเข้าถึงการเชื่อมต่อผ่านรีโมทเดสท็อปคอนเนคชั่น กำหนดปิดโปรแกรมแบบอัตโนมัติตามตารางเวลาที่กำหนด (Schedule Task) บนระบบปฏิบัติการวินโดวส์ การติดตั้งและการอัปเดตซอฟต์แวร์ เพื่อป้องกันการโจมตีจากมัลแวร์

ส่วนประกอบของแอคทีฟไดเรกทอรี่โดเมนนั้น จะมีส่วนประกอบอยู่ 2 ส่วนด้วยกัน คือ

1) แอคทีฟ ไดเรกทอรี่เซอรวิซ (Active Directory Service) เป็นส่วนประกอบที่ทำหน้าที่ให้บริการแก่ยูสเซอร์และแอดมิน (Admin)

2) แอคทีฟไดเรกทอรี่ ดาต้าเบส (Active Directory Database) เป็นฐานข้อมูลสำหรับใช้ในการเก็บไดเรกทอรี่ออฟเจค Directory Object (Directory Object) ต่าง ๆ เช่นยูสเซอร์แอคเคาท์ (User Account), กลุ่มแอคเคาท์ (Group Account), แชร์ โฟลเดอร์ (Shared Folder) เป็นต้น (คริชณะ ฉิมมณี และมณีสุข โชติรุ่งรัตน์, 2564)

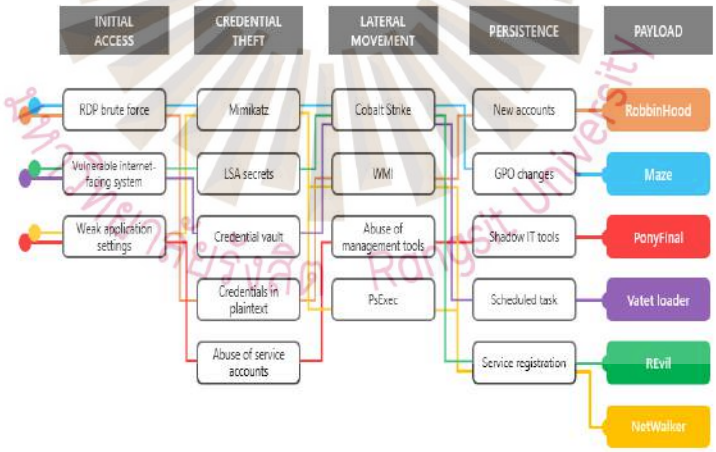
2.5 รีโมทเดสท็อปคอนเนคชั่น (Remote Desktop Connection)

อาร์ ดี พี (Remote Desktop Protocol: RDP) หรือ รีโมทเดสท็อปคอนเนคชั่น (Remote Desktop Connection) เป็นโปรแกรมที่มาพร้อมกับระบบปฏิบัติการ Windows ตั้งแต่รุ่น XP จนถึงปัจจุบัน โดยมีคุณสมบัติในการควบคุมคอมพิวเตอร์ระยะไกลผ่านเครือข่าย ทำให้ผู้ใช้สามารถเห็นและใช้งานหน้าจอของเครื่องคอมพิวเตอร์ปลายทางได้ราวกับนั่งอยู่หน้าเครื่องนั้นโดยตรง ข้อดีของ RDP คือช่วยลดเวลาที่ใช้ในการเดินทางมาที่ทำงาน เหมาะสำหรับการใช้งานจากระยะไกลทั้งในระดับบุคคลและองค์กร (Worachat, 2559)

ไมโครซอฟท์ได้ออกแจ้งเตือนพบว่ามีช่องโหว่การโจมตีหมายเลขพอร์ต 3389 แนะนำให้อัพเดทโปรแกรมรักษาความปลอดภัยล่าสุดจากไมโครซอฟท์ประจำเดือน เพื่อปิดช่องโหว่ ได้แนะนำปิดพอร์ต 3389 บนระบบเครือข่าย หรือสามารถเลือกใช้ จีพีโอ (GPO : Group Policy Object) ทำการปิดเซอร์วิสอาร์ดีพีบนระบบปฏิบัติการวินโดวส์เวอร์ชัน เอกพี, เจ็ด และระบบปฏิบัติการวินโดวส์เซิฟเวอร์เวอร์ชัน 2003 และ2008 โดยกลุ่มแฮกเกอร์สามารถเจาะระบบผ่านโปรโตคอลอาร์ดีพีซึ่งใช้หมายเลขพอร์ตปริยาย รวมถึงตั้งค่าบัญชีผู้ใช้งานและรหัสผ่านที่คาดเดาได้ง่ายโดยวิธีบรูตฟอร์ซ (Brute-forcing) ดังนั้น จึงแนะนำให้เปลี่ยนค่าพอร์ตปริยายนี้ เพื่อลดโอกาสการถูกโจมตีจากแฮกเกอร์ (Microsoft Security Response Center, 2019)

2.6 กรอบแนวคิดของไมโครซอฟท์การโจมตีของมัลแวร์เรียกค่าไถ่

เนื่องจากไมโครซอฟท์นำเสนอวิธีการที่มุ่งอำนวยความสะดวกในการนำทางฐานความรู้ของกลวิธีและเทคนิคของฝ่ายตรงข้าม ซึ่งสามารถช่วยให้ผู้ดูแลระบบมุ่งเน้นไปที่เทคนิคที่สำคัญ ในระบบควบคุมในโรงอุตสาหกรรมการผลิตชิ้นส่วนอิเล็กทรอนิกส์ ระบบปฏิบัติการวินโดวส์ถูกใช้อย่างแพร่หลายในเครื่องคอมพิวเตอร์ควบคุม และเซิร์ฟเวอร์ ที่ผู้พัฒนามัลแวร์เรียกค่าไถ่นั้นมีการพัฒนาเทคนิคใหม่อยู่ตลอดเวลา พบมัลแวร์เรียกค่าไถ่หลายสายพันธุ์ได้ใช้เทคนิคจากการโจมตีแล้วมีคุณลักษณะที่แตกต่างกัน จากกรอบแนวคิดของไมโครซอฟท์ได้แบ่งการดำเนินการของมัลแวร์เรียกค่าไถ่ออกเป็น 5 ขั้นตอน Initial Access, Credential theft, Lateral movement, Persistence ,and Payload (คริชณะ ฉิมมณี และมณีสุข โชติรุ่งรัตน์, 2564) ได้นำกรอบแนวคิดจากไมโครซอฟท์มาวิเคราะห์การโจมตี จากระบบปฏิบัติการวินโดวส์มีการใช้อย่างแพร่หลายและตกเป็นเป้าโจมตีหมายของแก๊งมัลแวร์เรียกค่าไถ่ ดังนั้นไมโครซอฟท์จึงได้วางกรอบแนวคิดในการแบ่งขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่ออกเป็น 5 ขั้นตอน (Microsoft, 2020)



รูปที่ 2.2 แสดงขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่ ตามกรอบแนวคิดของไมโครซอฟท์

ที่มา: Microsoft 365 Defender Threat Intelligence Team, 2020

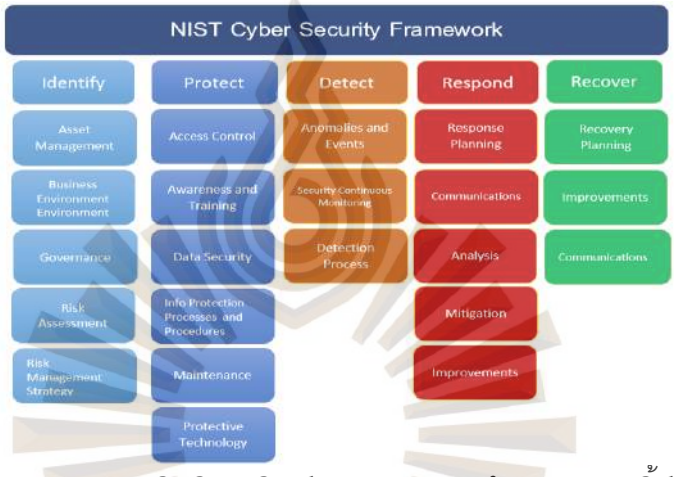
2.7 กลยุทธ์ เทคนิคและกระบวนการทำงานของแฮกเกอร์ด้วยไมเตอร์แอทแทค (MITRE ATT&CK)

ไมเตอร์แอทแทค (MITRE) ได้ก่อตั้งขึ้นเมื่อเดือนกรกฎาคม ปี ค.ศ. 1958 ที่รัฐเวอร์จิเนีย ประเทศสหรัฐอเมริกา โดยย่อมาจาก (Massachusetts Institute of Technology Research Establishment: MITRE) เป็นบริษัทที่ก่อตั้งขึ้นโดยไม่หวังผลกำไร ได้รวบรวมฐานความรู้ และอธิบายกระบวนการ กลยุทธ์ (Tactic) และเทคนิค (Technique) การเจาะระบบของแฮกเกอร์ (Threat Actor) ในการโจมตีแต่ละครั้ง โดยไมเตอร์แอทแทค ได้ออก ATT&CK for ICS ที่รวบรวมกลยุทธ์และเทคนิคที่แฮ็กเกอร์นิยมใช้โจมตีระบบ ICS โดยเน้นที่แอปพลิเคชันและโปรโตคอลที่ ICS ใช้งานตัวอย่างกลยุทธ์กลยุทธ์ Initial Access มีเทคนิคที่ชื่อว่า External Remote Services จะมีการอธิยายการทำงานของเทคนิคนั้น ๆ ข้อมูลอื่น ๆ (ID, แพลตฟอร์มที่ถูกโจมตี และอื่น ๆ) รวมถึงยกตัวอย่างกระบวนการที่เคยเกิดขึ้น วิธีการป้องกันเบื้องต้น ยกตัวอย่างเช่นกลยุทธ์ Initial Access ใช้โค้ดอ้างอิงกลยุทธ์ (TA) คือ TA0001 และในแต่ละกลยุทธ์ ก็จะมีเทคนิค ที่ใช้ในกลยุทธ์นั้น ๆ อีก เช่น เทคนิค Phishing ที่ใช้โค้ดอ้างอิงเทคนิค (T) คือ T1566 นอกเหนือจาก เทคนิคหลัก ๆ ทั้งหลายแล้วก็จะมีเทคนิคย่อย ๆ อีกจะเป็นโค้ดอ้างอิงเทคนิคตามด้วยจุด (.) และลำดับของเทคนิคย่อยอีกด้วย และล่าสุดไมเตอร์แอทแทคได้ออกอัพเดทในเดือนตุลาคม 2565 เวอร์ชัน 12 อัปเดตเทคนิค กลุ่ม และซอฟต์แวร์สำหรับองค์กร อุปกรณ์เคลื่อนที่ และ ICS การเปลี่ยนแปลงที่ใหญ่ที่สุดใน ATT&CK เวอร์ชัน12 คือการเพิ่มการตรวจหา ATT&CK สำหรับ ICS (thaicyberdefense, 2020)

2.8 สถาบันมาตรฐานและเทคโนโลยีแห่งชาติกระทรวงพาณิชย์ขอสหรัฐอเมริกา (NIST)

เอ็นไอเอสที ไซเบอร์ซีเคียวริตี้ เฟรมเวิร์ค (NIST Cybersecurity Framework)ในปี ค.ศ 2018 นิสต์ (NIST) ได้นำเสนอเฟรมเวิร์ก Framework for Improving Critical Infrastructure Cybersecurity ซึ่งเป็นการกำหนดแนวทางการจัดการความเสี่ยงด้านความปลอดภัยไซเบอร์ เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทั่วไป รวมไปถึงช่วยให้องค์กรสามารถวางแผน ป้องกัน ตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ถัดมาในปี ค.ศ. 2021 นิสต์ได้นำเสนอ Preliminary Draft NISTIR 8374 : Cybersecurity Framework Profile for Ransomware Risk Management ซึ่งเป็นเฟรมเวิร์กที่มุ่งเน้นไปสำหรับมัลแวร์เรียกค่าไถ่โดยเฉพาะ และได้ให้คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนอง และกู้คืน จากเหตุการณ์มัลแวร์เรียกค่าไถ่ คริชณะ ฉิมมณี และมณีสุข โชติรุ่งรัตน์ (2564) เพื่อครอบคลุมการรักษาความปลอดภัยในภาคอุตสาหกรรมได้ออกคู่มือการรักษาความปลอดภัยเทคโนโลยีการปฏิบัติงาน (OT) เวอร์ชัน SP 800-82 Rev. 3 (Draft) เฟรมเวิร์กนี้อธิบายถึงวิธีการรักษาความปลอดภัยเทคโนโลยีเชิงปฏิบัติการ

โดยพิจารณาข้อกำหนดด้านประสิทธิภาพ ได้ครอบคลุมระบบและอุปกรณ์ที่ติดตั้งโปรแกรมได้หลากหลาย ซึ่งสื่อสารระหว่างกันในสภาพแวดล้อมเชิงปฏิบัติการ และได้กล่าวถึงเพอร์ดูโมเดล (Purdue Model) เป็นแนวทางจัดหมวดหมู่และกำหนดระดับการป้องกันของระบบควบคุมอุตสาหกรรมที่มีความซับซ้อน (Keith et al., 2022) และล่าสุดเพื่อรับมือต่อสถานการณ์ปัจจุบันได้นำเสนอเฟรมเวิร์กในเดือนกุมภาพันธ์ ปี ค.ศ. 2022 สำหรับสนับสนุนการป้องกัน ตอบสนอง และกู้คืน จากเหตุการณ์มัลแวร์เรียกค่าไถ่ดังที่ได้แสดงดังรูปที่ 2.3



รูปที่ 2.3 แสดงขั้นตอนแนวทางปฏิบัติของนิสต์ (ปรับปรุง และนำเสนอเฟรมเวิร์ก February 2022)
ที่มา: ดัดแปลงจาก แนวทางปฏิบัติของนิสต์เฟรมเวิร์ค, 2565

2.8.1 การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)

คือ การระบุสภาพแวดล้อม ทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

2.8.1.1 การบริหารจัดการทรัพย์สิน (Asset Management: AM) ข้อมูลบุคลากร อุปกรณ์ ระบบ ต้องได้รับการระบุและจัดการตามความสำคัญที่สัมพันธ์กับวัตถุประสงค์ขององค์กร

2.8.1.2 การดำเนินการตรวจสอบสภาพแวดล้อม (Business Environment: BE) ภารกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสียและกิจกรรมสำคัญขององค์กร

2.8.1.3 การกำกับดูแล (Governance: GV) นโยบาย ขั้นตอนและกระบวนการการจัดการ และติดตามข้อกำหนดด้านกฎระเบียบ กฎหมาย ความเสี่ยง สิ่งแวดล้อม และการปฏิบัติงาน

2.8.1.4 การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment: RA)ความเข้าใจในความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อการดำเนินงาน

2.8.1.5 การกำหนดกลยุทธ์บริหารจัดการความเสี่ยง (Risk Management Strategy: RM) การลำดับความสำคัญ ความเสี่ยงที่ยอมรับได้ขององค์กรใช้เพื่อสนับสนุนหรือตัดสินใจ

2.8.1.6 การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management: SC) ลำดับความสำคัญของการยอมรับความเสี่ยง เพื่อสนับสนุนการตัดสินใจในการจัดการความเสี่ยงห่วงโซ่อุปทาน

2.8.2 **การปกป้องดูแลทรัพย์สินสารสนเทศ** (Protect)

คือ มาตรการป้องกันที่เหมาะสมสำหรับการให้บริการที่สำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบและลดโอกาสเกิดความเสี่ยง

2.8.2.1 กำหนดมาตรการควบคุมการเข้าถึง (Access Control: AC) การเข้าถึงทรัพย์สินและสิ่งอำนวยความสะดวกที่เกี่ยวข้องเฉพาะผู้ใช้ที่ได้รับอนุญาต

2.8.2.2 การสร้างความตระหนักและการฝึกอบรม (Awareness and Training: AT)บุคลากรขององค์กรได้รับการอบรมหรือสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

2.8.2.3 การกำหนดความมั่นคงปลอดภัยของข้อมูล (Data Security: DS) ข้อมูลและบันทึกได้รับการจัดการที่สอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับ ความสมบูรณ์และความพร้อมใช้งานของข้อมูล

2.8.2.4 กระบวนการบำรุงรักษา (Maintenance: MA) กระบวนการ วิธีการบำรุงรักษาและการซ่อมแซมระบบ

2.8.2.5 จัดหาเทคโนโลยีการป้องกัน (Protective Technology: PT) องค์กรต้องจัดหาระบบสำหรับป้องกัน และการรักษาความมั่นคงปลอดภัยเพื่อเพิ่มประสิทธิภาพในการจัดการความมั่นคงปลอดภัย

2.8.3 **ความสามารถในการตรวจพบเหตุภัยคุมคามไซเบอร์** (Detect)

คือ การตรวจหาเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวัง หรือตรวจติดตามอย่างต่อเนื่อง

มหาวิทยาลัยรังสิต Rangsit University

2.8.3.1 การตรวจจับเหตุการณ์ และความผิดปกติ (Anomalies and Events: AE) กระบวนการตรวจจับกิจกรรมผิดปกติ และสร้างเข้าใจผลกระทบที่เกิดขึ้นจากเหตุการณ์ที่พบ

2.8.3.2 การตรวจสอบด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring: CM) กระบวนการตรวจสอบระบบ ข้อมูล และทรัพย์สินสำหรับใช้ระบุเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยทางไซเบอร์

2.8.3.3 กระบวนการตรวจจับ (Detection Processes: DP) กระบวนการและขั้นตอนการตรวจจับได้รับการบำรุงรักษาและทดสอบเพื่อให้แน่ใจว่ามีการตระหนักถึงเหตุการณ์ผิดปกติ

2.8.4 การรับมือภัยคุกคาม (Respond)

คือ การตอบสนอง (Respond) การดำเนินการตอบสนองต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

2.8.4.1 การวางแผนการตอบสนอง (Response Planning: RP) กระบวนการและขั้นตอนการตอบสนองที่ใช้ในการวางแผนสำหรับใช้ในการตอบสนองต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

2.8.4.2 การสื่อสาร (Communications: CO) เพื่อประสานงานกับหน่วยงานที่เกี่ยวข้อง การตอบสนองการประสานงานกับผู้มีส่วนได้ส่วนเสีย

2.8.4.3 การวิเคราะห์ (Analysis: AN) การวิเคราะห์ดำเนินการเพื่อให้แน่ใจว่ามีการตอบสนองที่มีประสิทธิภาพและสนับสนุนกิจกรรมการกู้คืน

2.8.4.4 การควบคุมดูแลและจำกัด (Mitigation: MI) การควบคุมจำกัดขอบเขตและลดผลกระทบที่เกิดขึ้น กิจกรรมต่าง ๆ เพื่อป้องกัน และแก้ไขของเหตุการณ์

2.8.4.5 การปรับปรุง (Improvements: IM) กิจกรรมการตอบสนองขององค์กรได้รับการปรับปรุงโดยการพิจารณาสิ่งได้ที่เรียนรู้จากกิจกรรมการตรวจจับ/การตอบสนองในปัจจุบัน และก่อนหน้า

2.8.5 การกู้คืนข้อมูลและระบบหลังเหตุภัยคุกคามไซเบอร์ (Recovery)

คือ การดำเนินการกู้คืนสภาพระบบสารสนเทศที่ได้รับความเสียหายจากการถูกคุกคามด้านไซเบอร์ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

2.8.5.1 การวางแผนการกู้คืน (Recovery Planning: RP) กระบวนการและขั้นตอนการกู้คืนข้อมูล ระบบสารสนเทศที่ได้ผลกระทบได้รับการฟื้นฟู

2.8.5.2 การปรับปรุง (Improvements: IM) การวางแผนและกระบวนการกู้คืนได้รับการปรับปรุงเข้ากับกับกิจกรรมต่าง ๆ ในอนาคต

2.8.5.3 การสื่อสาร (Communications: CO) กิจกรรมการฟื้นฟูได้รับการประสานงานกับภายในและภายนอก (เช่น ศูนย์ประสานงาน ผู้ให้บริการอินเทอร์เน็ต เจ้าของระบบโจมตี ผู้ที่ได้รับผลกระทบ CSIRT อื่น ๆ และ ผู้ขาย)

ล่าสุดเพื่อรับมือต่อสถานการณ์ปัจจุบันนิสต์ได้นำเสนอเฟรมเวิร์กในเดือนกุมภาพันธ์ ปี ค.ศ. 2022 สำหรับสนับสนุนการป้องกัน ตอบสนอง และกู้คืน จากเหตุการณ์มัลแวร์เรียกค่าไถ่ดังที่ได้แสดงดังตารางที่ 2.3

ตารางที่ 2.3 คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนองและกู้คืนจากเหตุการณ์มัลแวร์เรียกค่าไถ่

หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)		
การจัดการสินทรัพย์ (ID.AM): ข้อมูล บุคลากร อุปกรณ์ ระบบ และสิ่งอำนวยความสะดวกที่ช่วยให้องค์กรบรรลุวัตถุประสงค์ทางธุรกิจได้รับการระบุ	ID.AM-1: อุปกรณ์ทางกายภาพและระบบภายในองค์กร ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 5 CM-8, PM-5	ควรมีการดำเนินการตรวจสอบและบำรุงรักษาสินค้าคงคลังของอุปกรณ์ทางกายภาพเพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้จะไม่เสี่ยงต่อมัลแวร์เรียกค่าไถ่ นอกจากนี้ยังเป็นประโยชน์ที่จะมีสินค้าคงคลังของฮาร์ดแวร์ในระหว่างขั้นตอนการกู้คืนหลังจากการโจมตีของมัลแวร์เรียกค่าไถ่ หากจำเป็นต้อง

ตารางที่ 2.3 คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนองและกู้คืน จากเหตุการณ์มัลแวร์เรียกค่าไถ่ (ต่อ)

หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)		
และจัดการโดยสอดคล้องกับความสำคัญที่สัมพันธ์กับวัตถุประสงค์ขององค์กร และกลยุทธ์ความเสี่ยงขององค์กร		ติดตั้งแอปพลิเคชันใหม่อีกครั้ง
	ID.AM-2: แพลตฟอร์มของซอฟต์แวร์และแอปพลิเคชันภายในองค์กรได้มีการจดบันทึกเป็นรายการทรัพย์สิน ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 5 CM-8, PM-5	รายการทรัพย์สินที่จดบันทึก ได้แก่ ติดตามข้อมูล เช่น ชื่อและเวอร์ชันของซอฟต์แวร์ อุปกรณ์ที่ติดตั้งอยู่ วันที่แก้ไขล่าสุดและช่องโหว่ที่ทราบในปัจจุบัน ข้อมูลนี้สนับสนุนการแก้ไขช่องโหว่ที่อาจใช้ในการโจมตีมัลแวร์เรียกค่าไถ่
	ID.AM-3: มีการวางผังการสื่อสารภายในองค์กร และการกระจายข้อมูลข่าวสารให้เป็นไปอย่างทั่วถึง ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 5 AC-4, CA-3, CA-9, PL-8	สามารถระบุได้ว่าข้อมูลหรือกระบวนการใดมีความเสี่ยง หากผู้โจมตีขยายการโจมตีไปยังระบบเครือข่ายอื่นภายในองค์กร
	ID.AM-4: มีการจัดหมวดหมู่ระบบข้อมูลภายนอก	เป็นสิ่งสำคัญสำหรับการวางแผนสื่อสารกับหุ้นส่วน และดำเนินการ

มหาวิทยาลัยรังสิต Rangsit University

	ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 5 AC-20, SA-9	ตามขั้นตอนที่เป็นไปได้เพื่อยกเลิกการเชื่อมต่อชั่วคราวจากระบบภายนอกเพื่อตอบสนองต่อเหตุการณ์มัลแวร์เรียกค่าไถ่ การระบุการเชื่อมต่อเหล่านี้จะช่วยให้องค์กรสามารถวางแผนการปฏิบัติการควบคุมความปลอดภัยไซเบอร์และสามารถระบุบริเวณที่ถูกควบคุมซึ่งอาจเปิดเผยแก่บุคคลที่เกี่ยวข้องรับทราบได้
	ID.AM-5: ทรัพยากรขององค์กร ได้แก่ ฮาร์ดแวร์ อุปกรณ์ ข้อมูล เวลา บุคลากรและซอฟต์แวร์ ได้รับการจัดลำดับความสำคัญแยกตามประเภท ความจำเป็น และมูลค่าทางธุรกิจ ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 5 CP-2, RA-2, RA-9, SC-6	การจัดลำดับความสำคัญของทรัพยากรช่วยให้องค์กรเข้าใจขอบเขตและผลกระทบของเหตุการณ์มัลแวร์เรียกค่าไถ่ที่แท้จริง และเป็นปัจจัยสำคัญในการวางแผนฉุกเฉินสำหรับเหตุการณ์มัลแวร์เรียกค่าไถ่ในอนาคต นอกจากนี้ยังเป็นการช่วยจัดลำดับความสำคัญของกระบวนการรับมือภัยคุกคามและการกู้คืนข้อมูลขององค์กร
	ID.AM-6: กำหนดบทบาทและความรับผิดชอบด้านความปลอดภัยไซเบอร์ให้กับพนักงาน บุคคลที่เกี่ยวข้อง รวมถึง ผู้มีส่วนได้เสีย เช่น ซัพพลายเออร์ ลูกค้า คู่ค้า เป็นต้น	สิ่งที่สำคัญคือ ทุกคนในองค์กรต้องเข้าใจบทบาทและความรับผิดชอบของตนในการป้องกันเหตุการณ์มัลแวร์เรียกค่าไถ่ รวมถึงการรับมือภัยคุกคาม และการกู้คืนข้อมูลจากเหตุการณ์ที่ถูกโจมตีด้วย

มหาวิทยาลัยรังสิต Rangsit University

	ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 5 CP-2, PS-7, PM-11	
สภาพแวดล้อมทางธุรกิจ (ID.BE): ภารกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสียและกิจกรรมขององค์กรได้รับการเข้าใจ และจัดลำดับความสำคัญข้อมูลนี้ใช้เพื่อแจ้งบทบาทความปลอดภัยทางไซเบอร์ ความรับผิดชอบ และการตัดสินใจในการจัดการความเสี่ยง	ID.BE-2: ตำแหน่งขององค์กรในโครงสร้างพื้นฐานที่สำคัญและภาคอุตสาหกรรมได้รับการระบุและสื่อสาร ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 5 PM-8	ซึ่งช่วยให้ทีมรับมือเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์แห่งชาติเข้าใจตำแหน่งขององค์กรเป้าหมายในสภาพแวดล้อมโครงสร้างพื้นฐานที่สำคัญได้ดีขึ้นและอนุญาตให้ตอบสนองในเวลาที่เหมาะสมในกรณีที่เกิดผลกระทบข้ามภาค นอกจากนี้ยังสนับสนุนให้องค์กรและผู้มีส่วนได้ส่วนเสียภายนอกพิจารณาผลกระทบจากดาวน์สตรีมจากการโจมตีของมัลแวร์เรียกค่าไถ่
	ID.BE-3: ลำดับความสำคัญสำหรับภารกิจขององค์กร วัตถุประสงค์และกิจกรรมได้รับการกำหนดและสื่อสาร NIST SP 800-53 Rev. 5 PM-11, SA-14	ซึ่งช่วยให้ฝ่ายปฏิบัติการและผู้เผชิญเหตุสามารถจัดลำดับความสำคัญของทรัพยากรได้ รองรับการวางแผนฉุกเฉินสำหรับเหตุการณ์มัลแวร์เรียกค่าไถ่ในอนาคต การตอบสนองฉุกเฉิน และการดำเนินการกู้คืน
	ID.BE-4: มีการจัดตั้งการพึ่งพาและหน้าที่ที่สำคัญสำหรับการส่งมอบบริการที่สำคัญ ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3	ซึ่งช่วยในการระบุองค์ประกอบทุติยภูมิและตติยภูมิที่สำคัญในการสนับสนุนหน้าที่หลักของธุรกิจขององค์กร สิ่งนี้จำเป็นสำหรับการจัดลำดับความสำคัญของแผนฉุกเฉินสำหรับเหตุการณ์ในอนาคต

มหาวิทยาลัยรังสิต Rangsit University

	NIST SP 800-53 Rev. 5 CP-8, PE-9, PE-11, PM-8, SA-20	และการตอบสนองต่อเหตุการณ์ฉุกเฉินของมัลแวร์เรียกค่าไถ่ หากมี ICS ที่เกี่ยวข้อง ควรรวมหน้าที่ที่สำคัญไว้ในการตอบสนองฉุกเฉินและการดำเนินการกู้คืน
Governance (ID.GV): นโยบาย ขั้นตอนและกระบวนการในการจัดการ และติดตามข้อกำหนดขององค์กร กฎหมาย ความเสี่ยง สิ่งแวดล้อม และการดำเนินงาน เป็นที่เข้าใจและแจ้งการจัดการความปลอดภัยทางไซเบอร์	ID.GV-1: มีการจัดทำ และสื่อสารนโยบายความปลอดภัยทางไซเบอร์ขององค์กร ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 5 AC-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, PE-01, PL-01, PM	การกำหนด และสื่อสารนโยบายที่จำเป็นในการป้องกันหรือบรรเทาเหตุการณ์มัลแวร์เรียกค่าไถ่เป็นสิ่งจำเป็นและเป็นพื้นฐานสำหรับกิจกรรมการป้องกันและบรรเทาผลกระทบอื่น ๆ ทั้งหมด ในทางปฏิบัติ ควรทบทวนนโยบายเหล่านี้เป็นระยะเพื่อสะท้อนธรรมชาติของความเสี่ยงและความเป็นจริงของการปรับเปลี่ยนอย่างต่อเนื่องที่จำเป็น
	ID.GV-3: ข้อกำหนดทางกฎหมาย และระเบียบข้อบังคับเกี่ยวกับความปลอดภัยทางไซเบอร์ รวมถึงความเป็นส่วนตัวและภาระหน้าที่เกี่ยวกับเสรีภาพของพลเมือง เป็นที่เข้าใจและจัดการ ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 5 CA-07, RA-02	นี่เป็นสิ่งจำเป็นสำหรับการพัฒนานโยบายความปลอดภัยทางไซเบอร์และการจัดลำดับความสำคัญในการวางแผนฉุกเฉินเพื่อตอบสนองต่อเหตุการณ์มัลแวร์เรียกค่าไถ่ในอนาคต

มหาวิทยาลัยรังสิต Rangsit University

	ID.GV-4: กระบวนการกำกับดูแล และการจัดการความเสี่ยงจัดการกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ISO/IEC 27001:2013 Clause 6NIST SP 800-53 Rev. 5 PM-3, PM-7, PM-9, PM-10, PM-11, SA-2	ความเสี่ยงจากมัลแวร์เรียกค่าไถ่ต้องนำมาพิจารณาในการกำกับดูแลการจัดการความเสี่ยงขององค์กร เพื่อสร้างนโยบายความปลอดภัยทางไซเบอร์ที่เพียงพอ
Risk Assessment (ID.RA): องค์กรเข้าใจถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อการดำเนินงานขององค์กร (รวมถึงภารกิจ หน้าที่ ภาพลักษณ์ หรือชื่อเสียง) ทรัพย์สินขององค์กรและบุคคล	ID.RA-1: ช่องโหว่ของสินทรัพย์ได้รับการระบุ และจัดทำเป็นเอกสาร ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	การระบุและการบันทึกจุดอ่อนของสินทรัพย์ขององค์กรเป็นสิ่งสำคัญในการพัฒนาแผน และจัดลำดับความสำคัญของการบรรเทาหรือกำจัดจุดอ่อนเหล่านั้น การกระทำเหล่านี้ยังเป็นกุญแจสำคัญในการวางแผนฉุกเฉินสำหรับการประเมินและตอบสนองต่อเหตุการณ์มัลแวร์เรียกค่าไถ่ในอนาคตและจะช่วยลดโอกาสที่การโจมตีมัลแวร์เรียกค่าไถ่จะประสบความสำเร็จ
	ID.RA-2: ได้รับข่าวกรองภัยคุกคามทางไซเบอร์จากฟอรัมและแหล่งข้อมูลการแบ่งปันข้อมูล ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 5 PM-15, PM-16, SI-5	การรับและการใช้ข่าวกรองภัยคุกคามทางไซเบอร์จากแหล่งแบ่งปันข้อมูลสามารถลดความเสี่ยงต่อการโจมตีของมัลแวร์เรียกค่าไถ่และอำนวยความสะดวกในการตรวจหาภัยคุกคามใหม่ตั้งแต่เนิ่น ๆ

	ID.RA-4: มีการระบุผลกระทบและโอกาสทางธุรกิจที่อาจเกิดขึ้น ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 5 PM-9, PM-11, RA-2, RA-3, SA-20	การทำความเข้าใจผลกระทบทางธุรกิจของเหตุการณ์มัลแวร์เรียกค่าไถ่ที่อาจเกิดขึ้นนั้นจำเป็นต่อการสนับสนุนการวิเคราะห์ต้นทุนและผลประโยชน์ด้านการรักษาความปลอดภัยทางไซเบอร์ เพื่อสร้างลำดับความสำคัญสำหรับกิจกรรมในแผนตอบสนองและกู้คืนมัลแวร์เรียกค่าไถ่ การทำความเข้าใจผลกระทบทางธุรกิจที่อาจเกิดขึ้นยังช่วยสนับสนุนการตัดสินใจตอบสนองฉุกเฉินในกรณีที่มีการโจมตีด้วยมัลแวร์เรียกค่าไถ่
	ID.RA-6: การตอบสนองความเสี่ยงได้รับการระบุและจัดลำดับความสำคัญ ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 5 PM-4, PM-9	ค่าใช้จ่ายที่เกี่ยวข้องกับการตอบสนองและการกู้คืนจากเหตุการณ์มัลแวร์เรียกค่าไถ่ได้รับผลกระทบโดยตรงจากประสิทธิภาพของการวางแผนฉุกเฉินสำหรับการตอบสนองต่อความเสี่ยงที่คาดการณ์ไว้
Risk Management Strategy (ID.RM): ลำดับความสำคัญขององค์กร ข้อจำกัดความเสี่ยงที่ยอมรับได้ และข้อสมมติขององค์กรได้รับการกำหนดและใช้เพื่อสนับสนุนการ	ID.RM-1: กระบวนการจัดการความเสี่ยงได้รับการจัดตั้งขึ้น จัดการ และตกลงโดยผู้มีส่วนได้ส่วนเสียขององค์กร ISO/ IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 5 PM-4, PM-9	การกำหนด และบังคับใช้นโยบาย บทบาท และความรับผิดชอบขององค์กรขึ้นอยู่กับผู้มีส่วนได้ส่วนเสียที่ตกลงและดำเนินการตามกระบวนการบริหารความเสี่ยงที่มีประสิทธิผล กระบวนการควรคำนึงถึงความเสี่ยงของเหตุการณ์มัลแวร์เรียกค่าไถ่ นโยบายเหล่านี้ควรได้รับการตรวจสอบเป็นระยะ

มหาวิทยาลัยรังสิต Rangsit University

ตัดสินใจด้านความเสี่ยงด้านปฏิบัติการ		เพื่อสะท้อนถึงลักษณะของความเสี่ยงแบบไดนามิกและความเป็นจริงของการปรับเปลี่ยนที่จำเป็นเมื่อเวลาผ่านไป
Supply Chain Risk Management (ID.SC): การจัดลำดับความสำคัญ ข้อจำกัด ความเสี่ยงที่ยอมรับได้ และการสันนิษฐานขององค์กรได้รับการกำหนด และใช้เพื่อสนับสนุนการตัดสินใจด้านความเสี่ยงที่เกี่ยวข้องกับการจัดการความเสี่ยงในห่วงโซ่อุปทาน องค์กรได้กำหนดและดำเนินการตามกระบวนการเพื่อระบุ ประเมิน และจัดการความเสี่ยงในห่วงโซ่อุปทาน	ID.SC-5: การวางแผนและการทดสอบการตอบสนองและการกู้คืนดำเนินการกับซัพพลายเออร์ และผู้ให้บริการบุคคลที่สาม ISO/ IEC 27001: 2013 A.17.1.3 NIST SP 800-53 Rev. 5 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9	การวางแผนฉุกเฉินของมัลแวร์เรียกค่าไถ่ควรประสานงานกับซัพพลายเออร์ และผู้ให้บริการบุคคลที่สาม และควรรวมถึงการทดสอบกิจกรรมที่วางแผนไว้ แผนควรรวมถึงสถานการณ์ที่องค์กร ซัพพลายเออร์ และบุคคลที่สามจัดเตรียมให้
Identity Management, Authentication and Access Control	PR.AC-1: ข้อมูลประจำตัวและข้อมูลประจำตัวจะออกจัดการ ตรวจสอบ เพิกถอน และตรวจสอบอุปกรณ์ ผู้ใช้	การโจมตีของมัลแวร์เรียกค่าไถ่ส่วนใหญ่ดำเนินการผ่านการเชื่อมต่อเครือข่าย และการโจมตีของมัลแวร์เรียกค่าไถ่มักเริ่มต้นด้วยการประนีประนอมข้อมูล
การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect)		

มหาวิทยาลัยรังสิต Rangsit University

(PR.AC): การเข้าถึงสินทรัพย์ทางกายภาพ และเชิงตรรกะ และสิ่งอำนวยความสะดวกที่เกี่ยวข้องนั้นจำกัดเฉพาะผู้ใช้ กระบวนการ และอุปกรณ์ที่ได้รับอนุญาต และได้รับการจัดการที่สอดคล้องกับความเสี่ยงที่ประเมินของการเข้าถึงกิจกรรมและธุรกรรมที่ได้รับอนุญาตโดยไม่ได้รับอนุญาต	และกระบวนการที่ได้รับอนุญาต ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	ประจำตัว (เช่น การแบ่งปันโดยไม่ได้รับอนุญาตหรือการบันทึกข้อมูลประจำตัว และรหัสผ่านในการเข้าสู่ระบบ) การจัดการข้อมูลประจำตัวที่เหมาะสมเป็นสิ่งสำคัญ แม้ว่าจะไม่ใช่เพียงการบรรเทาผลกระทบเท่านั้นที่จำเป็น
	PR.AC-3: มีการจัดการการเข้าถึงระยะไกล	การโจมตีมัลแวร์เรียกค่าไถ่ ส่วนใหญ่ดำเนินการจากระยะไกล การ

ตารางที่ 2.3 คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนองและกู้คืนจากเหตุการณ์มัลแวร์เรียกค่าไถ่ (ต่อ)

หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect)		
	ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1	จัดการสิทธิ์ที่เกี่ยวข้องกับการเข้าถึงระยะไกลสามารถช่วยรักษาความสมบูรณ์ของระบบและไฟล์ข้อมูลเพื่อป้องกันการแทรกโค้ดที่เป็นอันตรายและการขโมยข้อมูล การใช้

	NIST SP 800-53 Rev. 5 AC-1, AC-17, AC-19, AC-20, SC-15	การตรวจสอบสิทธิ์แบบหลายปัจจัยเป็นวิธีการที่สำคัญและง่ายต่อการใช้งานเพื่อลดโอกาสที่บัญชีจะเกิดการประนีประนอม
	PR.AC-4: สิทธิ์การเข้าถึง และการอนุญาตได้รับการจัดการโดยผสมผสานหลักการของสิทธิพิเศษน้อยที่สุด และการแบ่งแยกหน้าที่ ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 5 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	เหตุการณ์มัลแวร์เรียกค่าไถ่จำนวนมากเกิดขึ้นจากการทำลายข้อมูลรับรองผู้ใช้หรือเรียกใช้กระบวนการที่มีการเข้าถึงระบบที่มีสิทธิพิเศษโดยไม่จำเป็น นี่เป็นขั้นตอนการจัดการที่สำคัญมากในการป้องกันเหตุการณ์ดังกล่าว
	PR.AC-5: ความสมบูรณ์ของเครือข่ายได้รับการปกป้อง (เช่น การแยกเครือข่าย การแบ่งส่วนเครือข่าย) ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-	การแบ่งส่วนหรือการแบ่งแยกเครือข่ายสามารถจำกัดขอบเขตของเหตุการณ์มัลแวร์เรียกค่าไถ่โดยป้องกันมัลแวร์ไม่ให้แพร่กระจายไปยังระบบเป้าหมายที่เป็นไปได้ (เช่น การย้ายเข้าสู่เทคโนโลยีปฏิบัติการหรือระบบควบคุมจากเครือข่ายเทคโนโลยีสารสนเทศทางธุรกิจ) การแยกเครือข่ายไอที และOT ออกจากกันเป็นสิ่งสำคัญและต้องตรวจสอบความเป็นอิสระอย่างสม่ำเสมอ ซึ่งไม่เพียงแต่ช่วยลดความเสี่ยงที่ระบบ OT จะถูกบุกรุก แต่ยังช่วยให้การดำเนินการที่สำคัญระดับต่ำสามารถ

มหาวิทยาลัยรังสิต Rangsit University

		ดำเนินต่อไปได้ในขณะที่ระบบไอทีของธุรกิจกู้คืนจากมัลแวร์เรียกค่าไถ่ นี่เป็นสิ่งสำคัญอย่างยิ่งสำหรับฟังก์ชัน ICS ที่สำคัญ ซึ่งรวมถึงระบบเครื่องมือความปลอดภัย (SIS)
	PR.AC-6: ข้อมูลประจำตัวได้รับการพิสูจน์และผูกมัดกับข้อมูลประจำตัวและยืนยันในการโต้ตอบ ISO/IEC 27001:2013 A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 5 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	ข้อมูลประจำตัวที่ถูกบุกรุกเป็นเวกเตอร์การโจมตีทั่วไปในเหตุการณ์มัลแวร์เรียกค่าไถ่ ข้อมูลประจำตัวควรได้รับการพิสูจน์แล้วผูกไว้กับข้อมูลประจำตัว (เช่น การตรวจสอบสิทธิ์แบบสองปัจจัยของบุคคลที่ได้รับมอบอำนาจอย่างเป็นทางการ) เพื่อจำกัดความเป็นไปได้ที่ข้อมูลประจำตัวจะถูกบุกรุกหรือออกให้แก่บุคคลที่ไม่ได้รับอนุญาต
Awareness and Training (PR.AT): บุคลากร และพันธมิตรขององค์กรได้รับการศึกษาให้ความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์และได้รับการฝึกอบรมให้ปฏิบัติหน้าที่ และความรับผิดชอบที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ที่สอดคล้องกับนโยบาย	PR.AT-1: ผู้ใช้ทุกคนได้รับแจ้งและฝึกอบรม ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 5 AT-2, PM-13	การโจมตีของมัลแวร์เรียกค่าไถ่ส่วนใหญ่เกิดขึ้นได้โดยผู้ใช้ที่มีส่วนร่วมในการปฏิบัติที่ไม่ปลอดภัย ผู้ดูแลระบบที่ใช้การกำหนดค่าที่ไม่ปลอดภัย หรือนักพัฒนาที่มีการฝึกอบรมด้านความปลอดภัยไม่เพียงพอ

ขั้นตอน และข้อตกลงที่เกี่ยวข้อง		
Data Security (PR.DS): ข้อมูล และบันทึก (ข้อมูล) ได้รับการจัดการโดยสอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล	PR.DS-4: ความจุที่เพียงพอเพื่อให้แน่ใจว่ามีความพร้อมใช้งานอยู่ ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 5 AU-4, CP-2, SC-5	การดูแลให้มั่นใจว่ามีข้อมูลที่เพียงพอสามารถลดผลกระทบจากมัลแวร์เรียกค่าไถ่ได้ ซึ่งรวมถึงความสามารถในการรักษาการสำรองข้อมูลภายนอกและออฟไลน์ การทดสอบเวลาเฉลี่ยในการกู้คืนและความซ้ำซ้อนของระบบในกรณีที่จำเป็น
	PR.DS-5: มีการป้องกันการรั่วไหลของข้อมูล ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 5 AU-4, CP-2, SC-5	การขู่กรรโชกสองครั้ง เรียกร้องการชำระเงินทั้งเพื่อกู้คืนการเข้าถึงข้อมูลและไม่ขายหรือเผยแพร่ข้อมูลที่อื่นเป็นเรื่องปกติ ดังนั้นโซลูชันการป้องกันการรั่วไหลของข้อมูลจึงมีความสำคัญ
	PR.DS-6: กลไกการตรวจสอบความสมบูรณ์จะใช้ในการตรวจสอบซอฟต์แวร์ เฟิร์มแวร์ และความสมบูรณ์ของข้อมูล ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 5 SC-16, SI-7	กลไกการตรวจสอบความสมบูรณ์สามารถตรวจจับการอัปเดตซอฟต์แวร์ที่ถูกดัดแปลงซึ่งสามารถใช้เพื่อแทรก มัลแวร์ที่เปิดใช้งานเหตุการณ์ต่าง ๆมัลแวร์เรียกค่าไถ่
	PR.DS-7: สภาพแวดล้อมการพัฒนา และการทดสอบแยก	การรักษาสภาพแวดล้อมการพัฒนาและการทดสอบแยกจาก

มหาวิทยาลัยรังสิต Rangsit University

	จากสภาพแวดล้อมฝั่งการผลิต ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 5 CM-2	สภาพแวดล้อมการผลิตสามารถป้องกันมัลแวร์เรียกค่าไถ่ไม่ให้เผยแพร่จากระบบการพัฒนาและการทดสอบเข้าสู่ระบบการฝั่งผลิต
Information Protection Processes and Procedures (PR.IP): นโยบายการรักษาความปลอดภัย (ที่กล่าวถึงวัตถุประสงค์ ขอบเขต บทบาท ความรับผิดชอบ ความมุ่งมั่นในการจัดการ และการประสานงานระหว่างหน่วยงานขององค์กร) กระบวนการ และขั้นตอนต่าง ๆ ได้รับการดูแล และใช้เพื่อจัดการการป้องกันระบบข้อมูล และทรัพย์สิน	PR.IP-1: การกำหนดค่าพื้นฐานของเทคโนโลยีสารสนเทศ/ระบบควบคุมอุตสาหกรรมถูกสร้างขึ้น และคงไว้ซึ่งหลักการด้านความปลอดภัย (เช่น แนวคิดของการทำงานน้อยที่สุด) ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 5 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	ข้อมูลพื้นฐานมีประโยชน์สำหรับการสร้างชุดของฟังก์ชันที่ระบบจำเป็นต้องดำเนินการ เพื่อให้สามารถประเมินความเบี่ยงเบนใด ๆ จากเส้นพื้นฐานนั้นเพื่อหาความเสี่ยงทางไซเบอร์ที่อาจเกิดขึ้นได้ การเปลี่ยนแปลงการกำหนดค่าโดยไม่ได้รับอนุญาตสามารถใช้เป็นตัวบ่งชี้การโจมตีที่เป็นอันตราย ซึ่งอาจนำไปสู่การแนะนำของมัลแวร์เรียกค่าไถ่
	PR.IP-3:กระบวนการควบคุมการเปลี่ยนแปลงการกำหนดค่าอยู่ในสถานที่ ISO/IEC 27001:2013 A.12.1.2, A.12.5.1,	กระบวนการเปลี่ยนแปลงการกำหนดค่าที่เหมาะสมสามารถช่วยบังคับใช้การอัปเดตความปลอดภัยในเวลาที่เหมาะสมกับซอฟต์แวร์ รักษาการตั้งค่าการกำหนดค่าความ

มหาวิทยาลัยรังสิต Rangsit University

	A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	ปลอดภัยที่จำเป็น และไม่แนะนำให้เปลี่ยน
	NIST SP 800-53 Rev. 5 CM-3, CM-4, SA-10 PR.IP-4: การสำรองข้อมูลจะถูกดำเนินการ บำรุงรักษา และทดสอบ ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 5 CP-4, CP-6, CP-9	รหัสด้วยผลิตภัณฑ์ที่มีมัลแวร์หรือไม่เป็นไปตามนโยบายการจัดการการเข้าถึง การสำรองข้อมูลปกติที่ได้รับการดูแลและทดสอบมีความจำเป็นต่อการกู้คืนจากเหตุการณ์มัลแวร์เรียกค่าไถ่ในเวลาที่เหมาะสมและไม่ลำบาก การสำรองข้อมูลควรมีความปลอดภัยเพื่อให้แน่ใจว่าจะไม่ได้รับความเสียหายจากมัลแวร์เรียกค่าไถ่
	PR.IP-9: แผนรับมือเหตุการณ์ (การตอบสนองต่อเหตุการณ์และความต่อเนื่องทางธุรกิจ) และแผนการกู้คืน (การกู้คืนเหตุการณ์ และการกู้คืนจากภัยพิบัติ) อยู่ในสถานที่ และจัดการISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3NIST SP 800-53 Rev. 5 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	แผนการตอบกลับ และการกู้คืนควรมีเหตุการณ์มัลแวร์เรียกค่าไถ่ สำเนาของแผนการเผชิญเหตุควรเก็บไว้แบบออฟไลน์ในกรณีที่เหตุการณ์ดังกล่าวทำให้ไม่สามารถเข้าถึงสำเนาที่เก็บไว้ภายในเครือข่ายเป้าหมายได้ เหตุการณ์มัลแวร์เรียกค่าไถ่ควรได้รับการจัดลำดับความสำคัญอย่างเหมาะสมในระหว่างการพิจารณาเหตุการณ์โดยมีเป้าหมายในการจำกัดทันทีเพื่อป้องกันการแพร่กระจายของมัลแวร์เรียกค่าไถ่
	PR.IP-10: แผนการตอบสนองและการกู้คืนได้รับการทดสอบ ISO/IEC 27001:2013 A.17.1.3	แผนการตอบสนอง และการกู้คืนของมัลแวร์เรียกค่าไถ่ควรได้รับการทดสอบเป็นระยะเพื่อให้แน่ใจว่าความเสี่ยงและสมมติฐานและ

มหาวิทยาลัยรังสิต Rangsit University

	NIST SP 800-53 Rev. 5 CP-4, IR-3, PM-14	กระบวนการตอบสนองเป็นปัจจุบันเกี่ยวกับภัยคุกคามมัลแวร์เรียกค่าไถ่ที่พัฒนาขึ้น การทดสอบแผนการตอบสนอง และการกู้คืนควรรวมถึง ICS ที่เกี่ยวข้อง จำเป็นต้องอับเดตและบำรุงรักษาที่ต้องการ และโครงสร้างขององค์กรที่เปลี่ยนแปลง
Maintenance (PR.MA): การบำรุงรักษา และการซ่อมแซมส่วนประกอบระบบสารสนเทศ และการควบคุมอุตสาหกรรมเป็นไปตามนโยบาย และขั้นตอน	PR.MA-2: การบำรุงรักษาทรัพย์สินขององค์กรจากระยะไกลได้รับการอนุมัติ บันทึก และดำเนินการในลักษณะที่ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 5 MA-4	การบำรุงรักษาระยะไกลให้ช่องทางการเข้าถึงเครือข่ายและเทคโนโลยีหากไม่ได้รับการจัดการอย่างเหมาะสม อาชญากรอาจใช้การเข้าถึงนี้เพื่อแก้ไขการกำหนดค่าเพื่ออนุญาตให้มีการนำมัลแวร์เข้ามาการบำรุงรักษาส่วนประกอบระบบทั้งหมดจากระยะไกลโดยองค์กรหรือผู้ให้บริการต้องได้รับการตรวจสอบเพื่อให้แน่ใจว่ากระบวนการนี้ไม่ได้ให้การเข้าถึงแบ็คดอร์ไปยัง OT หรือเครือข่ายไอที
Protective Technology (PR.PT): โซลูชันการรักษาความปลอดภัยทางเทคนิคได้รับการจัดการเพื่อให้มั่นใจในความปลอดภัย และความยืดหยุ่นของระบบ และทรัพย์สิน สอดคล้องกับนโยบาย ขั้นตอน	PR.PT-1: บันทึกการตรวจสอบ/บันทึกจะถูกกำหนด จัดทำเป็นเอกสาร นำไปใช้ และทบทวนตามนโยบาย ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 5 AU-1, AU-2, AU-3, AU-4, AU-5,	ความพร้อมใช้งานของบันทึกการตรวจสอบบันทึกสามารถช่วยในการตรวจจับพฤติกรรมที่ไม่คาดคิดและสนับสนุนกระบวนการตอบสนองทางนิติเวช และการกู้คืน

และข้อตกลงที่เกี่ยวข้อง	AU-6, AU-7, AU-8, AU-9, AU-10, AU-12, AU-13, AU-14, AU-16	
	PR.PT-3: หลักการของการทำงานน้อยที่สุดถูกรวมเข้าด้วยกันโดยการกำหนดค่าระบบเพื่อให้มีความสามารถที่จำเป็นเท่านั้น ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 5 AC-3, CM-7	การรักษาหลักการของการทำงานที่น้อยที่สุดอาจป้องกันการเคลื่อนไหวระหว่างระบบเป้าหมายที่อาจเกิดขึ้น (เช่น การย้ายเข้าสู่ระบบควบคุมกระบวนการปฏิบัติงานจากเครือข่ายการบริหาร)
หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์ (Detect)		
Anomalies and Events (DE.AE): ตรวจพบกิจกรรมผิดปกติและเข้าใจผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์	DE.AE-3: ข้อมูลเหตุการณ์ถูกรวบรวม และเชื่อมโยงจากแหล่งที่มา และเซ็นเซอร์หลายตัว ISO/IEC 27001:2013 A.12.4.1, A.16.1.7NIST SP 800-53 Rev. 5 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	แหล่งที่มาและเซ็นเซอร์หลายตัวพร้อมกับโซลูชันการจัดการข้อมูลความปลอดภัย และเหตุการณ์ (SIEM) ช่วยเพิ่มการมองเห็นเครือข่าย ช่วยในการตรวจหามัลแวร์เรียกค่าไถ่ตั้งแต่เนิ่น ๆ และช่วยในการทำความเข้าใจว่ามัลแวร์เรียกค่าไถ่อาจแพร่กระจายผ่านเครือข่ายได้อย่างไร
Anomalies and Events (DE.AE): ตรวจพบกิจกรรมผิดปกติและเข้าใจ	DE.AE-3: ข้อมูลเหตุการณ์ถูกรวบรวม และเชื่อมโยงจากแหล่งที่มา และเซ็นเซอร์หลายตัว	ตรวจหามัลแวร์เรียกค่าไถ่ตั้งแต่เนิ่น ๆ และช่วยในการทำความเข้าใจว่ามัลแวร์เรียกค่าไถ่อาจแพร่กระจายผ่านเครือข่ายได้อย่างไร การพิจารณาผลกระทบของ

ผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์	ISO/IEC 27001:2013 A.12.4.1, A.16.1.7NIST SP 800-53 Rev. 5 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 DE.AE-4: กำหนดผลกระทบของเหตุการณ์ ISO/IEC 27001:2013 A.16.1.4NIST SP 800-53 Rev. 5 CP-2, IR-4, RA-3, SI-4 DE.CM-1: เครือข่ายถูกตรวจสอบเพื่อตรวจจับ	เหตุการณ์สามารถแจ้งลำดับความสำคัญในการตอบสนองและการกู้คืนสำหรับการโจมตีของมัลแวร์เรียกค่าไถ่

ตารางที่ 2.3 คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนองและกู้คืนจากเหตุการณ์มัลแวร์เรียกค่าไถ่ (ต่อ)

หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์ (Detect)		
Security Continuous Monitoring (DE.CM): ระบบข้อมูลแลทรัพย์สินได้รับการตรวจสอบเพื่อระบุเหตุการณ์ความปลอดภัยทางไซเบอร์ และตรวจสอบประสิทธิภาพของมาตรการป้องกัน	เหตุการณ์ความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น NIST SP 800-53 Rev. 5 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	การตรวจสอบเครือข่ายอาจตรวจพบการบุกรุก และเริ่มดำเนินการป้องกันก่อนที่จะสามารถแทรกโค้ดที่เป็นอันตรายหรือข้อมูลจำนวนมากได้รับการเข้ารหัส และกรองออก
	DE.CM-3: กิจกรรมของบุคลากรได้รับการตรวจสอบเพื่อตรวจจับเหตุการณ์ความ	การตรวจสอบกิจกรรมของบุคลากรอาจตรวจพบภัยคุกคามจากภายในหรือแนวทางปฏิบัติของพนักงานที่ไม่

	ปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 5 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	ปลอดภัยหรือข้อมูลประจำตัวที่ถูกบุกรุกและขัดขวางกิจกรรมของมัลแวร์เรียกค่าไถ่ที่อาจเกิดขึ้น
	DE.CM-4: ตรวจพบรหัสที่เป็นอันตราย ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 5 SI-3, SI-8	การตรวจจับอาจบ่งชี้ว่ามีเหตุการณ์มัลแวร์เรียกค่าไถ่เกิดขึ้นหรือกำลังจะเกิดขึ้น โค้ดที่เป็นอันตรายมักจะไม่ถูกเรียกใช้ในทันที ดังนั้นอาจมีเวลาระหว่างการแทรกโค้ดที่เป็นอันตรายและการเปิดใช้งานเพื่อตรวจหาโค้ดก่อนที่จะดำเนินการโจมตีมัลแวร์เรียกค่าไถ่
	DE.CM-7: มีการตรวจสอบบุคลากร การเชื่อมต่อ อุปกรณ์ และซอฟต์แวร์ที่ไม่ได้รับอนุญาต ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 5 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	บุคคลที่ไม่ได้รับอนุญาต การเชื่อมต่ออุปกรณ์ และซอฟต์แวร์เป็นแหล่งข้อมูลที่อาจใช้โจมตีมัลแวร์เรียกค่าไถ่ การตรวจสอบสามารถตรวจจับการโจมตีของมัลแวร์เรียกค่าไถ่จำนวนมากก่อนที่จะดำเนินการ
	DE.CM-8: มีการสแกนช่องโหว่ ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 5 RA-5	ช่องโหว่สามารถถูกโจมตีได้ในระหว่างการโจมตีของมัลแวร์เรียกค่าไถ่ การสแกนเป็นประจำช่วยให้องค์กรสามารถตรวจจับและบรรเทาช่องโหว่ส่วนใหญ่ได้ก่อนที่จะใช้เพื่อเรียกใช้มัลแวร์เรียกค่าไถ่

มหาวิทยาลัยรังสิต Rangsit University

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1:บทบาทและความรับผิดชอบในการตรวจจับได้รับการกำหนดไว้อย่างดีเพื่อให้แน่ใจว่ามีความรับผิดชอบ ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 5 CA-2, CA-7, PM-14	ความเข้าใจที่ชัดเจนเกี่ยวกับบทบาทและความรับผิดชอบเป็นกุญแจสำคัญในการรับผิดชอบและสนับสนุนให้ปฏิบัติตามนโยบาย และขั้นตอนขององค์กรเพื่อช่วยตรวจจับการโจมตีของมัลแวร์เรียกค่าไถ่
	DE.DP-2: กิจกรรมการตรวจจับเป็นไปตามข้อกำหนดที่เกี่ยวข้องทั้งหมด ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 5 AC-25, CA-2, CA-7, PM-14, SI-4, SR-9	กิจกรรมการตรวจจับควรดำเนินการตามนโยบาย และขั้นตอนขององค์กร
	DE.DP-3: กระบวนการตรวจจับได้รับการทดสอบ ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 5 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	การทดสอบช่วยให้มั่นใจได้ถึงกระบวนการตรวจจับที่ถูกต้องสำหรับการโจมตีโดยใช้มัลแวร์เรียกค่าไถ่โดยไม่ทราบว่าความพยายามในการบุกรุกทั้งหมดจะถูกตรวจพบ การทดสอบจะฝึกคนที่จะต้องดำเนินการตามแผน
	DE.DP-4: มีการสื่อสารข้อมูลการตรวจจับเหตุการณ์ ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 5	การสื่อสารอย่างทันท่วงทีของเหตุการณ์ผิดปกติเป็นสิ่งจำเป็นสำหรับความสามารถในการดำเนินการแก้ไขก่อนที่การโจมตี

มหาวิทยาลัยรังสิต Rangsit University

	AU-6, CA-2, CA-7, RA-5, SI-4	ของมัลแวร์เรียกค่าไถ่จะรับรู้ได้อย่างเต็มที่
	DE.DP-5: กระบวนการตรวจจับได้รับการปรับปรุงอย่างต่อเนื่อง ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 5 CA-2, CA-7, PL-2, PM-14, RA-5, SI-4	กลยุทธ์ที่ใช้ในการโจมตีมัลแวร์เรียกค่าไถ่นั้นได้รับการปรับปรุงอย่างต่อเนื่อง ดังนั้นกระบวนการตรวจจับจึงต้องพัฒนาอย่างต่อเนื่องเพื่อให้ทันกับภัยคุกคามใหม่ ๆ
Response Planning (RS.RP): กระบวนการ และขั้นตอนการตอบสนองจะได้รับการดำเนินการ และบำรุงรักษาเพื่อให้แน่ใจว่ามีการตอบสนองต่อเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ตรวจพบ	RS.RP-1: แผนรับมือจะดำเนินการในระหว่างหรือหลังเหตุการณ์ ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 5 CP-2, CP-10, IR-4, IR-8	ประชาสัมพันธ์ และการสื่อสารของแผนเผชิญเหตุเป็นสิ่งจำเป็นเพื่อหยุดการทุจริตหรือการกรองข้อมูลอย่างต่อเนื่อง ยับยั้งการแพร่กระจายของการติดไวรัสไปยังระบบ และเครือข่ายอื่น ๆ และเริ่มส่งข้อความที่สงวนไว้เพื่อลดความเสียหายเพิ่มเติม รวมถึงชื่อเสียงหรือความเสียหายทางกฎหมาย

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนองและกู้คืน จากเหตุการณ์มัลแวร์เรียกค่าไถ่ (ต่อ)

หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
	การรับมือภัยคุกคาม (Respond)	
Response Planning (RS.RP): กระบวนการ และขั้นตอนการตอบสนองจะได้รับการดำเนินการ และบำรุงรักษาเพื่อให้แน่ใจว่ามีการตอบสนองต่อเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ตรวจพบ	RS.RP-1: แผนรับมือจะดำเนินการในระหว่างหรือหลังเหตุการณ์ ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 5 CP-2, CP-10, IR-4, IR-8	การดำเนินการทันทีขององค์ประกอบการประชาสัมพันธ์ และการสื่อสารของแผนเผชิญเหตุเป็นสิ่งจำเป็นเพื่อหยุดการทุจริตหรือการกรองข้อมูลอย่างต่อเนื่อง ยับยั้งการแพร่กระจายของการติดไวรัสไปยังระบบ และเครือข่ายอื่น ๆ และเริ่มส่งข้อความที่สงวนไว้เพื่อลดความเสียหายเพิ่มเติม รวมถึงชื่อเสียงหรือความเสียหายทางกฎหมาย
Communications (RS.CO): กิจกรรมตอบสนองได้รับการประสานงานกับผู้มีส่วนได้ส่วนเสียภายใน และภายนอก (เช่น การสนับสนุนจากหน่วยงานบังคับใช้กฎหมาย)	RS.CO-1: บุคลากรรู้บทบาทและลำดับการปฏิบัติงานเมื่อต้องการคำตอบ ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 5 CP-2, CP-3, IR-3, IR-8	การตอบสนองต่อเหตุการณ์มัลแวร์เรียกค่าไถ่มีทั้งการตอบสนองทางเทคนิค และทางธุรกิจ การตอบสนองที่มีประสิทธิผล และประสิทธิผลต้องการให้ทุกฝ่ายเข้าใจบทบาท และความรับผิดชอบของตน บทบาทการตอบสนองด้านการสื่อสารควรมีการจัดทำเป็นเอกสารอย่างเป็นทางการในแผนเผชิญเหตุ และการกู้คืน และควรเสริมด้วยการใช้แผน

มหาวิทยาลัยรังสิต Rangsit University

	RS.CO-2: มีการรายงานเหตุการณ์ที่สอดคล้องกับเกณฑ์ที่กำหนดไว้ ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 5 AU-6, IR-6, IR-8	การตอบสนองต่อเหตุการณ์มัลแวร์เรียกค่าไถ่มีทั้งการตอบสนองทางเทคนิค และทางธุรกิจ การตอบสนองที่มีประสิทธิผล และประสิทธิผลต้องการเกณฑ์ที่กำหนดไว้ล่วงหน้าสำหรับการรายงาน และการปฏิบัติตามเกณฑ์เหล่านั้นในระหว่างเหตุการณ์
	RS.CO-3: ข้อมูลถูกแบ่งปันสอดคล้องกับแผนการตอบสนอง ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 5 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	ลำดับความสำคัญในการแบ่งปันข้อมูลรวมถึงการป้องกันการแพร่กระจายของการติดไวรัสไปยังระบบ และเครือข่ายอื่น ๆ รวมถึงการส่งข้อความแบบยึดเอาเสียก่อน
	RS.CO-4: การประสานงานกับผู้มีส่วนได้ส่วนเสียเกิดขึ้นสอดคล้องกับแผนเผชิญเหตุ ISO/IEC 27001:2013 Clause 7.4NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-8	การประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายใน และภายนอกมีความสำคัญต่อการจัดลำดับความสำคัญ เช่น การป้องกันการแพร่กระจายของข้อมูลที่ไม่ถูกต้องและการสร้างข้อความเชิงป้องกัน
	RS.CO-5: การแบ่งปันข้อมูลโดยสมัครใจเกิดขึ้นกับผู้มีส่วนได้ส่วนเสียภายนอกเพื่อให้เกิดการรับรู้ถึงสถานการณ์ความปลอดภัยทางไซเบอร์ในวงกว้าง	การแบ่งปันข้อมูลอาจให้ผลประโยชน์ทางนิติเวช และลดผลกระทบ และความสามารถในการทำกำไรของการโจมตีด้วยมัลแวร์เรียกค่าไถ่ การแบ่งปันโดยสมัครใจควรส่งเสริมข้อกำหนดด้านกฎระเบียบหรือการ

มหาวิทยาลัยรังสิต Rangsit University

	ISO/IEC 27001:2013 A.6.1.4NIST SP 800-53 Rev. 5 PM-15, SI-5	ปฏิบัติตามข้อกำหนดอื่น ๆ สำหรับการรายงานและการแบ่งปัน
Analysis (RS.AN): การวิเคราะห์ดำเนินการเพื่อให้แน่ใจว่ามีการตอบสนองที่มีประสิทธิภาพ และสนับสนุนกิจกรรมการกู้คืน	RS.AN-1: ตรวจสอบการแจ้งเตือนจากระบบตรวจจับ ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 5 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	การแจ้งเตือนจากระบบตรวจจับควรได้รับการตรวจสอบอย่างทันท่วงทีและทันท่วงที เนื่องจากสิ่งเหล่านี้มักบ่งชี้ถึงการโจมตีของมัลแวร์เรียกค่าไถ่ในช่วงแรก ๆ เพื่อให้สามารถระงับหรือลดผลกระทบได้
	RS.AN-2: เข้าใจผลกระทบของเหตุการณ์ ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 5 CP-2, IR-4	การทำความเข้าใจผลกระทบจะเป็นตัวกำหนดการดำเนินการตามแผนฟื้นฟู องค์กรควรพยายามทำความเข้าใจผลกระทบทางเทคนิคของการโจมตีด้วยมัลแวร์เรียกค่าไถ่ (เช่น ระบบใดที่ไม่พร้อมใช้งาน) จากนั้นจึงเข้าใจผลกระทบที่จะเกิดขึ้นกับธุรกิจ (เช่น กระบวนการทางธุรกิจที่ไม่สามารถจัดส่งได้) สิ่งนี้จะช่วยให้แน่ใจว่าการตอบสนอง และความพยายามในการกู้คืนได้รับการจัดลำดับความสำคัญและทรัพยากรอย่างเหมาะสม และสามารถดำเนินการตามแผนความต่อเนื่องทางธุรกิจได้ในระหว่างนี้
	RS.AN-3: การตรวจพิสูจน์จะดำเนินการ	การตรวจพิสูจน์ช่วยระบุสาเหตุที่แท้จริงในการกักเก็บ และกำจัดการโจมตี รวมถึงการรีเซ็ตรหัสผ่านของ

มหาวิทยาลัยรังสิต Rangsit University

	ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 5 AU-7, IR-4	ข้อมูลประจำตัวที่ถูกขโมยโดยผู้โจมตี การลบมัลแวร์ที่ผู้โจมตีใช้และการลบกลไกการคงอยู่ที่ใช้โดยผู้โจมตี นิติเวชยังสามารถแจ้งกระบวนการกู้คืน และช่วยในการรายงาน และแบ่งปันการดำเนินการ
	RS.AN-5: กระบวนการถูกสร้างขึ้นเพื่อรับ วิเคราะห์ และตอบสนองต่อช่องโหว่ที่เปิดเผยต่อองค์กรจากแหล่งภายในและภายนอก NIST SP 800-53 Rev. 5 PM-15, SI-5	กระบวนการวิเคราะห์สามารถป้องกันการโจมตีที่ประสบความสำเร็จในอนาคต และการแพร่กระจายของมัลแวร์เรียกค่าไถ่ไปยังระบบ และเครือข่ายอื่นๆ นอกจากนี้ยังสามารถช่วยฟื้นฟูความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย
Mitigation (RS.MI): มีการดำเนินกิจกรรมเพื่อป้องกันการขยายเหตุการณ์ลดผลกระทบ และแก้ไขเหตุการณ์	RS.MI-1: มีเหตุการณ์ยับยั้ง ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 5 IR-4	ต้องดำเนินการทันทีเพื่อป้องกันการแพร่กระจายของมัลแวร์เรียกค่าไถ่ไปยังระบบ และเครือข่ายอื่น ลดผลกระทบ และแก้ไเหตุการณ์ การกักกันมัลแวร์เรียกค่าไถ่รวมถึง ICS ที่เกี่ยวข้อง
	RS.MI-2: อุบัติการณ์บรรเทาลง ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 5 IR-4	ต้องดำเนินการทันทีเพื่อแยกมัลแวร์เรียกค่าไถ่ออกเพื่อลดความเสียหายต่อข้อมูล ป้องกันการติดเชื้อไม่ให้แพร่กระจายภายในเครือข่าย ระบบและเครือข่ายอื่น ๆ และลดผลกระทบต่อภารกิจหรือธุรกิจ
	RS.MI-3: ช่องโหว่ที่ระบุใหม่ได้รับการบรรเทาหรือบันทึกเป็นความเสี่ยงที่ยอมรับ	การจัดการช่องโหว่ลดความน่าจะเป็นของการโจมตี มัลแวร์เรียกค่าไถ่ ที่ประสบความสำเร็จ หากไม่สามารถแก้ไขหรือบรรเทาจุดอ่อนได้ การ

	ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 5 IR-4	บันทึกความเสี่ยงนี้อย่างน้อยก็อนุญาตให้รวมไว้ในการตัดสินใจในอนาคต และให้ความโปร่งใสสำหรับผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบจากเหตุการณ์มัลแวร์เรียกค่าไถ่
Improvements (RS.IM): กิจกรรมการตอบสนองขององค์กรได้รับการปรับปรุงโดยการรวมบทเรียนที่เรียนรู้จากกิจกรรมการตรวจจับการตอบสนองในปัจจุบันและก่อนหน้า	RS.IM-1: แผนการตอบสนองรวมบทเรียนที่ได้เรียนรู้ ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-8	วิธีนี้ช่วยลดความน่าจะเป็นของการโจมตีมัลแวร์เรียกค่าไถ่ที่ประสบความสำเร็จในอนาคต และสามารถช่วยฟื้นฟูความมั่นใจในส่วนของผู้มีส่วนได้ส่วนเสีย
	RS.IM-2: กลยุทธ์การตอบสนองได้รับการปรับปรุง ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev 5 CP-2, IR-4, IR-8	วิธีนี้ช่วยลดความน่าจะเป็นของการโจมตีมัลแวร์เรียกค่าไถ่ที่ประสบความสำเร็จในอนาคต และสามารถช่วยฟื้นฟูความมั่นใจในหมู่ผู้มีส่วนได้ส่วนเสีย
หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
การกู้คืนข้อมูล และระบบหลังเกิดเหตุภัยคุกคามไซเบอร์ (Recovery)		
Recovery Planning (RC.RP): กระบวนการ และขั้นตอนการกู้คืนได้รับการดำเนินการ และ	RC.RP-1: แผนการกู้คืนจะดำเนินการในระหว่างหรือหลังเหตุการณ์ความปลอดภัยทางไซเบอร์	การเริ่มแผนฟื้นฟูทันทีหลังจากระบุสาเหตุที่แท้จริงแล้ว สามารถลดการสูญเสียได้

มหาวิทยาลัยรังสิต Rangsit University

บำรุงรักษาเพื่อให้แน่ใจว่ามีการคืนค่าระบบหรือทรัพย์สินที่ได้รับผลกระทบจากเหตุการณ์ความ	ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 5 CP-10, IR-4, IR-8

ตารางที่ 2.3 คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนองและกู้คืนจากเหตุการณ์มัลแวร์เรียกค่าไถ่ (ต่อ)

หมวดหมู่	หมวดหมู่ย่อยและข้อมูลที่เลือกมาอ้างอิง	การประยุกต์ใช้เพื่อป้องกันมัลแวร์เรียกค่าไถ่ในแต่ละหัวข้อ
การกู้คืนข้อมูล และระบบหลังเกิดเหตุภัยคุกคามไซเบอร์ (Recovery)		
ปลอดภัยทางไซเบอร์.		
Improvements (RC.IM): การวางแผน และกระบวนการฟื้นฟูได้รับการปรับปรุงโดยนำบทเรียนที่เรียนรู้ไปใช้กับกิจกรรมในอนาคต	RC.IM-1: แผนการกู้คืนรวมบทเรียนที่เรียนรู้ ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev 5 CP-2, IR-4, IR-8	วิธีนี้ช่วยลดความน่าจะเป็นของการโจมตีมัลแวร์เรียกค่าไถ่ที่ประสบความสำเร็จในอนาคต และสามารถช่วยฟื้นฟูความมั่นใจในหมู่ผู้มีส่วนได้ส่วนเสีย
	RC.IM-2: อัปเดตกลยุทธ์การกู้คืน ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-8	นี่เป็นสิ่งจำเป็นเพื่อรักษาประสิทธิภาพของการวางแผนฉุกเฉินสำหรับการโจมตีมัลแวร์เรียกค่าไถ่ในอนาคต
Communications (RC.CO): กิจกรรมการฟื้นฟูได้รับการประสานงานกับฝ่ายภายใน และภายนอก	RC.CO-1: มีการจัดการประชาสัมพันธ์ ISO/IEC 27001:2013 A.6.1.4, Clause 7.4	ซึ่งช่วยลดผลกระทบทางธุรกิจโดยการเปิดกว้าง และโปร่งใส และคืนความมั่นใจให้กับผู้มีส่วนได้ส่วนเสีย

(เช่น ศูนย์ ประสานงาน ผู้ ให้บริการอินเทอร์เน็ต เจ้าของระบบโจมตี เหยื่อ CSIRT อื่น ๆ และผู้ขาย)		
	RC.CO-2: ชื่อเสียงได้รับการซ่อมแซมหลังจากเหตุการณ์ที่เกิดขึ้น ISO/IEC 27001:2013 Clause 7.4	การซ่อมแซมชื่อเสียงช่วยลดผลกระทบทางธุรกิจ และฟื้นฟูความเชื่อมั่นในหมู่ผู้มีส่วนได้ส่วนเสีย
	RC.CO-3: กิจกรรมการกู้คืนจะถูกสื่อสารไปยังผู้มีส่วนได้ส่วนเสียภายใน และภายนอกตลอดจนผู้บริหารและทีมผู้บริหาร ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 5 CP-2, IR-4	การสื่อสารเกี่ยวกับกิจกรรมการกู้คืนช่วยลดผลกระทบทางธุรกิจ และฟื้นฟู และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย

ที่มา: แนวทางปฏิบัติของนิสต์เฟรมเวิร์ค, 2565

นิสต์เฟรมเวิร์กนี้ได้ปรับล่าสุดในเดือนกุมภาพันธ์ ปี ค.ศ. 2022 ซึ่งแบ่งออกเป็น 5 ฟังก์ชันหลัก แต่ละฟังก์ชันหลักจะแบ่งออกเป็นฟังก์ชันย่อย ๆ พร้อมระบุเอกสารอ้างอิง เช่น ISO/IEC 27001:2013 , COBIT 5, NIST SP800-53 เพื่อนำกระบวนหรือแนวทางปฏิบัติจากเอกสารเหล่านั้นมาใช้เพื่อดำเนินการตามฟังก์ชันย่อย ๆ เหล่านี้ได้ทันที ในการสนับสนุนการป้องกัน ตอบสนอง และกู้คืน จากเหตุการณ์โจมตีจากมัลแวร์เรียกค่าไถ่ สามารถนำมาวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจยังคงดำเนินต่อไปได้อย่างต่อเนื่อง

มหาวิทยาลัยรังสิต Rangsit University

2.9 งานวิจัยที่เกี่ยวข้อง

ในหัวข้อนี้จะแบ่งออกเป็น 2 หัวข้อย่อย ได้แก่ บทความวิจัยจากต่างประเทศ และบทความจากเว็บไซต์ต่างประเทศ

2.9.1 บทความวิจัยจากต่างประเทศ

งานวิจัยของ Anant (2020) มัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ที่โจมตีการป้องกันระบบโดยใช้การเข้ารหัสที่เป็นอันตราย ตระกูลมัลแวร์เรียกค่าไถ่สมัยใหม่ เข้ารหัสไฟล์บางประเภทบนระบบที่ถูกบุกรุก การโจมตีไม่ได้มุ่งเป้าไปที่บุคคลใดบุคคลหนึ่งเท่านั้น แต่ยังมีองค์กร และสถาบันจำนวนมากที่เกี่ยวข้องด้วย ภัยคุกคามใหม่ต่อภาคการศึกษา และองค์กรที่คล้ายคลึงกันมีศูนย์กลางอยู่ที่นี่ การระบุที่เป็นไปได้ วิธีการป้องกัน และการตอบสนองต่อการโจมตีมัลแวร์เรียกค่าไถ่ที่เพิ่มขึ้น ซึ่งอธิบายไว้เพื่อต่อสู้มัลแวร์เรียกค่าไถ่ อย่างมีประสิทธิภาพ เหตุผลหลักของการวิจัยนี้คือ การระบุและทำความเข้าใจการทำงานของการเข้ารหัสมัลแวร์เรียกค่าไถ่ และทำความเข้าใจวิธีที่เป็นไปได้ในการตอบโต้ก่อนที่จะโจมตีระบบ และเครือข่ายของเรา การปฏิบัติตามวิธีการที่นำเสนอในบทความนี้ด้วยการวิเคราะห์อย่างรอบคอบสามารถป้องกัน และหลีกเลี่ยงการโจมตีของมัลแวร์เรียกค่าไถ่ได้อย่างมีประสิทธิภาพ

งานวิจัยของ Nagaraja and Rubia (2020) มัลแวร์เรียกค่าไถ่เป็นมัลแวร์ที่ป้องกันไม่ให้ผู้ใช้เข้าถึงระบบหรือจำกัดการใช้งานระบบ จะโจมตี และทำการล็อคหน้าจอของระบบหรือไฟล์ของผู้ใช้จึงป้องกันไม่ให้เข้าถึงหรือใช้งานได้ มีการเรียกร้องค่าไถ่ และการเข้าถึงถูกปฏิเสธเว้นแต่จะมีการจ่ายค่าไถ่ ทุกวันนี้ มัลแวร์เรียกค่าไถ่ สมัยใหม่บางตัว เรียกรวมกันว่าคริปโตมัลแวร์เรียกค่าไถ่ (crypto ransomware) สามารถเข้ารหัสไฟล์บางประเภทบนระบบที่ติดไวรัสได้ ผู้ใช้จะถูกบังคับให้จ่ายค่าไถ่ผ่านวิธีการชำระเงินออนไลน์ เพื่อรับคีย์ถอดรหัส เหตุการณ์เรียกค่าไถ่มีเป้าหมายที่องค์กรต่าง ๆ ทั่วทั้งอุตสาหกรรมและตามภูมิภาคและก่อให้เกิดภัยคุกคามต่อการโจมตีที่ก่อกวนและทำลายล้าง จุดประสงค์ของบทความนี้คือเพื่อตรวจสอบและ สร้างความตระหนักเกี่ยวกับการโจมตีของมัลแวร์เรียกค่าไถ่ ผลกระทบ และมาตรการป้องกันทางเทคนิค

งานวิจัยของ Juan, Lorena, Angel ,and Myriam (2019) สถานการณ์ปัจจุบันใน ไม่เพียงแต่เกี่ยวกับวิวัฒนาการ แต่ยังรวมถึงประเด็น และอนาคตด้วย ความท้าทาย แบบสำรวจนี้ยังมีการจัดหมวดหมู่บทความมัลแวร์เรียกค่าไถ่ตามการตรวจจับ และแนวทางการป้องกัน ในช่วงไม่กี่ปีมานี้ ภัยคุกคามอาชญากรรมทางอินเทอร์เน็ตได้เติบโตขึ้นอย่างมาก ซึ่งทำให้ ระบบ และอุปกรณ์ได้รับความเสียหายต่อด้านความปลอดภัย และเป็นอันตรายต่อการดำเนินธุรกิจขององค์กร ในบริบทนี้มัลแวร์เรียกค่าไถ่ใช้ประโยชน์จากการเข้ารหัสเพื่อประนีประนอมข้อมูลผู้ใช้หรือปฏิเสธการเข้าถึงระบบปฏิบัติการ ผู้โจมตีเข้ารหัสข้อมูลของเหยื่อเพื่อจ่ายค่าไถ่เพื่อเข้าถึง คืนสภาพข้อมูล หรือเก็บข้อมูลที่เป็นส่วนตัว ปัจจุบันการนำ (Situational Awareness: SA) และองค์ความรู้มาใช้เป็นแนวทาง สามารถอำนวยความสะดวกในการระบุภัยคุกคามมัลแวร์เรียกค่าไถ่อย่างรวดเร็ว เอสเอช่วยให้รู้ว่าคือ อะไรเกิดขึ้นในอุปกรณ์ที่ถูกบุกรุก และการสื่อสารในเครือข่ายได้ผ่านการตรวจสอบ

งานวิจัยของ Antonina et al. (2021) การโจมตีของมัลแวร์เรียกค่าไถ่ได้กลายเป็นภัยคุกคามความปลอดภัยทางไซเบอร์ที่สำคัญซึ่งข้อมูลที่สำคัญ ถูกโจมตีเข้ารหัส เมื่อระบบได้รับการโจมตีมัลแวร์เรียกค่าไถ่ ล่าสุดพบว่าใช้เทคนิคออฟเฟรชเคชั่น (Obfuscation) ขั้นสูงพร้อมกับความสามารถของเซิร์ฟเวอร์ซีทู C2 แบบออฟไลน์กำลังโจมตีผู้ใช้รายบุคคล และองค์กรขนาดใหญ่ ปัญหานี้ทำให้เกิดการหยุดชะงักของธุรกิจ และการสูญเสียทางการเงินอย่างแน่นอน เนื่องจากไม่มีเฟรมเวิร์กรวมที่สามารถจำแนก ตรวจจับและบรรเทาการโจมตีของมัลแวร์เรียกค่าไถ่ได้ในครั้งเดียว จึงมีแรงจูงใจที่จะนำเสนอการป้องกันการหลีกเลี่ยงการตรวจจับดีเอเอ็ม (DAM) ซึ่งเป็นกรอบทฤษฎีในการทบทวน และจัดประเภทเทคนิค เครื่องมือ และกลยุทธ์ในการตรวจจับ หลีกเลี่ยง และบรรเทา มัลแวร์เรียกค่าไถ่ เราควรมีตรวจสอบสถานการณ์ต่าง ๆ อย่างละเอียด และเปรียบเทียบการทบทวนเหตุการณ์ในปัจจุบัน

งานวิจัยของ Kamalanathan, Sethuraman, Krishanshree, and Venkat (2022) มัลแวร์คือ ซอฟต์แวร์อันตรายที่ติดตั้งในอุปกรณ์ของผู้อื่น มัลแวร์รวมถึงไวรัส สปายแวร์ มัลแวร์เรียกค่าไถ่ และโทรจัน ตัวอย่างเช่น โทรจัน มีชื่อว่า Trick Bot Banking ถูกใช้เป็นเครื่องมือเพื่อปรับใช้อายิวมัลแวร์เรียกค่าไถ่ เพื่อทำให้เกิด มัลแวร์เรียกค่าไถ่ การโจมตีในโรงพยาบาล มีการโจมตีมัลแวร์เรียกค่าไถ่เพิ่มขึ้นร้อยละ 7 ในภาคการดูแลสุขภาพในสหรัฐอเมริกาในช่วงเดือนตุลาคม 2020 และ อายิวมัลแวร์เรียกค่าไถ่อยู่เบื้องหลังร้อยละ 75 ของเหตุการณ์เหล่านี้

2.9.2 บทความจากเว็บไซต์ต่างประเทศ

งานวิจัยของ Ivan (2022) คริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่เป็นมัลแวร์เรียกค่าไถ่ที่กำหนดเป้าหมายอุปกรณ์ไมโครซอฟท์วินโดวส์เกิดขึ้นครั้งแรกในเดือนกันยายน 2556 ในการโจมตีต่อเนื่องจนถึงเดือนพฤษภาคมของปีถัดไป มัลแวร์เลือกเข้ารหัสข้อมูล ทำให้ผู้ใช้ไม่สามารถเข้าถึงไฟล์ได้ เมื่อเข้ารหัสแล้วข้อมูลจะถูกเรียกค่าไถ่โดยผู้โจมตีซึ่งถือคีย์การเข้ารหัส เหยื่อจะต้องจ่ายค่าไถ่ภายใน 72 ชั่วโมงเพื่อรับไฟล์คืนจากคริปโตล็อคเกอร์ โดยทั่วไปแล้ว คริปโตล็อคเกอร์จะการโจมตีส่งผ่านไฟล์แนบอีเมลที่ติดไวรัสและลิงก์จากผู้ส่งที่ไม่รู้จัก เมื่อผู้รับอีเมลที่ไม่สงสัยคลิกลิงก์หรือไฟล์แนบที่ติดไวรัส มัลแวร์จะเข้ารหัสไฟล์และเก็บคีย์ไว้ในเซิร์ฟเวอร์ของคริปโตล็อคเกอร์เอง จากนั้นเหยื่อจะได้รับข้อความเรียกค่าไถ่ กระบวนการเข้ารหัสแบบกุญแจไม่สมมาตร (Asymmetric Key Encryption) เป็นกระบวนการเข้ารหัสที่เปิดให้ผู้ส่งข้อมูลกับผู้รับข้อมูลสามารถใช้กุญแจคนละชุดกัน ที่สร้างมาคู่กันโดยเฉพาะ แล้วสร้างการเชื่อมต่อที่เข้ารหัสถึงกันได้

งานวิจัยของ Michael (2020) คริปโตล็อคเกอร์เป็นมัลแวร์ที่รู้จักกันดีซึ่งอาจสร้างความเสียหายโดยเฉพาะอย่างยิ่งสำหรับองค์กรที่ขับเคลื่อนด้วยข้อมูล เมื่อรหัสถูกดำเนินการ มันจะเข้ารหัสไฟล์บนเดสก์ท็อปและเครือข่ายที่ใช้ร่วมกัน และ "เก็บมันไว้เพื่อเรียกค่าไถ่" แจ้งให้ผู้ใช้ที่พยายามเปิดไฟล์นั้นจ่ายค่าธรรมเนียมในการถอดรหัส มัลแวร์อย่างคริปโตล็อคเกอร์ สามารถเข้าสู่เครือข่ายที่มีการป้องกันผ่านเวกเตอร์ต่าง ๆ รวมถึงอีเมล เว็บไซต์แบ่งปันไฟล์ และการดาวน์โหลดตัวแปรใหม่ ๆ สามารถประสบความสำเร็จในการหลีกเลี่ยงเทคโนโลยีป้องกันไวรัสและไฟร์วอลล์ และมีการพัฒนาที่ทันสมัยในการโจมตีมีการปรับเปลี่ยนตลอดเวลา ที่สามารถเลี่ยงมาตรการป้องกันได้ อัปเดตในเดือนกันยายน พ.ศ. 2561 การโจมตีของมัลแวร์เรียกค่าไถ่ลดลงอย่างมากตั้งแต่จุดสูงสุดในปี พ.ศ. 2560 คริปโตล็อคเกอร์และรูปแบบต่าง ๆ ของ คริปโตล็อคเกอร์ไม่ได้กระจายในวงกว้างอีกต่อไป และมัลแวร์เรียกค่าไถ่ตัวใหม่ได้เข้าครอบครอง มัลแวร์เรียกค่าไถ่ได้พัฒนาเป็นการโจมตีแบบกำหนดเป้าหมายมากกว่ารูปแบบการกระจายแบบกว้างแบบก่อนหน้านี้ และยังคงเป็นภัยคุกคามต่อธุรกิจและหน่วยงานของรัฐ[19]

จากบทความ With Ransomware like CryptoWall, CryptoLocker & Chimera what's in store for 2016 (2022) มัลแวร์เรียกค่าไถ่มีหลายประเภท ได้แก่ Crypto Wall, CryptoLocker, Torrent Locker, Chimera, TeslaCrypt และ CTB-Locker มัลแวร์เรียกค่าไถ่ที่เข้ามาใหม่คือแรนซัมสามสอง (Ransom32) ถูกออกแบบมาบนแนวคิดของ Software-as-a-Service (SaaS) ซึ่งได้รับการขนานนามว่าเป็น JavaScript ransomware ตัวแรก คริปโตล็อคเกอร์ดั้งเดิมยังคงอ้างสิทธิ์เหยื่อรายใหม่ ต้นปี พ.ศ. 2558 American Electric Power ซึ่งเป็นผู้ให้บริการระบบจ่ายไฟฟ้ารายใหญ่

ที่สุดในสหรัฐอเมริกา ติดไวรัสเมื่อหัวหน้างานเปิดอีเมลส่วนตัวในแล็ปท็อป (Laptop) ของบริษัท ได้รับข้อความทักทายบนหน้าจอคอมพิวเตอร์ แสดงหน้าป๊อบอับ (Pop-Up) ไฟล์ทั้งหมดของคุณถูกเข้ารหัสด้วยการเข้ารหัส RSA-2048 เป็นไปไม่ได้ที่จะกู้คืนไฟล์ของคุณหากไม่มีรหัสส่วนตัว แจ้งเรียกค่าเป็นเงินสกุลเป็นบิตคอยน์ต้องส่ง 0.7 บิตคอยน์ เพื่อแลกกับพีซีที่ได้รับผลกระทบแต่ละเครื่องหรือ 3 บิตคอยน์ เพื่อรับคีย์ส่วนตัวทั้งหมดสำหรับพีซีที่ได้รับผลกระทบทั้งหมด

2.10 ตารางสรุปบทความที่เกี่ยวข้อง

ในหัวข้อนี้จะกล่าวถึงงานวิจัยที่เกี่ยวข้อง (18) แสดงในตารางที่ 2.4 ภัยคุกคามไซเบอร์ที่เกิดจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมในโรงอุตสาหกรรมและบทความการนำเสนอแนวทางการป้องกันภัยคุกคามทางไซเบอร์จากมัลแวร์เรียกค่าไถ่

ตารางที่ 2.4 สรุปงานวิจัยที่เกี่ยวข้อง

		งานวิจัยที่เกี่ยวข้อง								
เรื่องที่เกี่ยวข้อง		OT/ICS	Ransomware	CryptoLocker	NIST	Identify	Protect	Detect	Respond	Recovery
งานวิจัยที่ / ปีที่ / จำนวนที่เกี่ยวข้อง		5	12	6	4	14	12	9	5	4
1	2019		X		X	X	X	X	X	X
2			X		X	X	X	X	X	X
3	2020		X	X		X				
4		X	X	X		X	X			
5			X	X		X	X	X		
6			X	X			X	X		
7	2021		X	X		X				
8			X		X	X	X	X	X	X
9		X						X		

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.4 สรุปงานวิจัยที่เกี่ยวข้อง (ต่อ)

งานวิจัยที่เกี่ยวข้อง										
เรื่องที่เกี่ยวข้อง		OT/ICS	Ransomware	CryptoLocker	NIST	Identify	Protect	Detect	Respond	Recovery
งานวิจัยที่ / ปีที่ / จำนวนที่เกี่ยวข้อง		5	12	6	4	14	12	9	5	4
10	2021		X					X		
11		X				X	X			
12		X				X				
13			X	X				X		
14						X	X			
15						X	X			
16						X	X			
17	2022		X		X	X	X	X	X	X
18		X	X			X	X		X	
งานวิจัยนี้		X	X	X	X	X	X	X	X	X

ที่มา: รวบรวมโดยผู้วิจัย, 2566

จากตารางที่ 2.4 สรุปงานวิจัยที่เกี่ยวข้อง ดังนี้

ตารางที่ 2.5 งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้อง			
ลำดับ	ปี ค.ศ.	ชื่อผู้วิจัย/ชื่อเรื่อง	สิ่งที่นำเสนอ
1.	2019	Jitti and Susan (2019) A Survey on Preventing	ได้กล่าวถึง Machine Learning มีศักยภาพในการป้องกัน Crypto Ransomware โดยการเรียนรู้พฤติกรรมและรูปแบบการโจมตี ซึ่งช่วยเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคาม

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.5 งานวิจัยที่เกี่ยวข้อง (ต่อ)

งานวิจัยที่เกี่ยวข้อง			
ลำดับ	ปี ค.ศ.	ชื่อผู้วิจัย/ชื่อเรื่อง	สิ่งที่นำเสนอ
		Crypto Ransomware Using Machine Learning.	แม้จะเป็นสายพันธุ์ใหม่ ๆ เนื่องจากพฤติกรรมที่เปลี่ยนแปลงไปของมัลแวร์เรียกค่าไถ่ ระบบการเรียงลำดับและการระบุตัวตนแบบธรรมดาจึงไม่สามารถค้นพบมัลแวร์เรียกค่าไถ่รูปแบบใหม่ได้ อย่างมีประสิทธิภาพ คริปโตมัลแวร์เรียกค่าไถ่เป็นอันตรายที่เข้ารหัสไฟล์ของผู้ใช้ในเวลาเดียวกันกับการซ่อนคีย์ถอดรหัสจนกว่าผู้เสียหายจะจ่ายค่าไถ่
2.	2019	Huang et al CSAT: A User-interactive Cyber Security Architecture Tool based on NIST-compliance Security Controls for Risk Management.	ได้กล่าวถึง การพัฒนาเครื่องมือชื่อ CSAT (Cyber Security Architecture Tool) ที่ช่วยให้องค์กรประเมินและจัดการความเสี่ยงทางไซเบอร์ได้ง่ายขึ้น โดยอ้างอิงตามมาตรฐาน NIST โดยเครื่องมือนี้จะสามารถโต้ตอบและมีอินเทอร์เฟซที่เป็นมิตรต่อผู้ใช้ ทำให้องค์กรสามารถประเมินและปรับปรุงระบบได้ตามข้อกำหนดด้านความปลอดภัยของ NIST สามารถจัดการความเสี่ยงด้านความปลอดภัยเป็นส่วนสำคัญของการพัฒนาระบบ และระบบข้อมูลอื่น ๆ ที่ต้องการความปลอดภัยโดยเฉพาะอย่างยิ่ง NIST ได้พัฒนาความปลอดภัยทางไซเบอร์ เช่น SP-800-53 เพื่อเป็นแนวทางในการจัดการความเสี่ยง
3.	2020	Li and Hankin Scalable approach to	ได้กล่าวถึง การเสนอแนวทางที่น่าสนใจ ในการเพิ่มความปลอดภัย และความยืดหยุ่น ให้กับระบบ ICS ซึ่งเป็นสิ่งสำคัญ ในยุคที่ภัยคุกคาม

		enhancing ICS resilience by network diversity.	ไซเบอร์ การแบ่งเครือข่ายออกเป็นส่วนย่อย ๆ เพื่อจำกัดขอบเขตความเสียหาย หากส่วนใดส่วนหนึ่งถูกโจมตี และ ใช้ซอฟต์แวร์และฮาร์ดแวร์ที่หลากหลายในระบบ เพื่อป้องกันมัลแวร์ที่ออกแบบมาโจมตีระบบเฉพาะเจาะจง ระบบควบคุมในอุตสาหกรรมเป็นระบบไซเบอร์ในภาคอุตสาหกรรม สมัยใหม่ได้มีการดำเนินการที่หลากหลายในโครงสร้างพื้นฐานด้านไอทีและเทคโนโลยีปฏิบัติการส่งผลให้เกิดระบบควบคุมในอุตสาหกรรมที่เชื่อมต่อระหว่างกัน การแบ่งเครือข่ายย่อย จึงสามารถปรับปรุงความยืดหยุ่นของเครือข่ายต่อต้านการแพร่กระจายของมัลแวร์สภาพแวดล้อมทางอุตสาหกรรมที่มีประสิทธิภาพ
4.	2020	Nagaraja Ransomware Threats.	ได้กล่าวถึงว่าคริปโต มัลแวร์เรียกค่าไถ่ (Crypto Ransomware) ซึ่งเป็นมัลแวร์ที่เข้ารหัสไฟล์ของผู้ใช้ ทำให้ไม่สามารถเข้าถึงระบบหรือข้อมูลได้ มัลแวร์ประเภทนี้สามารถโจมตีองค์กรต่าง ๆ ได้หลากหลายวิธี เช่น การส่งอีเมลฟิชชิ่ง หรือใช้ช่องโหว่ของระบบ ผู้เขียนยังแนะนำมาตรการป้องกัน เช่น การอัปเดตระบบอย่างสม่ำเสมอ และการใช้ซอฟต์แวร์ป้องกันไวรัสที่มีประสิทธิภาพเพื่อตรวจสอบและสร้างความตระหนักเกี่ยวกับการโจมตีของมัลแวร์เรียกค่าไถ่ ผลกระทบ มาตรการป้องกันและทางเทคนิค
5.	2020	Anant Ransomware Attacks: Impact,	ได้กล่าวถึง การวิเคราะห์ผลกระทบจากการโจมตีด้วย Ransomware ซึ่งเป็นมัลแวร์ที่เข้ารหัสไฟล์และเรียกค่าไถ่ มีการอธิบายถึง

มหาวิทยาลัยรังสิต Rangsit University

		Symptoms, Working, Preventive Measures and Response.	อาการและผลกระทบที่เกิดขึ้น เช่น การสูญเสียข้อมูลและความเป็นส่วนตัว และการเสียโอกาสทางธุรกิจ นอกจากนี้ ยังมีคำแนะนำในการป้องกัน เช่น การสำรองข้อมูล การอัปเดตระบบและใช้โปรแกรมป้องกันมัลแวร์ รวมถึงวิธีตอบโต้เมื่อถูกโจมตี เช่น การแจ้งเตือนหน่วยงานและไม่จ่ายค่าไถ่เพื่อลดการสนับสนุนอาชญากรรมออนไลน์
6.	2020	Ilker Cyber fraud: Detection and analysis of the crypto-ransomware.	ได้กล่าวถึง การวิเคราะห์วิธีการโจมตีและพฤติกรรมของ คริปโตมัลแวร์เรียกค่าไถ่ (Crypto-Ransomware) ที่มีเพิ่มมากขึ้นเรื่อย ๆ ซึ่งสร้างความเสียหายอย่างมากต่อทั้งบุคคลและองค์กร งานวิจัยนี้จึงนำเสนอการดำเนินการประกอบด้วยสามโมดูลหลัก การตรวจจับ การวิเคราะห์ และตอบสนองต่อเหตุการณ์ กับภัยคุกคามของคริปโตล็อคเกอร์ มัลแวร์เรียกค่าไถ่ได้อย่างมีประสิทธิภาพ และแนวทางที่สามารถป้องกันและตอบสนองได้อย่างรวดเร็ว เช่น การสำรองข้อมูลที่สำคัญไว้ในที่ปลอดภัย เช่น External Hard disk หรือ Cloud Storage เพื่อป้องกันการสูญหายของข้อมูล, การอัปเดตซอฟต์แวร์, และการให้ความรู้แก่ผู้ใช้
7.	2021	Marcel et al Cyber resilience for self-monitoring IOT devices.	ได้กล่าวถึง อุปกรณ์ไอโอที (IoT) ปัจจุบันเป็นเป้าหมายที่น่าสนใจสำหรับการโจมตีทางไซเบอร์ ตัวอย่างเช่น สามารถใช้เพื่อปิดการใช้งานทั้งโรงงานและเรียกค่าไถ่ การกู้คืนอุปกรณ์ที่ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ล่าสุดจาก NIST ได้กำหนดแนวคิดและองค์ประกอบพื้นฐานสำหรับ

มหาวิทยาลัยรังสิต Rangsit University

			มาตรการ การป้องกัน การตรวจจับ และการกู้คืน จากการโจมตีมัลแวร์ ตามแนวทางของ NIST การกู้คืนสามารถทำได้หลายวิธีและในระดับต่าง ๆ ได้เสนอสถาปัตยกรรมสำหรับการกู้คืนและการตรวจจับ และนำเสนอการใช้งานที่แตกต่างกันสองแบบโดยกำหนดเป้าหมายไปที่อุปกรณ์ โซลูชันการตรวจจับของเราช่วยให้สามารถกู้คืนได้ทันท่วงที
8.	2021	Ude and Swar Securing Remote Access Networks Using Malware Detection Tools for Industrial Control Systems.	ได้กล่าวถึง ระบบควบคุมอุตสาหกรรมเป็นส่วนสำคัญของการขับเคลื่อนการพัฒนาอุตสาหกรรมของทุกประเทศ แม้จะมีความก้าวหน้าที่สำคัญหลายประการ เช่น การเกษตรควบคุมสิ่งแวดล้อม ระบบรถไฟอัตโนมัติ และบ้านอัจฉริยะ ประสบความสำเร็จในภาคโครงสร้างพื้นฐานที่สำคัญผ่านการบูรณาการระบบสารสนเทศและความสามารถระยะไกลกับระบบควบคุมอุตสาหกรรม ความจริงก็คือความก้าวหน้าเหล่านี้ได้นำช่องโหว่ที่ก่อนหน้านี้ไม่มีอยู่หรือไม่มีนัยสำคัญ หนึ่งในนั้นคือ Remote Access Trojans (RATs)
9.	2021	Antonina et al Ransomware Attacks: Risks, Protection and Prevention Measures.	ได้กล่าวถึง ไอทีสมัยใหม่นำโอกาสที่ยิ่งใหญ่ที่สุดในการดำเนินงานด้วยข้อมูลอิเล็กทรอนิกส์ แต่ทุกวันนี้คอมพิวเตอร์และผู้ใช้อินเทอร์เน็ตสามารถตกเป็นเหยื่อของการโจมตีมัลแวร์เรียกค่าไถ่ได้อย่างง่ายดาย ผู้เชี่ยวชาญด้านไซเบอร์ยังมีความซับซ้อนมากขึ้น ก้าวหน้าขึ้น และมีความตระหนักในมาตรการรักษาความปลอดภัยทางไซเบอร์ที่ทันสมัยมากขึ้น เมื่อเร็ว ๆ นี้ มัลแวร์เรียกค่าไถ่ ชนิดใหม่ปรากฏขึ้นพร้อม

มหาวิทยาลัยรังสิต Rangsit University

			กับฟังก์ชั่น (Function) การแพร่กระจายด้วยตนเอง ความสูญเสียและความเสียหายมีความสำคัญทั่วโลกและมีแนวโน้มเพิ่มขึ้นทุกปี เหยื่อส่วนใหญ่ตกลงที่จะจ่ายค่าไถ่ แต่อาชญากรจำนวนมากในระหว่างการเจรจาเพิ่มยอดเรียกร้องค่าไถ่ เพื่อปกป้องระบบคอมพิวเตอร์และเป็นเจ้าของข้อมูล ควรใช้มาตรการที่ซับซ้อนซึ่งรวมถึงซอฟต์แวร์ระดับมืออาชีพ การลงทุนด้านความรู้ และความระมัดระวังส่วนบุคคล มาตรการเหล่านี้ต้องจัดเป็นสามวิธี ที่สำคัญที่สุดคือโปรแกรมป้องกันซอฟต์แวร์ พวกมันมีราคาแพงและมีประสิทธิภาพเพียงช่วงระยะเวลาหนึ่งเท่านั้น เนื่องจากผู้โจมตีสร้างโปรแกรมมัลแวร์เรียกค่าไถ่รูปแบบใหม่ที่มีความก้าวหน้ามากขึ้น
10.	2021	Giorgio, Vincenzo, & Micro Analysis, prevention and detection of ransomware attacks on Industrial Control Systems.	ได้กล่าวถึง ด้วยการถือกำเนิดของ Industry 4.0 ระบบควบคุมอุตสาหกรรม กำลังกลายเป็นเป้าหมายหลักสำหรับอาชญากรไซเบอร์จำนวนมาก เราเห็นจำนวนการโจมตีมัลแวร์เรียกค่าไถ่ที่ออกแบบมาโดยเฉพาะเพื่อโจมตีและเรียกค่าไถ่ กับระบบควบคุมในอุตสาหกรรมเพิ่มขึ้นอย่างต่อเนื่อง ผลที่ตามมาของการโจมตีเหล่านี้อาจสร้างความเสียหายร้ายแรง เนื่องจากสามารถบล็อกกระบวนการผลิตเป็นเวลาหลายวัน ส่งผลให้สูญเสียรายได้ การโจมตีมัลแวร์เรียกค่าไถ่ ต่อระบบควบคุมในอุตสาหกรรมเราได้พัฒนาระบบป้องกันการบุกรุก และตรวจจับแบบใหม่ที่สามารถตรวจจับและขัดจังหวะการ

มหาวิทยาลัยรังสิต Rangsit University

			เคลื่อนไหวจากการแฝงตัวในระบบเช่น การใช้ Windows Management Instrumentation (WMI) ที่เป็นอันตราย เครื่องมือบนระบบปฏิบัติการคอมพิวเตอร์ ที่ติดตั้งไว้ล่วงหน้า ไฟล์ที่ถ่ายโอนจะถูกแยก จัดเก็บ และวิเคราะห์ผ่านการจับคู่ลายเซ็นเพื่อตรวจสอบว่าเป็นมัลแวร์ที่รู้จักหรือไม่ ในกรณีนั้นวิธีการของเราขัดจังหวะการถ่ายโอนและแยกโฮสต์ที่ถูกบุกรุกซึ่งร้องขอการถ่ายโอนมัลแวร์จากอุปกรณ์เครือข่ายอื่น
11.	2021	Georgios et Industrial and Critical Infrastructure Security: Technical Analysis of real-life security incidents.	ได้กล่าวถึง ระบบควบคุมอุตสาหกรรม (ICS) สามารถแบ่งแนวคิดออกเป็นสองส่วน IT และโอที Operational Technology (OT) ส่วนไอทีให้บริการทั้งหมดที่สนับสนุนการดำเนินธุรกิจประกอบด้วยเวิร์กสเตชัน เซิร์ฟเวอร์และฐานข้อมูล ซึ่งทั้งหมดเชื่อมต่อถึงกันโดยใช้เครือข่ายแบบ IP ส่วนโอที เน้นด้านการปฏิบัติงานของเครื่องจักร ส่วนประกอบหลักของระบบโอที คืออุปกรณ์เฉพาะโดเมน เช่น Programmable Logic Controllers (PLC) และ Variable-Frequency Drives (VFDs)
12.	2021	Urooj, Maarof, & Al-rimy A proposed Adaptive Pre-Encryption Crypto-Ransomware	ได้กล่าวถึง Crypto-ransomware เป็นมัลแวร์ที่ใช้ฟังก์ชันการเข้ารหัสของระบบเพื่อเข้ารหัสข้อมูลผู้ใช้ ผลกระทบที่แก้ไขไม่ได้ของ crypto-ransomware ทำให้ยากต่อการเอาตัวรอดจากการโจมตีเมื่อเทียบกับมัลแวร์ประเภทอื่น ๆ เมื่อการโจมตี crypto-ransomware เข้ารหัสไฟล์ผู้ใช้ การเข้าถึงไฟล์เหล่านี้เป็นเรื่องยากขึ้นหากไม่มีคีย์ถอดรหัส เนื่องจากความพร้อมใช้งาน

มหาวิทยาลัยรังสิต Rangsit University

		Early Detection Model.	ของชุดเครื่องมือพัฒนามัลแวร์เรียกค่าไถ่ เช่น Ransomware as a Service (RaaS) จึงมีการพัฒนาตัวแปรมัลแวร์เรียกค่าไถ่จำนวนมาก สิ่งนี้มีส่วนทำให้เกิดการโจมตี ransomware ที่เพิ่มขึ้นในปัจจุบัน
13.	2021	อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564)	ได้กล่าวถึง การประเมินความเสี่ยงด้านไซเบอร์เป็นขั้นตอนสำคัญในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยเฉพาะอย่างยิ่งเมื่อองค์กรนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนภารกิจต่าง ๆ การประเมินความเสี่ยงช่วยให้สามารถกำหนดมาตรการควบคุมที่เหมาะสม สอดคล้องกับภารกิจ และมีประสิทธิภาพสูงสุด
14.	2021	จิตสุภา ฤทธิผลิน (2564)	ได้กล่าวถึง การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) มีความสำคัญอย่างยิ่งต่อองค์กร เพราะช่วยให้ธุรกิจดำเนินต่อไปได้ แม้เผชิญกับภัยคุกคามไซเบอร์ ส่งผลให้ลูกค้าเกิดความเชื่อมั่น และเพิ่มความได้เปรียบในการแข่งขันได้ กลยุทธ์การคืนสภาพทางไซเบอร์ที่มีประสิทธิภาพ รวมถึงองค์กรควรเตรียมความพร้อมและมีความสามารถในการปรับตัว รวมถึงฟื้นฟูระบบจากการโจมตีทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ โดยยึดหลักแนวคิดที่ว่าระบบป้องกันภัยคุกคามไม่สามารถมีความปลอดภัยได้อย่างสมบูรณ์ทั้งหมด องค์กรจึงควรมุ่งเน้นให้ความสำคัญต่อการพัฒนา 3 องค์ประกอบสำคัญในการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ เทคโนโลยี กระบวนการ และบุคลากร

มหาวิทยาลัยรังสิต Rangsit University

15.	2021	กิตติคุณ มีทองจันทร และวงศ์ยศ เกิดศรี (2564)	ได้กล่าวถึง ปัจจัยที่ส่งผลต่อการเกิดอาชญากรรมทางไซเบอร์ (Cybercrime) อาจมาจากหลายสาเหตุของผู้ใช้แพลตฟอร์มโซเชียลมีเดีย (Social Media) ในพื้นที่กรุงเทพมหานครและปริมณฑล พบว่า ความตระหนักรู้เกี่ยวกับอาชญากรรมไซเบอร์มีผลสำคัญต่ออัตราการเกิดอาชญากรรมทางไซเบอร์กล่าวคือ ยิ่งผู้ใช้มีความตระหนักถึงภัยคุกคามทางไซเบอร์ รูปแบบการโจมตี และวิธีการป้องกันตัว ก็จะยิ่งมีความเสี่ยงน้อยลงที่จะได้รับผลกระทบจากอาชญากรรมไซเบอร์ซึ่งการให้ความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีดิจิทัล รวมถึงความเสี่ยงและวิธีการป้องกันภัยคุกคามไซเบอร์ เป็นแนวทางสำคัญในการลดปริมาณการเกิดอาชญากรรมไซเบอร์ได้
16.	2021	คริชณะ ฉิมมณี และ มณีสุข โชติรุ่งรัตน์ (2564)	ได้กล่าวถึง จากการศึกษาวิธีการโจมตีของมัลแวร์เรียกค่าไถ่เมสแก๊ง (Maze Gang) พบว่า กลุ่มนี้มักแฝงตัวในระบบเครือข่ายระยะหนึ่งเพื่อขโมยข้อมูลก่อนเข้ารหัสไฟล์ ดังนั้นการเฝ้าระวังระบบเครือข่ายอย่างเข้มงวดจึงช่วยตรวจจับและป้องกันการโจมตีได้ กลุ่มผู้ใช้ระบบปฏิบัติการวินโดวส์เป็นเป้าหมายหลักของการโจมตีจากมัลแวร์เรียกค่าไถ่ โดยสอดคล้องกับข้อมูลงานศึกษาวิจัยด้านความปลอดภัยไซเบอร์ของ ทีเจ บอริส (Teejay Boris) พบว่าสถิติแสดงให้เห็นว่าร้อยละ 93 ของมัลแวร์เรียกค่าไถ่มีนามสกุลไฟล์เป็น .exe ซึ่งเป็นไฟล์ทำงานบนระบบปฏิบัติการวินโดวส์ การประยุกต์ใช้

มหาวิทยาลัยรังสิต Rangsit University

			แนวทางป้องกันตาม NISTIR 8374 (ฉบับร่าง) ซึ่งคาดว่าจะออกเป็นฉบับสมบูรณ์ในปี พ.ศ. 2565 จะช่วยเสริมประสิทธิภาพในการป้องกันภัยจากการโจมตีของมัลแวร์เรียกค่าไถ่ได้
17.	2022	Kamalanathan et al Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations.	ได้กล่าวถึง แนะนำเฟรมเวิร์กการรักษาความปลอดภัยทางไซเบอร์ของ NIST และวิเคราะห์ความเหมาะสมของระบบการดูแลสุขภาพในเอเชีย การจัดการความเสี่ยง การจัดการความเสี่ยง และการควบคุมความปลอดภัยของ NIST ได้รับการวิเคราะห์เช่นกัน โดยคำนึงถึงการโจมตีทางไซเบอร์ในเอเชีย การวิเคราะห์นี้ช่วยให้เข้าใจถึงความเหมาะสมของ NIST ในระบบการดูแลสุขภาพของเอเชีย NIST-CSF (สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กรอบความปลอดภัยทางไซเบอร์) แบ่งออกเป็นห้าหน้าที่หลัก: การระบุตัวตน ปกป้อง ตรวจจับ ตอบสนอง และกู้คืนเพื่อจัดการกับการตัดสินใจในการจัดการความเสี่ยง ภัยคุกคามและช่องโหว่ NIST CSF มีโครงสร้างมาตรฐานที่ยืดหยุ่นและปรับเปลี่ยนได้สำหรับการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ปัจจุบันกรอบการบริหารความเสี่ยงของ NIST ได้รับการนำไปใช้โดยองค์กรด้านการดูแลสุขภาพหลายแห่งทั่วโลกเพื่อเป็นพื้นฐาน
18.	2022	Zhang et al Defeat magic with magic: A novel ransomware	ได้กล่าวถึง ระบบควบคุมอุตสาหกรรม (ICS) เป็นสถานที่สาธารณะที่ให้บริการแก่ผู้ใช้จำนวนมาก ดังนั้นการรักษาความปลอดภัยจึงเป็นปัจจัยสำคัญในการวัดความพร้อมใช้งานเสมอ เมื่อเร็ว ๆ นี้ การโจมตีรูปแบบใหม่บน ระบบ

มหาวิทยาลัยรังสิต Rangsit University

	attack method to dynamically generate malicious payloads based on PLC control logic.	ควบคุมอุตสาหกรรม ได้เกิดขึ้นบ่อยครั้ง ซึ่งตระหนักถึงการขู่กรรโชกของผู้ใช้โดยการบุกรุกโดเมนข้อมูลและทำลายโดเมนทางกายภาพ อย่างไรก็ตาม เนื่องจากความหลากหลายและความไม่พร้อมใช้งานของตรรกะการควบคุมระบบควบคุมอุตสาหกรรม เป้าหมายของการโจมตีดังกล่าวมักจะจำกัดอยู่ที่พีซีและเซิร์ฟเวอร์เท่านั้น การโจมตีมัลแวร์เรียกค่าไถ่ระบบควบคุมอุตสาหกรรมสามารถคุกคามได้มากกว่าเดิม เนื่องจาก ICS จำนวนมากเกี่ยวข้องกับความปลอดภัย จึงต้องศึกษาวิธีการโจมตีที่เป็นไปได้ของมัลแวร์เรียกค่าไถ่ระบบควบคุมอุตสาหกรรม เพื่อป้องกัน ระบบควบคุมอุตสาหกรรมจากการบุกรุกในอนาคต

ที่มา: รวบรวมโดยผู้วิจัย, 2566

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 3

วิธีวิทยาการวิจัย

การวิจัยเรื่อง “แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ในระบบควบคุมอุตสาหกรรมของกลุ่มอุตสาหกรรมผลิตชิ้นส่วนอิเล็กทรอนิกส์ กรณีศึกษาจากเหตุการณ์ที่เกิดจริง” เพื่อใช้เป็นแนวทางในการบริหารความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในบริษัทวิทยานิพนธ์ฉบับนี้เป็นงานวิจัยเชิงผสานวิธีซึ่งประกอบไปด้วย 1) กระบวนวิธีการวิจัยเชิงเอกสาร (Documentary Research) 2) การวิจัยเชิงทดลอง (True Experiment) และ 3) การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group โดยมีขอบเขตในการดำเนินการศึกษาวิจัย ดังต่อไปนี้

3.1 กรอบแนวคิด

3.2 แนวทางการป้องกันและการประยุกต์ใช้ที่นำเสนอ

3.2.1 แนวทางป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมบนพื้นฐานจากแนวทางปฏิบัติ ของเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม

3.2.2 โมเดลการนำไปใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการและระบบควบคุมอุตสาหกรรม กรณีศึกษาโรงงานอุตสาหกรรมขนาดใหญ่

3.3 การทดลอง

การทดลองแบ่งออกเป็น 2 ส่วนหลัก ได้แก่ ส่วนแรก คือ การวิเคราะห์การโจมตีในการทดลองที่ 1 และ 2 ส่วนที่สอง คือ แนวทางการป้องกันในการทดลองที่ 3

3.3.1 การทดลองที่ 1: การวิเคราะห์การโจมตีโดยมี 3 กรณีศึกษาโดยใช้การวิจัยเชิงเอกสาร (Documentary Research)

3.3.2 การทดลองที่ 2: การวิเคราะห์การโจมตีโดยมี 1 การวิจัยเชิงทดลอง(True Experiment)

3.3.3 การทดลองที่ 3: แนวทางการป้องกัน โดยใช้การวิจัยเชิงคุณภาพการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

3.4 เครื่องมือในใช้ในการวิจัย

3.4.1 การทดลองที่ 2: ไฟร์วอลล์ (Firewall) และ อีดีอาร์ (EDR)

3.4.2 การทดลองที่ 3: แบบสอบถาม

3.5 การเก็บรวบรวมข้อมูล

มหาวิทยาลัยรังสิต Rangsit University

3.5.1 การทดลองที่ 2: บันทึกเหตุการณ์จาก ไฟร์วอลล์ (Firewall) และ อีดีอาร์ (EDR)

3.5.2 การทดลองที่ 3: จากการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

3.6 การวิเคราะห์ข้อมูล

3.6.1 การทดลองที่ 2: กรอบแนวคิดไมโครซอฟท์ (Microsoft Framework) และไมเตอร์แอทแทค (MITRE ATT&CK)

3.6.2 การทดลองที่ 3: การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

3.1 กรอบแนวคิด

รูปที่ 3.1 กรอบแนวคิดบทความวิชาการ

กรอบแนวคิดของงานวิจัยฉบับนี้ได้ แสดงลำดับขั้นตอนวิธีการวิจัยเชิงผสานวิธี ดังรูปที่ 3.1

3.2 แนวทางการป้องกันและการประยุกต์ใช้ที่นำเสนอ

3.2.1 แนวทางป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมบนพื้นฐานจากแนวทางปฏิบัติ ของเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS)

มัลแวร์เรียกค่าไถ่เป็นภัยคุกคามร้ายแรงต่อระบบควบคุมอุตสาหกรรม (ICS) ซึ่งควบคุมกระบวนการทางกายภาพที่สำคัญในภาคส่วนต่าง ๆ เช่น เทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม การหยุดชะงักของระบบเหล่านี้อาจก่อให้เกิดความเสียหายทางกายภาพ และความสูญเสียทางการเงินอย่างมาก ดังนั้นการป้องกันมัลแวร์เรียกค่าไถ่จึงมีความสำคัญอย่างยิ่ง แนวทางป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรม บนพื้นฐานจากแนวทางปฏิบัติประกอบด้วยดังนี้

3.2.1.1 การแบ่งส่วนเครือข่าย แยกเครือข่าย OT ออกจากเครือข่าย IT และแบ่งส่วนภายในเครือข่าย OT เพื่อจำกัดการเคลื่อนที่ของมัลแวร์

3.2.1.2 การจัดการช่องโหว่ ประเมิน จัดลำดับความสำคัญ และแก้ไขช่องโหว่ของระบบเป็นประจำ รวมถึงการอัปเดตซอฟต์แวร์และเฟิร์มแวร์

3.2.1.3 การควบคุมการเข้าถึง ใช้การตรวจสอบสิทธิ์แบบหลายปัจจัยหลักการสิทธิ์น้อยที่สุด และการจัดการข้อมูลประจำตัวที่แข็งแกร่ง เพื่อจำกัดการเข้าถึงระบบ ICS

3.2.1.4 การสำรองข้อมูล สำรองข้อมูลสำคัญเป็นประจำและทดสอบการกู้คืนข้อมูลเพื่อให้แน่ใจว่าสามารถกู้คืนระบบได้อย่างรวดเร็วในกรณีที่เกิดการโจมตี

3.2.1.5 การตรวจสอบความปลอดภัย ตรวจสอบกิจกรรมเครือข่ายและระบบเพื่อตรวจจับและตอบสนองต่อกิจกรรมที่เป็นอันตราย ใช้ระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) เพื่อเพิ่มความปลอดภัย

3.2.1.6 การฝึกอบรมบุคลากร ให้ความรู้แก่บุคลากรเกี่ยวกับภัยคุกคามจากมัลแวร์เรียกค่าไถ่ แนวทางปฏิบัติที่ดีที่สุดด้านความปลอดภัยทางไซเบอร์ และวิธีการระบุและรายงานกิจกรรมที่น่าสงสัย

3.2.1.7 แผนการตอบสนองเหตุการณ์ พัฒนาและทดสอบแผนการตอบสนองเหตุการณ์ เพื่อจัดการกับเหตุการณ์มัลแวร์เรียกค่าไถ่ รวมถึงขั้นตอนการบรรจุ การกู้คืน และการสื่อสาร

การดำเนินการตามแนวทางเหล่านี้ องค์กรสามารถลดความเสี่ยงจากมัลแวร์เรียกค่าไถ่ในระบบ ICS และปกป้องทรัพย์สิน การดำเนินงาน และชื่อเสียงขององค์กรได้

3.2.2 โมเดลการนำไปใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) กรณีศึกษาโรงงานอุตสาหกรรมขนาดใหญ่

การเลือกโมเดลการใช้งานเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม ขึ้นอยู่กับปัจจัยหลายอย่าง องค์กรควรพิจารณาความต้องการและข้อจำกัดของตนเองเพื่อเลือกโมเดลที่เหมาะสมและมีประสิทธิภาพสูงสุด

เพอร์ดูโมเดล (Purdue Model) สำหรับการจัดการในเทคโนโลยีเชิงปฏิบัติการ และ ระบบควบคุมอุตสาหกรรมในโรงงานอุตสาหกรรมขนาดใหญ่ เป็นแบบจำลองสถาปัตยกรรมที่ใช้กันอย่างแพร่หลายในการออกแบบและจัดการระบบควบคุมอุตสาหกรรม โดยเอ็นไอเอสทีเวอร์ชัน (Version) SP 800-82r3 ซึ่งเป็นเฟรมเวิร์ก มุ่งเน้นไปที่การแนะนำแนวทางปฏิบัติสำหรับการรักษาความปลอดภัยเทคโนโลยีเชิงปฏิบัติการ เฟรมเวิร์กนี้อธิบายถึงวิธีการรักษาความปลอดภัยเทคโนโลยีเชิงปฏิบัติการ โดยพิจารณาข้อกำหนดด้านประสิทธิภาพ ความน่าเชื่อถือ และความปลอดภัยที่เหมาะสม เฟรมเวิร์กได้ครอบคลุมระบบและอุปกรณ์ที่ติดตั้งโปรแกรมได้หลากหลาย ซึ่งสื่อสารระหว่างกันในสภาพแวดล้อมเชิงปฏิบัติการ และได้กล่าวถึงเพอร์ดูโมเดล (Purdue Model)ซึ่งได้เสนอแนะพิเศษในหน้า 71 ถึงหน้า 75 โมเดลนี้เน้นการแบ่งระบบออกเป็นเลเยอร์ (Layer) เพื่อแยกฟังก์ชันการทำงาน ของระบบควบคุมอุตสาหกรรม การจัดการ และการวางแผน ออกจากกัน เพื่อเพิ่มประสิทธิภาพ และความปลอดภัยเพื่อป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์จากมัลแวร์เรียกค่าไถ่ (Ransomware) โดยเป็นเชื่อมต่อระหว่างส่วนงานเทคโนโลยีสารสนเทศส่วนงานเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม

3.3 การทดลอง

3.3.1 การทดลองที่ 1 : การวิเคราะห์การโจมตีโดยมี 3 กรณีศึกษาโดยใช้การวิจัยเชิงเอกสาร (Documentary Research)

Alamri (2022) จากเว็บไซต์ดาร์กอต ปี พ.ศ. 2565 พบว่า การโจมตีมัลแวร์เรียกค่าไถ่ทั้งหมดในไตรมาสที่ 1 มีเป้าหมายไปที่ภาคการผลิตคิดเป็นร้อยละ 75 มัลแวร์เรียกค่าไถ่กลายเป็นเวกเตอร์โจมตีอันดับหนึ่งในบรรดาองค์กรอุตสาหกรรม โดยภาคการผลิตเป็นภาคส่วนที่ตกเป็นเป้าหมายมากที่สุด ในการโจมตีด้วยมัลแวร์เรียกค่าไถ่ที่มีการพัฒนาอย่างต่อเนื่อง มีการโจมตีด้วยขั้นตอนที่หลากหลายและซับซ้อนในระบบควบคุมอุตสาหกรรม ดังนั้น การวิจัยเชิงเอกสาร (Documentary Research) ในวิทยานิพนธ์ฉบับนี้ จึงได้ศึกษาเหตุการณ์การโจมตีทางไซเบอร์จากมัลแวร์เรียกค่าไถ่ที่เกิดขึ้นจริง จำนวน 3 กรณีศึกษา (Case Study)

3.3.1.1 กรณีศึกษาที่ 1 บริษัท Asteelflash บริษัทแอสตีลแฟลช (Asteelflash) ดำเนินงานโรงงาน 18 แห่ง และศูนย์ อาร์แอนด์ดี (R&D) สองแห่ง มีพนักงาน 6,200 คน และมีรายได้ต่อปีมากกว่าหนึ่งพันล้านยูโร บริการการผลิตอุปกรณ์อิเล็กทรอนิกส์ของฝรั่งเศส (EMS) เป็นบริการการผลิตอุปกรณ์อิเล็กทรอนิกส์ระดับไฮเอนด์จากโรงงานอัจฉริยะที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์โดยแก๊งแรนซั่มแวร์เรฟวิล (REvil) เมื่อวันที่ 2 เมษายน ปี ค.ศ. 2021 โดยยืนยันว่าบริษัทเป็นผู้ได้รับผลกระทบจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่ส่งผลกระทบต่อเซิร์ฟเวอร์ที่ถูกโจมตีประสบความสำเร็จในการเข้ารหัสไฟล์บนระบบที่ได้รับผลกระทบและเป็นผู้เรียกร้องค่าไถ่ 24 ล้านเหรียญ ผู้คุกคามได้แชร์ไฟล์ชื่อ 'asteelflash_data_part1.7z' ซึ่งแชร์เพื่อพิสูจน์ว่าไฟล์ถูกขโมยระหว่างการโจมตี จุดเริ่มต้นอาจเป็นบริการไมโครซอฟท์ อาร์พีซี (Microsoft RPC) ที่เปิดเผยซึ่งมีอยู่ตั้งแต่เดือนพฤศจิกายนปีที่แล้ว การโจมตีของ REvil มีความแตกต่างในการรับช่องโหว่ใหม่ ๆ แต่เทคนิคของพวกเขาทับซ้อนกับกลุ่มอื่น ๆ โดยอาศัยเครื่องมือขโมยข้อมูลส่วนตัวอย่าง “Mimikatz” โดยใช้เครื่องมืออย่างพีเอส เอ็กเซ็ก (PS Exec) (Lawrence, 2021)

รูปที่ 3.2 แสดงการเรียกค่าไถ่ของแรนซั่มแวร์ REvil จากการโจมตีทางไซเบอร์บริษัท Asteelflash

ที่มา: Lawrence, 2021

3.3.1.2 กรณีศึกษาที่ 2 บริษัท Foxconn Electronics Manufacturer ด้วยประสบการณ์มากกว่า 35 ปีในการผลิตผลิตภัณฑ์อิเล็กทรอนิกส์ซึ่งผลิตคอมพิวเตอร์ ทีวีแอลซีดี (LCD) อุปกรณ์พกพา และกล่องรับสัญญาณ ซึ่งเดิมใช้โดยระบบ Sony, Motorola และ Cisco โดยบริษัทฟ็อกซ์คอนน์ (Foxconn) ได้ยืนยันว่าหนึ่งในบริษัทที่มีฐานอยู่ในเม็กซิโก โรงงานผลิตโรงงานในตีฮัวนาเป็นแห่งที่สองที่โดนมัลแวร์เรียกค่าไถ่โจมตีในเวลาไม่ถึงสองปี การโจมตีครั้งแรกเกิดขึ้นเมื่อวันที่ 29 พฤศจิกายน 2020 โดยมัลแวร์เรียกค่าไถ่แบบดอปเปลเพย์เมอร์ (DoppelPaymer Ransomware) ผู้โจมตีเรียกค่าไถ่ 34 ล้านดอลลาร์และอ้างว่าขโมยข้อมูล 100GB เข้ารหัสระหว่างเซิร์ฟเวอร์ 1,200 ถึง 1,400 เครื่อง และทำลายข้อมูลสำรอง 20 TB ถึง 30TB และการโจมตีครั้งที่สองโดย LockBit 2.0 ransomware เมื่อวันที่ 31 พฤษภาคม 2022 โดยเผยแพร่ ประกาศแจ้งว่าจะทำการรั่วไหลข้อมูลที่ได้ขโมยจากบริษัทฟ็อกซ์คอนน์เว้นแต่จะมีการจ่ายค่าไถ่ภายในวันที่ 11 มิถุนายน 2022 แรนซั่มแวร์ล็อกบิต (LockBit) ได้รับการพิจารณาจากหลายหน่วยงานให้เป็นส่วนหนึ่งของตระกูลมัลแวร์ “LockerGoga & MegaCortex” การโจมตีเป็นแบบแพร่กระจายตัวเอง กำหนดเป้าหมาย และใช้เครื่องมือที่คล้ายกัน ขั้นตอนของการโจมตีแบบล็อกบิตมีสามขั้นตอนโดยประมาณคือ เจาะระบบ แทรกซึม และปรับใช้ (Bill, 2022)

LockBit claiming Foxconn as victim *(KELA)*

รูปที่ 3.3 แสดงการเรียกค่าไถ่ของแรนซั่มแวร์ Lock Bit จากการโจมตีทางไซเบอร์บริษัท Foxconn
ที่มา: Bill, 2022

3.3.1.3 กรณีศึกษาที่ 3 บริษัท Panasonic บริษัทพานาโซนิค (Panasonic) ยักษ์ใหญ่ด้านเทคโนโลยีของญี่ปุ่นยืนยันว่าการดำเนินงานของแคนาดาถูกแรนซั่มแวร์คอนติ Conti Ransomware (RaaS) โจมตีในเดือนกุมภาพันธ์ ปี ค.ศ. 2021 การโจมตีมี

เป้าหมายและส่งผลกระทบต่อเซิร์ฟเวอร์ เครือข่าย และกระบวนการบางอย่างแรนซั่มแวร์คอนติ ได้อ้างว่าพวกเขาใช้ทรัพยากรบุคคลและข้อมูลทางบัญชีประมาณ 3 กิกะไบต์ ผู้บุกรุกเข้าถึงระบบของบริษัทได้นานกว่าสี่เดือนก่อนที่จะถูกตรวจพบและตามรายงาน ผู้คุกคามสามารถเข้าถึงข้อมูลที่เป็นความลับของลูกค้าและพนักงานได้ ซึ่งแรนซั่มแวร์คอนติได้ทำการอัปโหลด (Upload) ไฟล์เหล่านั้นที่รั่วไหลของไฟล์สู่ออนไลน์ในเดือนพฤศจิกายน ปี ค.ศ. 2021 บริษัทได้ยอมรับว่าเครือข่ายนั้น “เข้าถึงโดยมิชอบด้วยกฎหมายโดยบุคคลที่สาม” และในบันทึกเหตุการณ์พบว่าข้อมูลบางส่วนบนเซิร์ฟเวอร์ไฟล์ ได้มีการถูกเข้าถึงระหว่างการหยุดชะงัก และในเดือนตุลาคม ปี ค.ศ. 2020 แฮ็กเกอร์ได้แบ่งปันข้อมูลสี่กิกะไบต์ไปยังไฟล์ที่รั่วไหลทางออนไลน์ รวมถึงข้อมูลทางการเงินและที่อยู่อีเมล (Teri, 2022)

รูปที่ 3.4 แสดงการเรียกค่าไถ่ของแรนซัมแวร์ Conti จากการโจมตีทางไซเบอร์ บริษัท Panasonic

ที่มา: Teri, 2022

3.3.2 การทดลองที่ 2 : การวิเคราะห์การโจมตีโดยมี 1 การวิจัยเชิงทดลอง (True Experiment)

เนื่องจากลำดับเหตุการณ์ของการโจมตีและพยานหลักฐานดิจิทัลเป็นสิ่งที่สำคัญที่ใช้ในการสืบสวนและการวิเคราะห์ ดังนั้น การวิจัยเชิงทดลอง (True Experiment) ในวิทยานิพนธ์ฉบับนี้จึงได้ศึกษาเหตุการณ์การโจมตีทางไซเบอร์จากมัลแวร์เรียกค่าไถ่ที่เกิดขึ้นจริงพร้อมลำดับเหตุการณ์ของการโจมตีและพยานหลักฐานดิจิทัลจำนวน 1 กรณีศึกษา (Real Case Study) ดังนี้ บริษัท ABC Technology (ชื่อสมมุติ) เป็นโรงงานที่มีระบบเครื่องอัตโนมัติที่มีความแม่นยำซึ่งเชี่ยวชาญในการออกแบบ พัฒนา ในการผลิต ซึ่งมีโรงงานผลิตหนึ่งแห่งในประเทศไทยและอีกสอง

แห่งในจีน การโจมตีทางไซเบอร์เริ่มที่เครื่องจักรที่ควบคุมด้วยคอมพิวเตอร์ 3 เครื่องบนระบบปฏิบัติการวินโดว์ (Windows) 10 รุ่น 1809 ซึ่งเป็นเครื่องจักรที่ควบคุมด้วยคอมพิวเตอร์ในสายการผลิตเทคโนโลยีเชิงปฏิบัติงานที่ใช้ในระบบควบคุมอุตสาหกรรม พบว่ามีเครื่องที่ควบคุมด้วยคอมพิวเตอร์เครื่องหนึ่งได้ทำการเข้ารหัสไฟล์ข้อมูล การเข้าถึงเบื้องต้นคือบริการระยะไกลภายนอกโดยโปรแกรมทีมวีเวอร์ (TeamViewer) จากซัพพลายเออร์ (Supplier) บริการติดตั้งโปรแกรมจากภายนอก เนื่องจากการติดตั้งดำเนินการโดยบัญชีในโลคอล แก๊งมัลแวร์เรียกค่าไถ่จึงใช้การอนุญาตนี้ สำหรับการเคลื่อนไหวโจมตีไปยังเครื่องอื่นซึ่งพบว่ามีสองวิธี 1)แบบผ่าน USB และ 2) HTTP 80 พบว่าขั้นตอนสุดท้ายในการโจมตีได้กำหนดเวลาถูกตั้งค่าให้รัน “Update.exe” โดยอัตโนมัติเป็นเครื่องมือบนระบบปฏิบัติการวินโดว์สำหรับขั้นตอนสุดท้ายในการเปิดใช้งานของคริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่

รูปที่ 3.5 แสดงความต้องการค่าไถ่ของแรนซั่มแวร์คริปโตล็อคเกอร์จากการโจมตีกรณีศึกษาจริง

3.3.3 การทดลองที่ 3 : แนวทางการป้องกัน โดยใช้การวิจัยเชิงคุณภาพ การสนทนากลุ่ม

มุทิตา เอี่ยมทิพย์ (2564) การสนทนากลุ่ม (Focus Group) เป็นวิธีการเก็บรวบรวมข้อมูลเชิงคุณภาพที่ได้รับความนิยมอย่างแพร่หลาย โดยการรวมกลุ่มคน (ปกติ 6-12 คน) ที่มีประสบการณ์หรือความสนใจที่เหมือนกันในประเด็นที่กำลังอภิปราย มาร่วมแลกเปลี่ยนความคิดเห็นในหัวข้อที่กำหนด ซึ่งได้รับการพัฒนาในระหว่างสงครามโลกครั้งที่ 2 (ค.ศ. 1939-1945) เพื่อประเมินคุณภาพของรายการวิทยุ และถูกนำมาใช้ในงานด้านสังคมศาสตร์ภายหลัง

สงครามโลกครั้งที่ 2 เป็นการสนทนาแบบมีแบบแผน โดยมีผู้ดำเนินรายการ (Moderator) กำกับทิศทาง และผู้เข้าร่วม (Participants) ซึ่งเป็นบุคคลที่ได้รับการคัดเลือกตามเกณฑ์ที่กำหนด โดยมุ่งเน้นการแลกเปลี่ยนความคิดเห็น ประสบการณ์ และข้อคิดเห็นเกี่ยวกับประเด็นที่สนใจ การสนทนากลุ่มถือเป็นเครื่องมือที่มีประสิทธิภาพในการรวบรวมข้อมูลเชิงคุณภาพ ซึ่งช่วยให้สามารถเข้าใจความคิดเห็น ทัศนคติ และประสบการณ์ของกลุ่มเป้าหมายได้อย่างลึกซึ้ง ซึ่งเป็นประโยชน์ต่อการวิจัยในหลากหลายสาขา อย่างเช่น ในงานวิจัยเชิงคุณภาพ และงานวิจัยแบบผสมวิธี (Mixed Method) โดยใช้การสนทนากลุ่มเป็นส่วนหนึ่งของการเก็บรวบรวมข้อมูลเชิงคุณภาพ

การศึกษาวิจัยในครั้งนี้เป็นงานวิจัยเชิงคุณภาพเพื่อหาแนวทางป้องกันมัลแวร์เรียกค่าไถ่ตลอดจนข้อปฏิบัติในการรับมือการโจมตีจากมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรม มีแนวทางการคัดเลือกผู้เข้าร่วมการสนทนากลุ่ม คือ ต้องสำเร็จการศึกษาในระดับปริญญาตรีขึ้นไป และมีประสบการณ์ในด้านการรักษาความมั่นคงปลอดภัยอย่างน้อย 1 ปี มีผู้เข้าร่วมการสนทนากลุ่มแบ่งออกเป็น 2 กลุ่ม ได้แก่

กลุ่มที่ 1: ตัวแทนจำหน่ายผลิตภัณฑ์ด้านไอทีหรือผู้ติดตั้งระบบ

กลุ่มที่ 2: ผู้ดูแลระบบหรือภาคการศึกษา

นำผลจากการสนทนากลุ่ม และนำทฤษฎีและงานวิจัยที่เกี่ยวข้องมาประยุกต์ใช้ เพื่อหาแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยการป้องกันจากมัลแวร์เรียกค่าไถ่ ประยุกต์แนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ของกลุ่มอุตสาหกรรมผลิตชิ้นส่วนอิเล็กทรอนิกส์

3.4 เครื่องมือในใช้ในการวิจัย

3.4.1 การทดลองที่ 2 : ไฟร์วอลล์ (Firewall) และ อีดีอาร์ (EDR)

ไฟร์วอลล์ (Firewall) คือ ระบบรักษาความปลอดภัยเครือข่ายที่ทำหน้าที่เป็นเสมือนปราการปกป้องเครือข่ายของคุณจากการเข้าถึงที่ไม่ได้รับอนุญาต ตรวจสอบการรับส่งข้อมูลระหว่างเครือข่ายภายในขององค์กร กับเครือข่ายภายนอก การอนุญาตหรือบล็อกการเชื่อมต่อตามกฎที่กำหนดไว้ อย่างเช่น การตรวจสอบข้อมูลในระดับแพ็กเก็ต (Packet Filtering), ตรวจสอบสถานะของการเชื่อมต่อ (Stateful Inspection), ทำหน้าที่เป็นตัวกลาง (Application-Level

Gateway Proxy) และ ฟีเจอร์ขั้นสูงป้องกันการบุกรุก (Next-Generation Firewall) ซึ่งเป็นสิ่งจำเป็นสำหรับความปลอดภัยของเครือข่ายช่วยป้องกันภัยคุกคาม และปกป้องข้อมูลในองค์กรได้

อีดีอาร์ (EDR) หรือ Endpoint Detection and Response คือชุดโปรแกรมที่ช่วยปกป้องอุปกรณ์ปลายทาง (Endpoint) ซึ่งเป็นโซลูชันความปลอดภัยที่จำเป็นในยุคปัจจุบัน ช่วยปกป้องอุปกรณ์ปลายทางจากภัยคุกคามที่ซับซ้อน และเพิ่มประสิทธิภาพในการใช้งานระบบ ตรวจจับภัยคุกคามแบบ Zero-day ที่ไม่เคยพบมาก่อน และช่วยลดเวลาในการตอบสนองต่อเหตุการณ์ได้

3.4.2 การทดลองที่ 3 : แบบสอบถาม

แนวคำถามในการสนทนากลุ่ม (Focus Group) แนวคำถามสำหรับการสนทนากลุ่ม ได้แบ่งออกเป็น 4 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถามจะกล่าวถึงประวัติต่าง ๆ และประสบการณ์ด้านการทำงานของผู้ถูกสัมภาษณ์

ส่วนที่ 2 ทฤษฎีที่เกี่ยวข้องขั้นตอนแนวทางปฏิบัติของความมั่นปลอดภัย National Institute of Standards and Technology (NIST) ถามความเห็นและข้อแนะนำเกี่ยวกับแนวทางการปฏิบัติการ และการบริหารจัดการ เพื่อการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ และการป้องกันโจมตี แบ่งออกเป็น 5 คำถามตามขั้นตอนของเอ็นไอเอสที (NIST) ได้แก่

1) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)

2) การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect)

3) ความสามารถในการตรวจพบเหตุภัยคุมคามไซเบอร์ (Detect)

4) การรับมือภัยคุกคาม (Respond)

5) การกู้คืนข้อมูล และ ระบบหลังเหตุภัยคุกคามไซเบอร์ (Recovery)

ส่วนที่ 3 ข้อแนะนำแนวทางการปฏิบัติการ และการบริหารจัดการ เพื่อการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ และการป้องกันโจมตี

ส่วนที่ 4 เป็นแบบสอบถาม อ้างอิงจากทฤษฎีของ NIST

จากรูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group ทั้ง 4 ส่วน และรูปที่ 3.7 สรุปผล แบบประเมินความสอดคล้อง (IOC) ของผู้เชี่ยวชาญดังต่อไปนี้

มหาวิทยาลัยรังสิต Rangsit University

แบบสอบถามสัมภาษณ์การสนทนากลุ่ม (Focus Group)

แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ของอุตสาหกรรมผลิตชิ้นส่วนอิเล็กทรอนิกส์ กรณีศึกษาของคริปโตลือคเกอร์ (A GUIDELINE FOR RANSOMWARE DETECTION AND PREVENTION AT THE MANUFACTURING ELECTRONIC SUSPENSIONS INDUSTRY: A CASE STUDY OF HACKER ONE)

แบบสอบถาม

การวิจัยเรื่อง	แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรีอยุธยา กรณีศึกษาคริปโตล็อคเกอร์แรนซัมแวร์
จัดทำโดย	พิทยา นครไทย
สาขาวิชา	การจัดการเทคโนโลยีสารสนเทศ
คณะ	วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	รศ.ดร. ศริชณะ ชิมมณี

ข้อมูลประกอบความตรงเชิงเนื้อหาของเครื่องมือวิจัย

ข้อมูลประกอบความตรงเชิงเนื้อหาของเครื่องมือวิจัย ประกอบด้วยวัตถุประสงค์ของการวิจัยดังนี้

1.1 เพื่อความตระหนักรู้และหาแนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่เหมาะสมของระบบควบคุมในอุตสาหกรรม จากแนวทางของนิสต์

1.2 เพื่อเป็นการประเมินความรู้ ความเข้าใจ และทราบถึงแนวทางการป้องกันภัยคุกคามจากการโจมตีโดยมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในอุตสาหกรรมในโรงงาน

แบบตรวจสอบความเที่ยงตรงของเนื้อหาและความสอดคล้องกับวัตถุประสงค์ของการวิจัย

เรื่อง แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่อยุธยา กรณีศึกษาคริปโตล็อคเกอร์แรนซัมแวร์

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

คำชี้แจง โปรดทำเครื่องหมาย ✓ ใน ❍ หน้าข้อความที่ตรงกับรายละเอียดส่วนตัวของท่าน

1.1 ระดับการศึกษา

❍ ปวส. / อนุปริญญา ❍ ปริญญาตรี

❍ ปริญญาโท ❍ ปริญญาเอก

1.2 ท่านมีประสบการณ์การทำงานในหน่วยงานที่เกี่ยวข้องกับด้านระบบคอมพิวเตอร์ หรือสอนรายวิชาด้านการบริหารระบบคอมพิวเตอร์ กี่ปี

❍ ไม่มี ❍ 1 – 5 ปี

❍ 6 – 10 ปี ❍ มากกว่า 10 ปี

1.3 ท่านมีประสบการณ์ที่เกี่ยวข้องกับการให้บริการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information System Security) และ/หรือ ส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศในโรงงานอุตสาหกรรม อย่างไร

❍ ผู้ดูแลระบบ (Admin) ❍ ผู้ออกแบบและติดตั้งระบบ

❍ ผู้ฝึกอบรม หรือสอน ❍ ผู้ให้คำปรึกษา / ที่ปรึกษาการจัดการ

1.4 หน่วยงานของท่านจัดเป็นหน่วยงานประเภทไหน

❍ หน่วยงานราชการ / รัฐวิสาหกิจ

❍ โรงงาน สถานประกอบการ

❍ เจ้าของผลิตภัณฑ์ (Product Owner)

❍ ผู้ติดตั้งระบบ (System Integrator : SI)

ส่วนที่ 2 แบบสอบถามสัมภาษณ์เชิงลึกอ้างอิงจากทฤษฎีของ NIST (https://bit.ly/3eaKz80)

คำถามสำหรับการสนทนากลุ่มเฉพาะประเด็น (focus group)

2.1 Identify (ID)

2.1.1 Asset Management, Risk Assessment and Risk Management Strategy ท่านมีวิธีการปกป้องดูแลทรัพย์สินสารสนเทศ การจัดการบริหารความความเสี่ยง ด้านซัพพลายเชน และ กลยุทธ์การบริหารความเสี่ยง ทางด้านความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

_____

_____

_____

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group (ต่อ)

2.1.2 Governance ท่านมีแผนการบริหารจัดการระบบสารสนเทศการรักษาความมั่นคงปลอดภัยการกำกับดูแลที่มีประสิทธิภาพ จากมัลแวร์เรียกค่าไถ่ในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

2.2 Protect (PR)

2.2.1 Identity Management and Access Control ท่านมีแผนการบริหารจัดการข้อมูลประจำตัวและการควบคุมการเข้าถึงในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

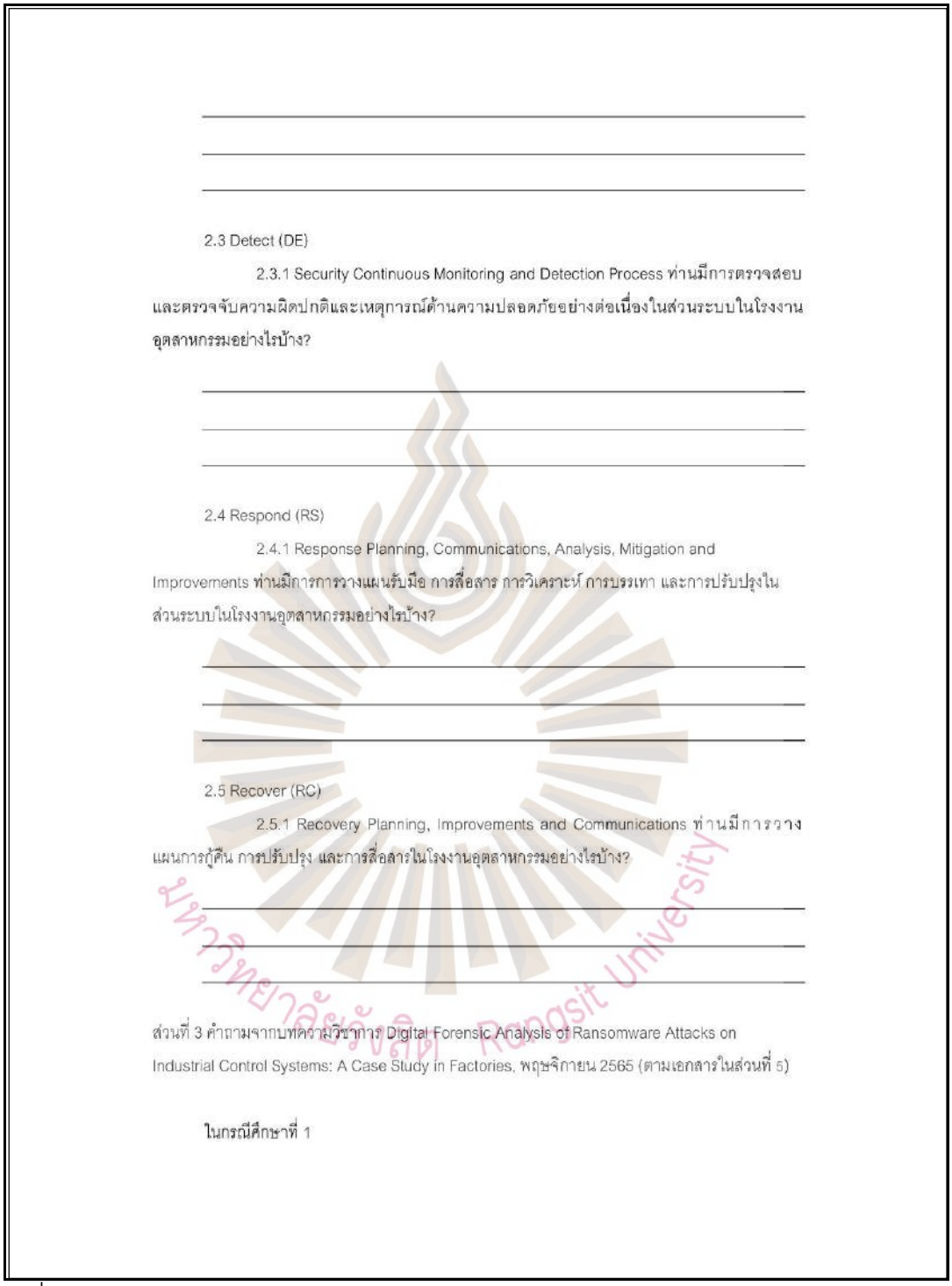
2.2.2 Awareness and Training ท่านมีแผนการสร้างความตระหนักและการฝึกอบรมอย่างไรบ้าง?

2.2.3 Data Security and Remote Access ท่านมีการจัดการความปลอดภัยทางข้อมูลและการป้องกันเข้าถึงระยะไกลในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

2.2.4 Protective Technology and Information Protection Processes and Procedures ท่านมีเทคโนโลยีการป้องกัน และกระบวนการขั้นตอนการป้องกันปกป้องข้อมูลในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group (ต่อ)



2.3 Detect (DE)

2.3.1 Security Continuous Monitoring and Detection Process ท่านมีการตรวจสอบและตรวจจับความผิดปกติและเหตุการณ์ด้านความปลอดภัยอย่างต่อเนื่องในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

2.4 Respond (RS)

2.4.1 Response Planning, Communications, Analysis, Mitigation and Improvements ท่านมีการการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การบรรเทา และการปรับปรุงในส่วนระบบในโรงงานอุตสาหกรรมอย่างไรบ้าง?

2.5 Recover (RC)

2.5.1 Recovery Planning, Improvements and Communications ท่านมีการวางแผนการกู้คืน การปรับปรุง และการสื่อสารในโรงงานอุตสาหกรรมอย่างไรบ้าง?

ส่วนที่ 3 คำถามจากบทความวิชาการ Digital Forensic Analysis of Ransomware Attacks on Industrial Control Systems: A Case Study in Factories, พฤษจิกายน 2565 (ตามเอกสารในส่วนที่ 5)

ในกรณีศึกษาที่ 1

รูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group (ต่อ)

กลุ่ม Asteelflash ผู้ผลิตอุปกรณ์อิเล็กทรอนิกส์ ดำเนินงานโรงงาน 18 แห่ง และศูนย์อาร์แอนด์ดี สองแห่ง มีพนักงาน 6,200 คน และมีรายได้ต่อปีมากกว่าหนึ่งพันล้านยูโร ให้บริการการผลิตอุปกรณ์อิเล็กทรอนิกส์ของฝรั่งเศส (EMS) เป็นบริการการผลิตอุปกรณ์อิเล็กทรอนิกส์ได้ปฏิวัติทางอุตสาหกรรมโดยการนำเอาเทคโนโลยีเครื่องจักรต่าง ๆ ปัญญาประดิษฐ์ (AI) และ IoT (Internet of Things) เข้ามาเพื่อบริหารจัดการภายในโรงงาน ที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์โดยมัลแวร์เรียกค่าไถ่รีวิล (REvil) เมื่อวันที่ 2 เมษายน 2564 โดยออกประกาศยืนยันว่าบริษัทเป็นผู้ได้รับผลกระทบจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่ส่งผลกระทบต่อเซิร์ฟเวอร์ที่ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ ได้ประสบความสำเร็จในการเข้ารหัสไฟล์บนระบบ เรียกร้องค่าไถ่ 24 ล้านเหรียญ ตรวจพบว่าผู้คุกคามได้แชร์ไฟล์ชื่อ 'asteelflash_data_part1.7z' ซึ่งได้ทำการแชร์เพื่อพิสูจน์ว่าไฟล์ถูกขโมยในระหว่างการโจมตี จุดเริ่มต้นอาจเป็นบริการไมโครซอฟท์อาร์พีซี (RPC) ที่เปิดช่องโหว่ซึ่งมีอยู่ตั้งแต่เดือนพฤศจิกายนปีก่อนหน้า การโจมตีของโดยมัลแวร์เรียกค่าไถ่รีวิล (REvil) มีความแตกต่างในการโจมตีช่องโหว่ใหม่ ๆ แต่เทคนิคของพวกเขาทับซ้อนกับกลุ่มอื่น ๆ โดยอาศัยเครื่องมือขโมยข้อมูลส่วนตัวอย่าง Mimikatz เพื่อ Lateral Movement และการลาดตระเวนโดยใช้เครื่องมืออย่างพีเอสเอ็กเซ็ก (PS Exec)

จากกรณีศึกษานี้ท่านมีแนวทางป้องกันอย่างไร

ในกรณีศึกษาที่ 2

Foxconn ผู้ผลิตอุปกรณ์อิเล็กทรอนิกส์ด้วยประสบการณ์มากกว่า 35 ปีในการผลิตผลิตภัณฑ์อิเล็กทรอนิกส์ซึ่งผลิตคอมพิวเตอร์ พีซีจอแอลซีดี อุปกรณ์พกพา และกล่องรับสัญญาณ ซึ่งเดิมใช้โดยระบบ Sony, Motorola และ Cisco Foxconn ได้ยืนยันว่าหนึ่งในบริษัทที่มีฐานอยู่ในเม็กซิโก โรงงานผลิตในตีฮัวน่าเป็นแห่งที่สองที่โดนแรนซัมแวร์โจมตีในเวลาไม่ถึงสองปี การโจมตีครั้งแรกเกิดขึ้นเมื่อวันที่ 29 พฤศจิกายน พ.ศ. 2564 โดย DoppelPaymer แรนซัมแวร์ ผู้โจมตีเรียกค่าไถ่ 34 ล้านดอลลาร์และอ้างว่าขโมยข้อมูล 100GB เข้ารหัสระหว่างเซิร์ฟเวอร์ 1,200 ถึง 1,400 เครื่อง และทำลายข้อมูลสำรอง 20 ถึง 30TB และการโจมตีครั้งที่สองโดย LockBit 2.0 Ransomware เมื่อวันที่ 31 พฤษภาคม พ.ศ. 2565 โดยเผยแพร่ ได้ข่มขู่ว่าจะรั่วไหลข้อมูลที่ถูกขโมยจาก Foxconn เว้นแต่จะมีการจ่ายค่าไถ่ภายในวันที่ 11 มิถุนายน พ.ศ. 2565 แรนซัมแวร์ LockBit ได้รับการพิจารณาจากหลายหน่วยงานให้เป็นส่วนหนึ่งของตระกูลมัลแวร์ "LockerGoga & MegaCortex" การโจมตีเป็นแบบแพร่กระจายตัวเอง กำหนดเป้าหมาย

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group (ต่อ)

และใช้เครื่องมือที่คล้ายกัน ขั้นตอนของการโจมตีแบบล็อกบิตโดยมีสามขั้นตอนโดยประมาณคือ เจาะระบบ แทรกซึม และปรับใช้

จากกรณีศึกษานี้ท่านมีแนวทางป้องกันอย่างไร

ในกรณีศึกษาที่ 3

Panasonic บริษัทยักษ์ใหญ่ด้านเทคโนโลยีของญี่ปุ่นยืนยันว่าโรงงานในแคนาดาถูกมัลแวร์เรียกค่าไถ่ Conti ransomware (RaaS) โจมตีในเดือนกุมภาพันธ์ พ.ศ. 2565 การโจมตีมีเป้าหมายและส่งผลกระทบต่อเซิร์ฟเวอร์ เครือข่าย และกระบวนการบางอย่าง Conti อ้างว่าพวกเขาใช้ทรัพยากรบุคคลและข้อมูลทางบัญชีประมาณ 3 กิกะไบต์ ผู้บุกรุกเข้าถึงระบบของบริษัทได้นานกว่าสี่เดือนก่อนที่จะถูกตรวจพบและตามรายงาน ผู้คุกคามสามารถเข้าถึงข้อมูลที่สำคัญของลูกค้าและพนักงานได้ โดยมัลแวร์เรียกค่าไถ่ Conti ตั้งใจอัปโหลดไฟล์เหล่านั้นที่รั่วไหลของไฟล์ออนไลน์ในเดือนพฤศจิกายน พ.ศ. 2564 บริษัทยอมรับว่าเครือข่ายนั้น "เข้าถึงโดยมิชอบด้วยกฎหมายโดยบุคคลที่สาม" และในเหตุการณ์ บันทึกพบว่าข้อมูลบางอย่างบนเซิร์ฟเวอร์ไฟล์ถูกเข้าถึงระหว่างการการหยุดชะงัก และในเดือนตุลาคม พ.ศ. 2563 แฮ็กเกอร์ได้แบ่งบันข้อมูลสี่กิกะไบต์ไปยังไฟล์ที่รั่วไหลทางออนไลน์ รวมถึงข้อมูลทางการเงินและที่อยู่อีเมล

จากกรณีศึกษานี้ท่านมีแนวทางป้องกันอย่างไร

ส่วนที่ 4 ท่านเคยมีประสบการณ์จากการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ อย่างไร และมีแนวทางป้องกันอย่างไร

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.6 แสดงแบบสอบถามสำหรับการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group (ต่อ)

สรุปผล แบบประเมินความสอดคล้อง (IOC) ของผู้เชี่ยวชาญ

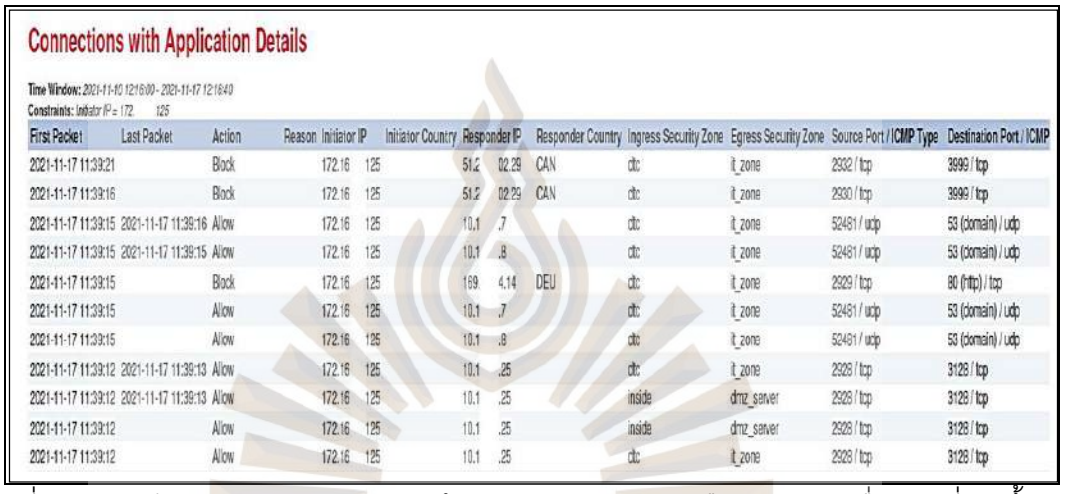
ข้อที่	ผู้ทรงคุณวุฒิ จำนวน 3 ท่าน คะแนน			รวม (∑ R)	IOC	สรุปผล	ข้อเสนอแนะ
	คนที่ 1	คนที่ 2	คนที่ 3				
ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม							
1	0	1	1	2	0.67	ใช้ได้	
2	1	1	1	3	1.0	ใช้ได้	
3	1	1	1	3	1.0	ใช้ได้	
4	1	1	1	3	1.0	ใช้ได้	
ส่วนที่ 2 แบบสอบถามสัมภาษณ์เชิงลึกอ้างอิงจากทฤษฎีของ NIST							
1	1	1	1	3	1.0	ใช้ได้	
2	1	1	1	3	1.0	ใช้ได้	
3	1	1	1	3	1.0	ใช้ได้	
4	1	1	1	3	1.0	ใช้ได้	
5	1	1	1	3	1.0	ใช้ได้	
6	1	1	1	3	1.0	ใช้ได้	
7	1	1	1	3	1.0	ใช้ได้	
8	1	1	1	3	1.0	ใช้ได้	
9	1	1	1	3	1.0	ใช้ได้	
ส่วนที่ 3 คำถามจากบทความวิชาการ Digital Forensic Analysis of Ransomware Attacks on Industrial Control Systems: A Case Study in Factories							
1	1	1	1	3	1.0	ใช้ได้	
2	1	1	1	3	1.0	ใช้ได้	
3	1	1	1	3	1.0	ใช้ได้	
ส่วนที่ 4 ท่านเคยมีประสบการณ์จากการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ อย่างไร และมีแนวทางป้องกันอย่างไร							
1	0	1	1	2	0.67	ใช้ได้	

รูปที่ 3.7 สรุปผล แบบประเมินความสอดคล้อง (IOC) ของผู้เชี่ยวชาญ

3.5 การเก็บรวบรวมข้อมูล

3.5.1 การทดลองที่ 2 : บันทึกเหตุการณ์จาก ไฟร์วอลล์ (Firewall) และ อีดีอาร์ (EDR)

3.5.1.1 บันทึกเหตุการณ์จาก ไฟร์วอลล์ (Firewall) การเก็บรวบรวมข้อมูลบันทึกเหตุการณ์ต่าง ๆ จาก ไฟร์วอลล์ (Firewall) จากรูปที่ 3.6 การตรวจสอบพบว่าการรับส่งข้อมูลระหว่างเครือข่ายภายในกับเครือข่ายภายนอก อนุญาตหรือบล็อกการเชื่อมต่อตามกฎที่กำหนดไว้ อย่างเช่น บล็อกการเชื่อมต่อพอร์ตเครือข่าย 3999 ไปยังเครือข่ายภายนอก และการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์เครื่องอื่นภายในเครือข่าย



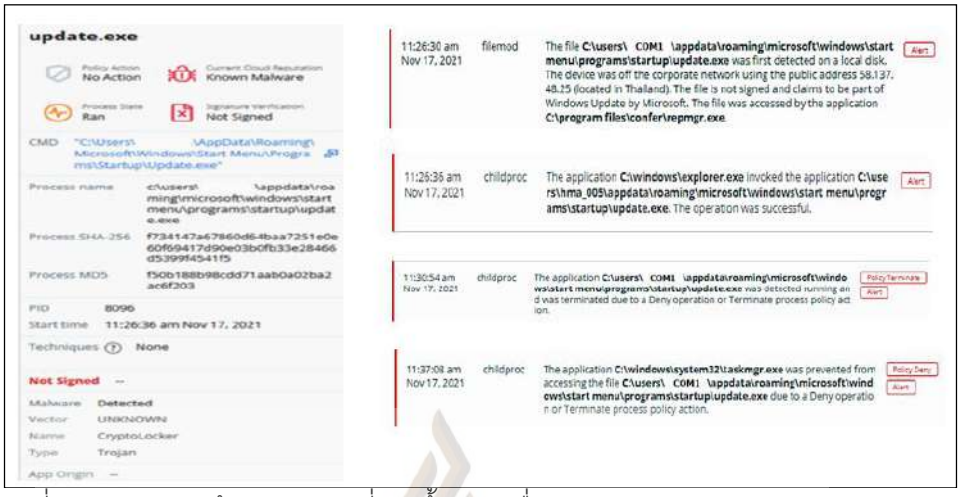
Connections with Application Details

Time Window: 2021-11-10 12:16:00 - 2021-11-17 12:16:40
Constraints: Initiator IP = 172. 125

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP
2021-11-17 11:39:21		Block		172.16 .125		51.2 .02.29	CAN	dtc	it_zone	2932 / tcp	3999 / tcp
2021-11-17 11:39:16		Block		172.16 .125		51.2 .02.29	CAN	dtc	it_zone	2930 / tcp	3999 / tcp
2021-11-17 11:39:15	2021-11-17 11:39:16	Allow		172.16 .125		10.1 .7		dtc	it_zone	52461 / udp	53 (domain) / udp
2021-11-17 11:39:15	2021-11-17 11:39:15	Allow		172.16 .125		10.1 .8		dtc	it_zone	52461 / udp	53 (domain) / udp
2021-11-17 11:39:15		Block		172.16 .125		169. 4.14	DEU	dtc	it_zone	2929 / tcp	80 (http) / tcp
2021-11-17 11:39:15		Allow		172.16 .125		10.1 .7		dtc	it_zone	52461 / udp	53 (domain) / udp
2021-11-17 11:39:15		Allow		172.16 .125		10.1 .8		dtc	it_zone	52461 / udp	53 (domain) / udp
2021-11-17 11:39:12	2021-11-17 11:39:13	Allow		172.16 .125		10.1 .25		dtc	it_zone	2928 / tcp	3128 / tcp
2021-11-17 11:39:12	2021-11-17 11:39:13	Allow		172.16 .125		10.1 .25		inside	dmz_server	2928 / tcp	3128 / tcp
2021-11-17 11:39:12		Allow		172.16 .125		10.1 .25		inside	dmz_server	2928 / tcp	3128 / tcp
2021-11-17 11:39:12		Allow		172.16 .125		10.1 .25		dtc	it_zone	2928 / tcp	3128 / tcp

รูปที่ 3.8 แสดงไฟร์วอลล์ (Firewall) บันทึกเหตุการณ์อนุญาต หรือบล็อกการเชื่อมต่อที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ไปยังปลายทาง

3.5.1.2 บันทึกเหตุการณ์จาก อีดีอาร์ (EDR) บันทึกเหตุการณ์ต่าง ๆ เช่นจาก VMware Carbon Black (EDR) จากเหตุการณ์การโจมตีตั้งแต่เริ่มต้นจนถึงขั้นตอนสุดท้ายที่เกิดขึ้นเครื่องคอมพิวเตอร์ปลายทาง (Endpoint) ได้แจ้งเตือนไปยังผู้ดูแลระบบความปลอดภัยทางไซเบอร์เพื่อช่วยในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคาม ดังรูปที่ 3.7



รูปที่ 3.9 แสดงบันทึกเหตุการณ์ที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ปลายทาง (Endpoint) จาก อีดีอาร์ (EDR)

3.5.2 การทดลองที่ 3 : จากการจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group

ในวิทยานิพนธ์ฉบับนี้ ได้ใช้การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ (Focus Group) ในการศึกษาแนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ เพื่อให้ได้ข้อมูลเชิงลึกสำหรับการศึกษาแนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ผู้วิจัยได้ออกแบบแนวคำถามสัมภาษณ์แบบปลายเปิด โดยอ้างอิงจากกรอบกรอบแนวทางปฏิบัติของนิสต์ และทฤษฎีที่เกี่ยวข้อง เพื่อใช้ในแนวคำถามในการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญ ซึ่งในการดำเนินการการสัมภาษณ์ผู้เชี่ยวชาญและการวิเคราะห์ข้อมูลอย่างเป็นระบบ เป็นวิธีการรวบรวมและวิเคราะห์ข้อมูลเชิงลึก โดยอาศัยความรู้และประสบการณ์ของผู้เชี่ยวชาญในสาขาที่เกี่ยวข้อง เพื่อให้ได้ข้อมูลที่มีคุณภาพนำไปสู่ข้อสรุปแนวทางการป้องกันที่มีประสิทธิภาพ และแนวทางการรักษาความมั่นคงปลอดภัยที่ครอบคลุม ตรงตามวัตถุประสงค์ของงานวิจัย ซึ่งประเด็นคำถามที่ใช้ในการสัมภาษณ์จากกรอบแนวทางปฏิบัติของนิสต์ดังนี้ ประกอบด้วยดังนี้ การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify) การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect) ความสามารถในการตรวจพบเหตุภัยคุมคามไซเบอร์ (Detect) การรับมือภัยคุกคาม (Respond) การกู้คืนข้อมูล และระบบหลังเหตุภัยคุกคามไซเบอร์ (Recovery)ประชากร คือ ผู้เชี่ยวชาญจำนวน 44 คนแบ่งออกเป็น 2 กลุ่ม ได้แก่

กลุ่มที่ 1 ตัวแทนจำหน่ายผลิตภัณฑ์ด้านไอทีหรือผู้ติดตั้งระบบ มีจำนวน 13 คน

กลุ่มที่ 2 ผู้ดูแลระบบหรือภาคการศึกษา มีจำนวน 41 คน

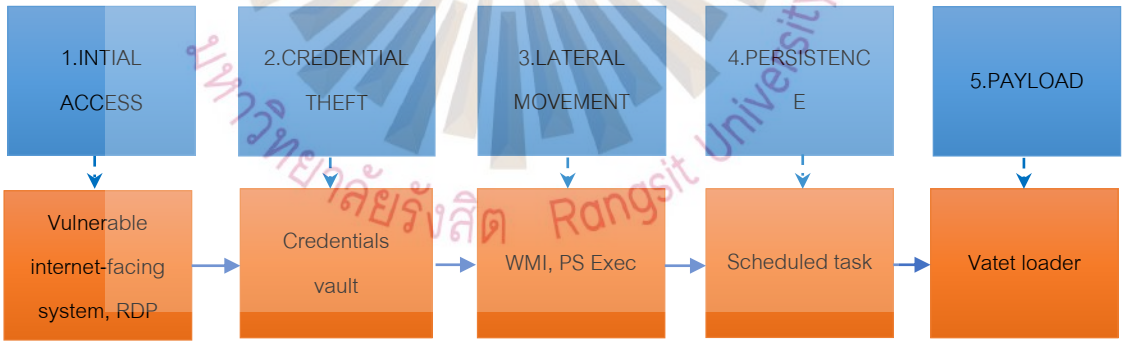
ในการศึกษาวิจัยในครั้งนี้ได้จัดเก็บข้อมูลในการสนทนากลุ่มด้วยกูเกิลฟอร์ม (Google Form) และบันทึกวิดีโอในส่วนสำคัญ เพื่อได้ข้อมูลครบถ้วนพร้อมความคิดเห็นและข้อเสนอแนะเฉพาะจากมุมมองที่หลากหลายในส่วนของระบบควบในโรงงานอุตสาหกรรม (ICS) ตามแนวทางปฏิบัติของเอ็นไอเอสที (NIST) ทั้ง 5 ส่วน เพื่อนำมาทำการวิเคราะห์ข้อมูลหาแนวทางการป้องกันและสรุปผลเป็นตาราง

3.6 การวิเคราะห์ข้อมูล

3.6.1 การทดลองที่ 2: กรอบแนวคิดไมโครซอฟท์ (Microsoft Framework) และ ไมเตอร์แอทแทค (MITRE ATT&CK)

3.6.1.1 กรอบแนวคิดไมโครซอฟท์ (Microsoft Framework)

ศึกษาขั้นตอนการดำเนินการมัลแวร์เรียกค่าไถ่ จากกรอบแนวคิดของไมโครซอฟท์ (Microsoft, 2020) เนื่องจากในประเทศไทยมีการใช้ระบบปฏิบัติการวินโดวส์อย่างแพร่หลาย และตกเป็นเป้าโจมตีหมายของแก๊งมัลแวร์เรียกค่าไถ่ ดังนั้น ในการค้นคว้าอิสระฉบับนี้จึงได้ ศึกษากรอบแนวคิดของไมโครซอฟท์ โดยแบ่งขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่ออกเป็น 5 ขั้นตอน



รูปที่ 3.10 แสดงขั้นตอนการดำเนินการคริปโตล็อคเกอร์มัลแวร์เรียกค่าไถ่

ที่มา: ดัดแปลงจาก Microsoft 365 Defender Threat Intelligence Team, 2022 ; ผู้วิจัย

1) วิธีการเจาะระบบเครือข่าย (Initial Access) ตามที่ คริชณะ ฉิมมณี และมณีสุข โชติรุ่งรัตน์ (2021) ได้ศึกษาไว้สำหรับขั้นตอนแรกสุดของการโจมตีคือ การเข้าถึงระบบของเป้าหมายจากไมโครซอฟ์ตได้แบ่งออกเป็น 3 วิธีการหลัก ดังรูปที่ 3.1 ได้แก่

1.1) ผ่านโปรโตคอลอาร์ดีพี และการบรูตฟอร์ซ (RDP Brute Force)

1.2) ผ่านช่องโหว่งที่เข้าถึงได้จากอินเตอร์เน็ต (Internet Facing)

1.3) จุดอ่อนจากการกำหนดค่าความมั่นคงปลอดภัยของแอพพลิเคชัน (Weak Application Settings)

2) การโจรกรรมข้อมูลเพื่อยกระดับสิทธิ (Credential Theft) การโจมตีด้วยการขโมยชื่อผู้ใช้ และพาสเวิร์ดคือการโจมตีที่ผู้โจมตีได้รับสิทธิ์สูงสุดในขั้นต้น (ผู้ดูแลระบบหรือระบบขึ้นอยู่กับระบบปฏิบัติการที่ใช้) ในการเข้าถึงคอมพิวเตอร์บนเครือข่าย จากนั้นใช้เครื่องมือที่มีให้ใช้งานฟรีเพื่อดึงข้อมูลชื่อผู้ใช้ และพาสเวิร์ดทั้งหมดในระบบเครือขายเพื่อยกระดับสิทธิ

3) การขยายการโจมตีไปยังเน็ตเวิร์คที่เกี่ยวข้อง (Lateral Movement) หลังจาก
แฮกเกอร์ได้เจาะเครือข่ายคอมพิวเตอร์เข้ามาในโซนแรก (Zone) เช่น ดีเอ็มแซตโซน (DMZ) และต้องขยายวงการโจมตีไปยังโซนอื่น ๆ หลายครั้งการโจมตีจะไม่ได้เกิดขึ้นแค่ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง แต่จะเป็นการรวบรวมข้อมูลเครือข่ายแล้วเจาะไปยังคอมพิวเตอร์เครื่องอื่นต่อซึ่งอาจมีข้อมูลสำคัญหรือมีสิทธิ์ในการทำงานมากกว่าเครื่องที่เจาะได้ตอนแรก

4) การแอบฝังตัวในระบบเครือข่าย (Persistence) การแอบฝังตัวในระบบเครือข่าย ประกอบด้วยเทคนิคที่ฝ่ายตรงข้ามใช้เพื่อคงการเข้าถึงระบบไว้ตลอดการรีสตาร์ท ข้อมูลประจำตัวที่เปลี่ยนแปลง และการหยุดชะงักอื่น ๆ ที่อาจตัดการเข้าถึง เทคนิคที่ใช้เพื่อความคงอยู่รวมถึงการเข้าถึงการดำเนินการ หรือการเปลี่ยนแปลงการกำหนดค่าที่ช่วยให้ผู้โจมตีสามารถตั้งหลักในระบบได้ เช่น การเปลี่ยนหรือได้รหัสที่ถูกต้อง หรือเพิ่มรหัสเริ่มต้น

5) เปย์โหลด (Payload) เมื่อผู้โจมตีเข้าถึงเครือข่ายได้ ขั้นตอนสุดท้ายของการโจมตีจะเป็นการสั่งติดตั้งมัลแวร์เรียกค่าไถ่ เป็นการโจมตีในรูปแบบประมวลผลโปรแกรมแบบอัตโนมัติตามตารางเวลาที่กำหนด (Schedule Task) บนระบบปฏิบัติการวินโดวส์ และมีการแสดงป๊อบอัป (Pop-up) เรียกค่าไถ่

จากกรอบแนวคิดของไมโครซอฟท์ ขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่ออกเป็น 5 ขั้นตอนคือ (1) วิธีการเจาะระบบเครือข่าย (Initial Access), (2) การโจรกรรมข้อมูลเพื่อยกระดับ

สิทธิ (Credential Theft), (3) การขยายการโจมตีไปยังเน็ตเวิร์คที่เกี่ยวข้อง (Lateral Movement), (4) การแอบฝังตัวในระบบเครือข่าย (Persistence) และ (5) เปย์โหลด (Payload)

จาก Microsoft 365 Defender Research Team (2022) ได้แสดงตัวอย่างเทคนิค 10 อันดับแรกในการโจมตีมัลแวร์เรียกค่าไถ่ หลังจากสร้างวิธีการแล้ว รายการเทคนิคมัลแวร์เรียกค่าไถ่ 10 อันดับแรกถูกสร้างขึ้นเพื่อทดสอบวิธีการใหม่นี้ในทางปฏิบัติ ไมโครซอฟท์ พยายามในการทำงานร่วมกับคู่ค้าได้วิเคราะห์การโจมตีมัลแวร์เรียกค่าไถ่ที่แพร่หลายในช่วงสามปีที่ผ่านมา มีการศึกษาการโจมตีโดยใช้เทคนิค (ATT&CK) ได้แก่

1) ข้อมูลที่เข้ารหัสเพื่อผลกระทบ Data Encrypted for Impact (T1486)

2) ยับยั้งการกู้คืนระบบ Inhibit System Recovery (T1490)

3) ไฟล์หรือข้อมูลที่คลุมเครือ Obfuscated Files or Information (T1027)

4) เครื่องมือจัดการบนวินโดว์ Windows Management Instrumentation (T1047)

5) การปลอมตัว Masquerading (T1036)

6) ตัวแปลคำสั่งและสคริปต์ Command and Scripting Interpreter (T1059)

7) ทำให้เสียการป้องกัน Impair Defenses (T1562)

8) แก้ไขรีจิสทรี Modify Registry (T1112)

9) การดำเนินการของผู้ใช้ User Execution (T1204)

10) กระบวนการอินเจ็คชั่น Process Injection (T1055)

มหาวิทยาลัยรังสิต Rangsit University

3.6.1.2 ไมเตอร์แอทแทค (MITRE ATT&CK)

MITRE ATT&CK คือแหล่งความรู้เกี่ยวกับกลยุทธ์ เทคนิค และกระบวนการทำงาน เป็นแพลตฟอร์มจัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ (TTPs) ที่แฮกเกอร์ใช้ในโลกดิจิตอล MITRE ATT&CK แบ่งเป็นหมวดหมู่ทั้งแบบ Pre-ATT&CK, Enterprise, Mobile และสำหรับระบบควบคุมอุตสาหกรรม (ICS) โดยมีตัวอย่างของ กลยุทธ์สำหรับ เอ็นเทอร์ไพรซ์ (Enterprise) ประกอบด้วย 12 กลยุทธ์ ซึ่งแต่ละกลยุทธ์จะมีข้อมูลของเทคนิคที่แฮกเกอร์นิยมใช้ทั้งหมด รวมถึงอธิบายถึงกระบวนการทำงานในแต่ละเทคนิค รายการย่อยในแต่ละแทคติกส์ (Tactics) จะเป็นเทคนิคย่อย ๆ ซึ่งแต่ละเทคนิคจะมีคำแนะนำการมิทอิเกท (Mitigate) และ ดีเทคชัน (Detection) รวมถึงมีการอ้างอิงไปยังกลุ่มแฮคเกอร์ที่เคยใช้เทคนิคเหล่านี้ โดยอยู่บนพื้นฐานของข้อมูลรายงานการโจมตีในอดีต (MITRE ATT&CK, 2022)

3.6.2 **การทดลองที่** 3: **การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ** Focus Group

เมื่อได้ข้อสรุปจากการประชุมทางวิชาการกลุ่มเป้าหมายที่กำหนดหรือสนทนากลุ่ม (Focus Group) พร้อมทั้งได้ข้อมูลความคิดเห็นและการตอบข้อคำถามจากผู้เข้าร่วมสนทนากลุ่มผ่านกูเกิลฟอร์ม ซึ่งได้ข้อมูลครบถ้วน จากมุมมองที่หลากหลายของผู้เชี่ยวชาญ เพื่อนำไปวิเคราะห์หาแนวทางการป้องกัน

บทที่ 4

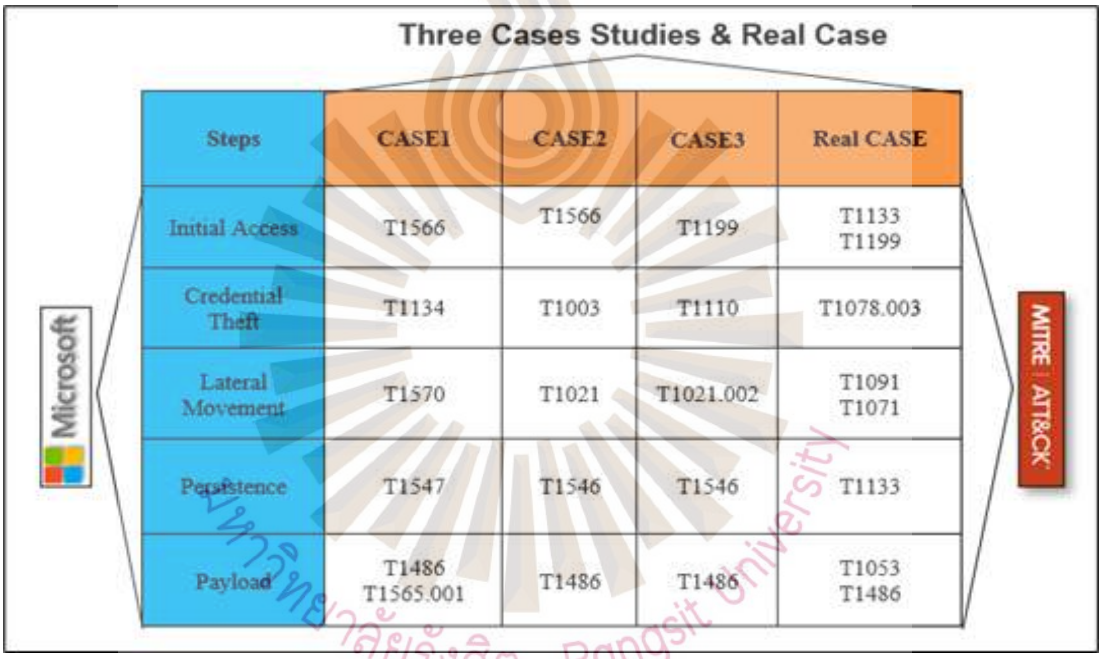
ผลการวิจัย

งานวิจัยนี้ผลการทดลองได้แบ่งออกเป็น 2 ส่วนหลัก ได้แก่ ส่วนแรก คือ การวิเคราะห์การโจมตีในการทดลองที่ 1 และ 2 ส่วนที่สอง คือ แนวทางการป้องกันในการทดลองที่ 3 ซึ่งได้ผลการทดลองดังนี้

4.1 ผลการทดลองที่ 1 และผลการทดลอง ที่ 2

ผู้วิจัยได้ศึกษาและนำเสนอผลการทดลองจากการวิเคราะห์ทางนิติวิทยาศาสตร์ดิจิทัลจากการวิจัยเชิงคุณภาพ (Qualitative Research) และการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้การทดลองที่ 1 การวิจัยเอกสาร (Documentary Research) และการทดลองที่ 2 การวิจัยเชิงทดลองจริง (True Experiment) เป็นเครื่องมือการวิจัยได้นำเสนอบทความการวิเคราะห์ทางนิติวิทยาศาสตร์ดิจิทัลจากกรณีศึกษาการโจมตีที่เกิดขึ้นจริงจากมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) ซึ่งประกอบด้วยการทดลองที่ 1 จาก 3 กรณีศึกษา โดยเป็นการวิจัยเชิงเอกสาร (Research Document) และการทดลองที่ 2 จาก 1 กรณีศึกษาที่เกิดขึ้นจากเหตุการณ์จริง ซึ่งในทุกกรณีได้ใช้การวิเคราะห์ และรวบรวมจากการสัมพันธ์ เปรียบเทียบด้วยกรอบการโจมตี จากกรอบแนวคิดของไมโครซอฟท์ (Microsoft Framework) (Microsoft Threat Intelligence, 2020) เนื่องจากในโรงงานร้อยละ 95 ใช้ระบบปฏิบัติการเป็นไมโครซอฟท์ วินโดว์ (Microsoft Windows) และจากกรอบแนวคิดของไมเตอร์แอทแทค (MITER ATT&CK Framework) เพื่อระบุและติดตามภัยคุกคามทางไซเบอร์ บทความยังให้รายละเอียดของกรณีจริง และไทม์ไลน์ทางนิติวิทยาศาสตร์ดิจิทัลแก่เจ้าหน้าที่ดูแลระบบเครือข่าย และสถาปนิกด้านความมั่นคงปลอดภัยทางไซเบอร์เพื่อเพิ่มประสบการณ์ โดยสรุปผลการวิเคราะห์ขั้นตอนการโจมตีจากกรณีศึกษาทั้งหมดในรูปที่ 4.1 โดยในตารางคอลัมน์ที่ 1 คือ เทคนิคการโจมตี 5 ขั้นตอนของกรอบแนวคิดของไมโครซอฟท์ คอลัมน์ที่ 2-4 เป็นกรณีศึกษาที่เกิดขึ้นจริง และคอลัมน์ที่ 5 เป็นการโจมตีที่เกิดขึ้นจริง เช่นการเข้าถึงครั้งแรก (Initial Access) ด้วยเทคนิค (Techniques) T1133 ซึ่งคือ การเข้าถึงและควบคุมคอมพิวเตอร์ภายในระบบควบคุมอุตสาหกรรมจากระยะไกลผ่านบริการที่เปิดให้เข้าถึงจากภายนอก และเทคนิค T1199 ซึ่งหมายถึง บุคคลที่สามที่เชื่อถือได้ ซึ่งอาจเป็นคู่ค้า หรือผู้ให้บริการ ขั้นตอนในลำดับถัดมา

การเคลื่อนที่ภายในเครือข่าย (Lateral Movement) ได้ใช้เทคนิค T1091 ซึ่งคือ การแพร่กระจายมัลแวร์ผ่านยูเอสบีแฟลชไดรฟ์ (USB Flesh Drive) และได้ใช้เทคนิค T1071 ซึ่งคือ การใช้โปรโตคอลชั้นแอปพลิเคชัน (Application) การถ่ายโอนไฟล์ด้วยโปรโตคอล (Protocol) เอสเอ็มบี (SMB) เป็นต้น ประโยชน์ของงานวิจัยก่อนหน้านี้ คือ ได้รวบรวมข้อมูลขั้นตอนการโจมตีและวิเคราะห์ด้วยกรอบแนวคิดของไมโครซอฟท์ และใช้หมายเลขเทคนิคของไมเตอร์แอทแทคเพื่อเป็นกรณีศึกษาให้เจ้าหน้าที่ดูแลระบบเครือข่าย (Network Administrator) และสถาปนิกด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Architect) สำหรับใช้เพื่อเข้าใจขั้นตอนการโจมตี (Nakhonthai & Chimmanee, 2022)



รูปที่ 4.1 ขั้นตอนเจาะระบบของคริปโตล็อคเกอร์ จากกรอบแนวคิดของไมโครซอฟท์ และไมเตอร์แอทแทค

จากรูปที่ 4.1 ผลการทดลองการโจมตีที่เกิดขึ้นจริงจากมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) กรณีจริง (Real Case) ดังนั้นแผนเผชิญเหตุ และการป้องกันจึงอยู่ในขั้นตอนต่อไป ซึ่งนำเสนอแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ที่เหมาะสมของระบบควบคุมในโรงงานอุตสาหกรรม จากการสนทนากลุ่มโดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)

4.2 ผลการทดลองที่ 3

การประชุมกลุ่มเป้าหมายที่กำหนด หรือ การสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของนิสต์ (NIST) การวิจัยเชิงคุณภาพ การสนทนากลุ่มนี้ ผู้วิจัยได้จัดเตรียมแผนดำเนินการอย่างเป็นขั้นตอน ได้เชิญผู้มีประสบการณ์เชี่ยวชาญในการร่วมการสนทนาจากผู้มีประสบการณ์ด้านเครือข่ายคอมพิวเตอร์โดยเป็นผู้ติดตั้งระบบ ดูแลระบบด้านความมั่นคงปลอดภัยไซเบอร์ และภาคการศึกษาชำนาญการ การสนทนากลุ่มภายในห้องประชุมมีการนำเสนออธิบายขั้นตอนอย่างละเอียดในแต่ละหัวข้อแบบสอบถามโดยใช้แนวทางปฏิบัติของนิสต์พร้อมมีเครื่องเสียงเข้ามาช่วยให้การสนทนาเป็นไปอย่างราบรื่นชัดเจน ได้ดำเนินการสนทนาพร้อมยกตัวอย่างเจาะทุกประเด็นข้อคำถามตามแนวทางปฏิบัติของนิสต์ ทั้ง 5 ส่วน พร้อมเก็บรวบรวมข้อมูลแบบสอบถามและข้อเสนอแนะนำมาทำการวิเคราะห์ข้อมูลเพื่อได้ข้อสรุปแนวทางป้องกันมัลแวร์เรียกค่าไถ่ตลอดจนข้อปฏิบัติในการรับมือในกรณีที่ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรม

ในการศึกษาวิจัยในครั้งนี้ได้จัดเก็บข้อมูลในการสนทนากลุ่มด้วยกูเกิลฟอร์ม (Google Form) และบันทึกวิดีโอในส่วนสำคัญ เพื่อได้ข้อมูลครบถ้วนพร้อมความคิดเห็นและข้อเสนอแนะเฉพาะจากมุมมองที่หลากหลายในส่วนของระบบควบในโรงงานอุตสาหกรรม (ICS) ตามแนวทางปฏิบัติของเอ็นไอเอสที (NIST) ทั้ง 5 ส่วน เพื่อนำมาทำการวิเคราะห์ข้อมูลและสรุปผลเป็นตาราง

เมื่อได้ข้อสรุปจากการประชุมทางวิชาการกลุ่มเป้าหมายที่กำหนดหรือสนทนากลุ่ม พร้อมทั้งได้ข้อมูลความคิดเห็นและคำตอบข้อคำถามจากผู้เข้าร่วมผ่านกูเกิลฟอร์ม ซึ่งได้ข้อมูลครบถ้วนจากมุมมองที่หลากหลายของผู้เชี่ยวชาญ เพื่อนำมาวิเคราะห์หาแนวทางการป้องกัน

รูปที่ 4.2 สรุปผลการประชุมกลุ่มเป้าหมายที่กำหนด หรือ (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)

จากตางรางที่ 4.1 แสดงคุณสมบัติและความเชี่ยวชาญของผู้เข้าร่วมการสนทนากลุ่ม ทั้งหมด 44 คน

ตารางที่ 4.1 คุณสมบัติและความเชี่ยวชาญของผู้เข้าร่วมการสนทนากลุ่ม ทั้งหมด 44 คน

ผู้มีประสบการณ์เชี่ยวชาญ (P=44)	ระดับการศึกษา			ใบรับรองความปลอดภัยทางไซเบอร์ (Cybersecurity Certifications)
	ปริญญาตรี	ปริญญาโท	ปริญญาเอก	
P1-P3	-	-	3	3 CompTIA Security+ (Plus), ECSS, PECB DPO, CCDP, and CEH
P4-P18	-	15	-	9 AZ-500, AZ900, SC200, SC300, SC400, SC900, DP900, AI900 CompTIA Security+, AZ-104, CISSP, and CEHv11
P19-P44	26	-	-	14 VCP, CHFI, CompTIA Security+ (Plus), CompTIA Pen Test+, EICSS, ACE, ISC, CCNA CEH, CASP, CHFI, and ECSS

มหาวิทยาลัยรังสิต Rangsit University

จากการสนทนากลุ่มผู้วิจัยได้เก็บรวบรวมข้อมูลมาทำการการวิเคราะห์ข้อมูลแบบเชิงคุณภาพจากหลักการแนวทางปฏิบัติของเอ็นไอเอสที (NIST) ทั้ง 5 ส่วน ซึ่งได้ข้อสรุปในแต่ละขั้นตอนแนวการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ภัยในระบบควบคุมอุตสาหกรรมดังตารางที่ 4.2 ดังนี้

ตารางที่ 4.2 สรุปผลการประชุมกลุ่มเป้าหมายที่กำหนด หรือ (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)

สรุปผลการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)	
แนวคำถามสนทนากลุ่ม	สรุปข้อมูลจากการสนทนากลุ่ม
1. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิตร่างกายของบุคคล (Identify) 1.1 การบริหารจัดการทรัพย์สิน (Asset Management: AM) 1.2 การดำเนินการตรวจสอบสภาพแวดล้อม (Business Environment: BE) 1.3 การกำกับดูแล (Governance: GV)	1. ต้องมีการจัดการระบบทะเบียนทรัพย์สิน (Inventory) ในส่วนเทคโนโลยีสารสนเทศ (IT) เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) ที่ระบุทรัพย์สินของบริการที่สำคัญ ควรมีการตรวจสอบทะเบียนทรัพย์สิน และต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง 2. ระบุความเสี่ยงที่อาจจะเกิดขึ้นในแต่ละโซน เช่น ส่วนไอที (IT) ส่วนออฟฟิศ (Office) เทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม ได้แก่ เครือข่าย (Network) เซิร์ฟเวอร์ (Server) เดสก์ท็อป (Desktop) แล็ปท็อป (Laptop) อุปกรณ์ในเทคโนโลยีเชิงปฏิบัติการ ร่วมถึงผู้ใช้งานภายในและภายนอก 3. มีการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ตัวอย่าง เช่น เครื่องมือชื่อว่าอัปกาด (Up-Guard) ในการสแกนตรวจจับช่องโหว่ พร้อมแนะนำแนวทางการแก้ไขที่ละขั้นตอน 4. มีการจัดการผู้ให้บริการภายนอก (Third Party Management) รวมถึงการนำอุปกรณ์ต่าง ๆ ที่นำเข้าถึงในแต่ละโซนภายในบริษัทและส่วนเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม พร้อมบันทึกเหตุการณ์ไว้ทั้งหมด

ตารางที่ 4.2 สรุปผลการประชุมกลุ่มเป้าหมายที่กำหนด หรือ (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST) (ต่อ)

สรุปผลการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)	
แนวคำถามสนทนากลุ่ม	สรุปข้อมูลจากการสนทนากลุ่ม
1.4 การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment: RA) 1.5 การกำหนดกลยุทธ์บริหารจัดการความเสี่ยง (Risk Management Strategy: RM) 1.6 การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management: SC)	5. การจัดการการเข้าถึงที่ปลอดภัยจากภายนอกทั้งภายในไอทีโซน ออฟฟิศโซน และโอทีโซน เช่น การเชื่อมต่อคอมพิวเตอร์ระบบเครือข่ายแบบแลน (LAN) หรือวายฟาย (Wi-Fi) การเข้าถึงอินเทอร์เน็ต (Internet) แอปพลิเคชัน (Application) อีเมล (Email) ยูเอสบีแฟลชไดรฟ์ (USB Flesh drive) บลูทูธ (Bluetooth) เครือข่ายเสมือนส่วนตัววีพีเอ็น (Virtual Private Network: VPN) และผู้ให้บริการภายนอกมีข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาอย่างเคร่งครัด 6. การบริหารจัดการ (Governance) การกำหนดนโยบาย (Policy Setting) การกำหนดนโยบายที่ชัดเจน และเหมาะสมสำหรับองค์กร ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่สำหรับระบบควบคุมอุตสาหกรรม (ICS) จากกรณีการโจมตีที่เกิดขึ้นจริงจากมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) องค์กรได้พิจารณาถึงความสำคัญของรายการสินทรัพย์ให้สมบูรณ์ครบถ้วนและถูกต้องสำหรับการจัดการความเสี่ยงภายในสภาพแวดล้อมในส่วนเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม การป้องกันเชิงรุกรวมถึงนำแนวคิดไม่เชื่อใจใครตรวจสอบทุกอย่าง (Zero Trust) ในการประเมินความเสี่ยง การจัดการช่องโหว่ และการติดตามความล้าสมัย และเพิ่มในเนื้อหาการฝึกอบรมบุคลากรประจำไตรมาส ในส่วนไอที ตลอดจนข้อกำหนดด้านความปลอดภัยไซเบอร์ทางกฎหมาย และข้อบังคับที่มีผลต่อการปฏิบัติงาน เช่น จากเหตุ

มหาวิทยาลัยรังสิต Rangsit University

	การโจมตีของมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) เพื่อลดความเสี่ยงการเกิดซ้ำ ได้ออกข้อบังคับอย่างเคร่งครัดในการใช้ยูเอสบีแฟลชไดรฟ์ (USB Flesh Drive) และเพิ่มนโยบายป้องกันความเสี่ยงในขั้นตอนปฏิบัติงานอย่างเคร่งครัด พร้อมตรวจสอบความปลอดภัยในการนำเครื่องจักรเข้าออกภายในระบบควบคุมอุตสาหกรรม
2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) 2.1 กำหนดมาตรการควบคุมการเข้าถึง (Access Control: AC) 2.2 การสร้างความตระหนักและการฝึกอบรม (Awareness and Training: AT) 2.3 การกำหนดความมั่นคงปลอดภัยของข้อมูล (Data Security: DS) 2.4 กระบวนการบำรุงรักษา (Maintenance: MA) 2.5 จัดหาเทคโนโลยีการป้องกัน (Protective Technology: PT)	1. การควบคุมการเข้าถึงองค์กรต้องจัดหาระบบสำหรับป้องกันและการรักษาความมั่นคงปลอดภัยเพื่อเพิ่มประสิทธิภาพในการจัดการความมั่นคงปลอดภัย ต้องมีการเก็บรักษาบันทึกเหตุการณ์ของการเข้าถึงทั้งหมด 2. การสร้างความตระหนักผ่านข่าวสาร และการฝึกอบรม การจำลองเหตุการณ์เสมือนถูกโจมตีด้วยเทคนิคต่าง ๆ ไซเบอร์เอ็กเซอร์ไซส์ (Cyber Exercise) สำหรับเจ้าหน้าที่ไอที ไซเบอร์ดริล (Cyber Drill) สำหรับเจ้าหน้าที่ปฏิบัติการในออฟฟิศ และในส่วนของเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรมอย่างน้อยปีละ 1 ครั้ง 3. การกำหนดความมั่นคงปลอดภัยของข้อมูล มีการจัดการสำรองข้อมูล สาม-สอง-หนึ่ง รวมถึงสำรองข้อมูลอุปกรณ์ในส่วนของเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบไอทีทั้งหมด 4. การบำรุงรักษา การปรับปรุงซอฟต์แวร์ และการอัปเดตความปลอดภัยปิดช่องโหว่ที่เกิดขึ้นทันที 5. จัดหาเทคโนโลยีการป้องกันที่ทันสมัยอย่าง เช่น การเข้ารหัสข้อมูล (Data Encryption) ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDPS) ไฟร์วอลล์รักษาความปลอดภัยที่ช่วยปกป้องเว็บแอปพลิเคชัน (Web Application) จากการโจมตีทางไซเบอร์ (Web Application

	Firewall: WAF) ระบบจัดการข้อมูลและเหตุการณ์ความปลอดภัย ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามด้านความปลอดภัยได้อย่างมีประสิทธิภาพ (Security Information and Event Management: SIEM) ระบบป้องกันการสูญหายของข้อมูล (Data Loss Prevention: DLP), และการปกป้องอุปกรณ์ปลายทาง (Endpoint Detection and Response: EDR) ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับระบบควบคุมอุตสาหกรรม (ICS) การออกแบบสถาปัตยกรรมระบบโดยมีการป้องกันในเชิงลึกได้แบ่งออกเป็น 5 ชั้นดังนี้ 1) การจัดการความปลอดภัย (Security Management) 2) ความปลอดภัยทางกายภาพ (Physical Security) 3) ความปลอดภัยเครือข่าย (Network Security) 4) ความปลอดภัยของฮาร์ดแวร์ (Hardware Security) 5) ความปลอดภัยของซอฟต์แวร์ (Software Security) ในการป้องกันในเชิงลึกชั้นที่ 3 ความปลอดภัยเครือข่าย (Network Security) องค์กรอาจพิจารณา การแบ่งส่วนและการแยกเครือข่ายในด้านความปลอดภัยเครือข่าย เช่น เพอร์ดูโมเดล (Purdue Model) เพื่อเป็นแนวทางในกระบวนการออกแบบและจัดการป้องกันที่เหมาะสม สามารถช่วยป้องกันและลดความเสี่ยงจากการโจมตี ตรวจจับการเข้าถึงที่ผิดปกติด้วยระบบการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor and Password Authentication: MFA) ในการเข้าถึงแอปพลิเคชัน (Application) ส่วนเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) พร้อมป้องกันการสูญเสียข้อมูลด้วยการสำรองข้อมูลแบบออฟไลน์ตามหลักการสาม-สอง-หนึ่ง 3-2-1
3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	1. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ต้องสร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ การจัดประเภทและวิเคราะห์

มหาวิทยาลัยรังสิต Rangsit University

3.1 การตรวจจับเหตุการณ์และความผิดปกติ (Anomalies and Events: AE) 3.2 การตรวจสอบด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring: CM) 3.3 กระบวนการตรวจจับ (Detection Processes: DP)	เหตุการณ์ การระบุว่ามีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมด 2. การตรวจสอบด้านความมั่นคงปลอดภัยต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละ 1 ครั้ง 3. กระบวนการตรวจจับ ปรับใช้เครื่องมือที่ทันสมัยอย่าง เช่นเอสไออีเอ็ม (SIEM) เอกซ์ดีอาร์ (XDR) อีดีอาร์ (EDR) และเอสโอเออาร์ (SOAR) พร้อมเจ้าหน้าที่ตรวจสอบและแก้ไขได้ตามแผนที่กำหนดไว้ ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับระบบควบคุมอุตสาหกรรม ในส่วนของระบบปฏิบัติการ (Operating system: OS) หรือ โปรแกรมส่วนใหญ่ยังคงล้าสมัยในการใช้โปรแกรมป้องกันไวรัส การตรวจจับอาจต้องใช้แนวทางปฏิบัติพิเศษ และต้องตรวจสอบความเข้ากันได้ อย่างเช่น เครื่องมือเอกซ์ดีอาร์ที่ให้บริการสนับสนุนป้องกันเฉพาะของระบบควบคุมอุตสาหกรรม ชื่อว่าทีเอ็กซ์วัน สเตลลาร์ (TXOne Stellar) ของเทรนด์ไมโคร (Kobialka, 2023)
4. มาตรการเผชิญเหตุเมื่อตรวจพบภัยคุกคามทางไซเบอร์ (Respond) 4.1 การวางแผนการตอบสนอง (Response Planning: RP) 4.2 การสื่อสาร (Communications: CO) 4.3 การวิเคราะห์ (Analysis: AN) 4.4 การควบคุมดูแลและจำกัด (Mitigation: MI)	1. แผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan) ทีมมีจัดทำขั้นตอนสื่อสาร ฝึกซ้อม ควรมีการทบทวนและปรับปรุงปีละ 1 ครั้งหรือมากกว่า 2. แผนการสื่อสารในภาวะวิกฤต ควรจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อให้สามารถตอบสนองต่อวิกฤตที่เกิดขึ้นจากเหตุการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ 3. การฝึกซ้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Exercise) ควรมีการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง 4. การประเมินและการจัดการเหตุการณ์ทางความมั่นคงปลอดภัยไซเบอร์และไม่ใช่ทางไซเบอร์ (Cyber and Non-Cyber

4.5 การปรับปรุง (Improvements: IM)	Event Handling) ระบุและจำแนกเหตุการณ์ที่เกิดขึ้นที่ส่งผลกระทบต่อระบบควบคุมอุตสาหกรรม ตามแผนเผชิญเหตุ ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับระบบควบคุมอุตสาหกรรม (ICS) และแผนการตอบสนองภัยคุกคามทางไซเบอร์ (Incident Response Plan) เช่น การสื่อสาร การวิเคราะห์ การควบคุมดูแลและจำกัดขอบเขตการบุกรุกโจมตี เป็นต้น จากนั้นนำประสบการณ์ที่เกิดขึ้นจริงมาปรับปรุง นอกจากนี้องค์กรควรพิจารณา บุคลากรที่จำเป็น รวมถึงทรัพยากรทั้งภายในและภายนอกไว้ในแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)
5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) 5.1 การวางแผนการกู้คืน (Recovery Planning: RP) 5.2. การปรับปรุง (Improvements: IM) 5.3 สื่อสาร (Communications: CO)	1.จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ตรวจสอบให้แน่ใจว่าฝึกซ้อมอย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนตามที่กำหนดไว้ 2. แหล่งกู้ภัยสำรอง (Disaster Recovery Site: DR) ทำการสำรองข้อมูลสถานที่อื่นโดยสิ้นเชิงและสำรองข้อมูลตามหลักการสาม-สอง-หนึ่ง ในการกู้คืนสภาพข้อมูล ต้องมีการกำหนดระยะเวลาที่สำคัญของระยะเวลาหยุดชะงักที่ยอมรับได้ (Tolerable Period of Disruption: TPD) ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD) กำหนดเป้าหมายเวลาสำหรับการกู้คืนระบบให้กลับมาใช้งานได้ (Recovery Time Objective: RTO) พร้อมกำหนดจุดเวลาสำคัญสำหรับแผนการกู้คืนระบบ (Recovery Point Objective: RPO) เป็นต้น ควรมีแผนการทดสอบกู้ข้อมูลอย่างน้อยปีละ 1 ครั้ง 3. แผนกู้คืนสภาพคอมพิวเตอร์ควบคุมเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) ควรสำรองข้อมูลของค่าติดตั้งอุปกรณ์ในระบบควบคุมปีละ 1 ครั้ง 4. การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Management) มีการกำหนด

ข้อตกลงระดับสัญญาการให้บริการ (Service Level Agreement: SLA) ในกระบวนการบริหารจัดการเหตุการณ์ที่ผิดปกติ เพื่อความรวดเร็วในการแก้ปัญหาตามแผนงานที่กำหนดไว้ได้

5. มีกระบวนการดำเนินการเหตุการณ์ที่มีผลกระทบร้ายแรงต่อการดำเนินงานธุรกิจในส่วนระบบควบคุมอุตสาหกรรม

ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) ของระบบควบคุมอุตสาหกรรม ได้แก่ 1) การวางแผนการกู้คืนรายการทรัพยากรภายในและภายนอก ควรมีแผนการทดสอบการกู้ข้อมูลคืนจากการสำรองข้อมูลแบบออฟไลน์ อย่างน้อยปีละ 1 ครั้ง 2) แผนการสื่อสารที่มีประสิทธิภาพทั้งภายในและภายนอก

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 5

บทสรุปและข้อเสนอแนะ

ในบทนี้จะนำเสนอบทสรุปและข้อเสนอแนะของแนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่เหมาะสมของระบบควบคุมในโรงงานอุตสาหกรรม จากแนวทางของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกา (NIST) โดยใช้ข้อมูลจากการวิจัยเชิงคุณภาพ การจัดกลุ่มสนทนาเฉพาะประเด็น หรือ Focus Group โดยมีหัวข้อดังต่อไปนี้

5.1 สรุปแนวทางทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่เหมาะสมของระบบควบคุมในโรงงานอุตสาหกรรมในกรอบของนิสต์จากสนทนากลุ่ม

5.2 อภิปรายผลแนวทางที่นำเสนอ

5.3 ข้อเสนอแนะ

5.1 สรุปทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ที่เหมาะสมของระบบควบคุมในโรงงานอุตสาหกรรมในกรอบของนิสต์จากสนทนากลุ่ม

งานวิจัยนี้ดำเนินการศึกษาการป้องกันมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) สำหรับระบบควบคุมอุตสาหกรรม (ICS) จากกรณีศึกษาโรงงานอุตสาหกรรมขนาดใหญ่ และได้นำแนวคิดไม่เชื่อใจใครตรวจสอบทุกอย่าง (Zero Trust) ซึ่งเป็นแนวคิดด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นที่การป้องกันการเข้าถึงระบบควบคุมอุตสาหกรรมตั้งแต่เริ่มต้น และการสร้างความสามารถในการกู้คืนระบบอย่างรวดเร็วหากเกิดการโจมตี ซึ่งได้สอดคล้องกับผลจากการสนทนากลุ่มบนพื้นฐานของเอ็นไอเอสที (NIST) การจัดการในส่วนเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม โดยในงานวิจัยฉบับนี้ได้ นำเสนอแผนภาพแสดงความสัมพันธ์ของแนวทางป้องกันมัลแวร์เรียกค่าไถ่สำหรับระบบควบคุมอุตสาหกรรมตามแนวทางของมาตรฐานเอ็นไอเอสที ทั้ง 5 ขั้นตอน และโมเดล (Model) ในการใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม เพื่อป้องกันภัยจากมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์

ตารางที่ 5.1 แนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานโดยใช้แนวทางปฏิบัติของนิสต์

ลำดับขั้นตอน	แนวทางทางการรักษาความมั่นคงปลอดภัย	ข้อเสนอแนะพิเศษในส่วนของระบบควบคุมในโรงงานอุตสาหกรรม
1. ระบุสินทรัพย์	ระบุและจัดทำเอกสาร OT/ ICS รายการอุปกรณ์ ทั้งหมด รวมถึง ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และบริการ	ในส่วนโอทีและไอซีเอส (OT,ICS) การป้องกันเชิงรุกจัดการรายการสินทรัพย์ที่สมบูรณ์ครบถ้วนและถูกต้อง นำแนวคิด ไม่เชื่อใจใครตรวจสอบทุกอย่าง (Zero Trust) สำหรับการจัดการความเสี่ยงภายใน และภายนอก รวมถึงการประเมินความเสี่ยง การจัดการช่องโหว่ จัดลำดับความสำคัญของสินทรัพย์ และการติดตามความล้าสมัยตลอดจนข้อกำหนดด้านความปลอดภัยทางไซเบอร์ทางกฎหมายและข้อบังคับที่มีผลต่อการปฏิบัติงาน การสื่อสารและการประสานงานระหว่างองค์กร
2. ป้องกันความเสี่ยง	ประเมินความเสี่ยงต่อ OT/ ICS รายการอุปกรณ์ ระบุภัยคุกคามและช่องโหว่ พัฒนาแผนป้องกันความเสี่ยง	ในส่วนโอทีและไอซีเอส (OT,ICS) การป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) ต้องมีการป้องกันแบบหลายชั้น (Defense-in-Depth) การแบ่งส่วนและการแยกเครือข่าย โดยใช้โมเดลที่ได้รับการยอมรับในอุตสาหกรรม เช่นเพอร์ดูโมเดล (Purdue Model) เพื่อเป็นแนวทางในการออกแบบและจัดการป้องกันที่เหมาะสม และตรวจความถูกต้องด้วยการยืนยันตัวตนแบบหลายปัจจัย (MFA) ในการเข้าถึงแอปพลิเคชัน สำรองข้อมูลแบบออฟไลน์ และการฝึกอบรมและให้ความรู้แก่พนักงาน (Training and Awareness) เกี่ยวกับการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware)

ตารางที่ 5.1 แนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานโดยใช้แนวทางปฏิบัติของนิสต์ (ต่อ)

ลำดับขั้นตอน	แนวทางทางการรักษาความมั่นคงปลอดภัย	ข้อเสนอแนะพิเศษในส่วนของระบบควบคุมในโรงงานอุตสาหกรรม
3. ป้องกัน	การป้องกันข้อมูล การป้องกันระบบ และการกู้คืนข้อมูล	ในส่วนโอทีและไอซีเอส (OT,ICS) การป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) ควรปรับใช้เครื่องมือที่ทันสมัยในการตรวจจับเหตุการณ์และความผิดปกติ เช่นระบบตรวจจับการบุกรุกไอดีเอส (IDS) และ ระบบป้องกันการบุกรุกไอพีเอส (IPS) และใช้ระบบตรวจจับที่ครอบคลุมด้วยเอกซ์ดีอาร์ (XDR) ผสมผสานกับการตอบสนองต่อปลายทางอีดีอาร์ (EDR) ระบบปฏิบัติการหรือโปรแกรมส่วนใหญ่ยังคงเป็นเวอร์ชันที่ล้าสมัยอาจต้องใช้แนวทางปฏิบัติพิเศษและตรวจสอบความเข้ากันได้
4. ตรวจสอบและตรวจสอบ	ตรวจสอบและตรวจสอบมาตรการป้องกันอย่าง	ในส่วนโอทีและไอซีเอส (OT,ICS) แผนการตอบสนองภัยคุกคามทางไซเบอร์ (Incident Response Plan) เช่น การสื่อสาร การวิเคราะห์ การควบคุมดูแลและจำกัดขอบเขตการบุกรุกโจมตี เป็นต้น จากนั้นนำประสบการณ์ที่เกิดขึ้นจริงมาปรับปรุง นอกจากนี้องค์กรควรพิจารณาบุคลากรที่จำเป็น รวมถึงทรัพยากรทั้งภายในและภายนอกไว้ในแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)
5. ตอบสนองต่อเหตุการณ์	พัฒนาและทดสอบแผนตอบสนองต่อเหตุการณ์เพื่อจัดการกับภัย	ในส่วนโอทีและไอซีเอส (OT,ICS) การวางแผนการกู้คืนเมื่อถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ทีมไออาร์ (IR Team) ปฏิบัติตามขั้นตอนการป้องกันส่วนที่เหลือ พร้อมการกู้

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 5.1 แนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานโดยใช้แนวทางปฏิบัติของนิสต์ (ต่อ)

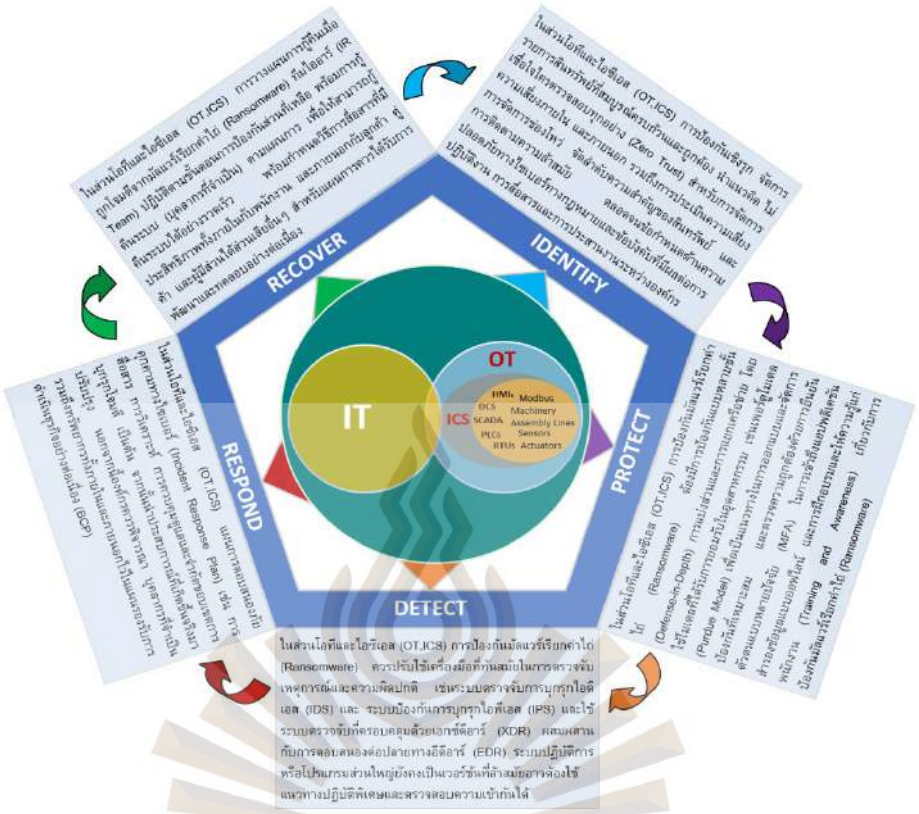
ลำดับขั้นตอน	แนวทางทางการรักษาความมั่นคงปลอดภัย	ข้อเสนอแนะพิเศษในส่วนของระบบควบคุมในโรงงานอุตสาหกรรม
	คุกคามและเหตุการณ์ร้ายแรง	คืนระบบ (บุคลากรที่จำเป็น) ตามแผนการ เพื่อให้สามารถกู้คืนระบบได้อย่างรวดเร็ว พร้อมกำหนดวิธีการสื่อสารที่มีประสิทธิภาพทั้งภายในกับพนักงาน และภายนอกกับลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียอื่น ๆ สำหรับแผนการควรได้รับการพัฒนาและทดสอบอย่างต่อเนื่อง

5.2 อภิปรายผลแนวทางที่นำเสนอ

5.2.1 แนวทางที่นำเสนอ

จากตารางที่ 5.1 ได้นำเสนอแผนภาพแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานแสดงถึงความสัมพันธ์ระหว่างเทคโนโลยีสารสนเทศ (IT), เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) บนพื้นฐาน 5 ขั้นตอนของแนวทางของเอ็นไอเอสที (NIST) ได้ดังรูปที่ 5.1

มหาวิทยาลัยรังสิต Rangsit University



รูปที่ 5.1 แนวทางป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมบนพื้นฐานจากแนวทางปฏิบัติของเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) เฉพาะจุดเด่นที่เพิ่มเติมจากเอ็นไอเอสที

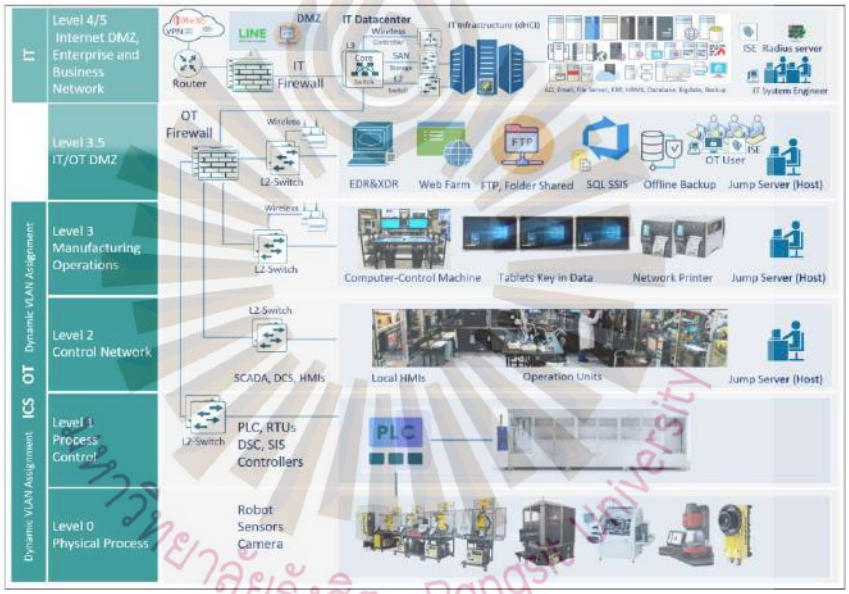
จากรูปที่ 5.1 ที่ได้นำเสนอในในงานวิจัยฉบับนี้ เป็นแผนภาพแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานในภาพรวม สำหรับในในรูปที่ 5.2 เป็นโมเดลในการใช้งานจริงระหว่างไอทีโซน (IT Zone) และโอทีโซน (OT Zone) ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรี อยุธยา เพื่อป้องกันภัยจากมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์

จากรูปที่ 5.1 ได้ใช้แนวทางเดียวกันกับงานวิจัยของ คริชณะ ฉิมมณี และมณีสุข โชติรุ่งรัตน์ (2564) ที่ได้นำเสนอการแนวทางการป้องกันมัลแวร์เรียกค่าไถ่บนพื้นฐานของไอเอสที (NIST) เวอร์ชัน (Version) 8374 (Draft) ฉบับร่าง แต่ยังไม่ได้ออกแบบมาสำหรับส่วนเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) นอกจากนี้ยังสอดคล้องกับงานวิจัยของ Wiboonrat (2022) ซึ่งได้นำเสนอแนวทางการป้องกันมัลแวร์เรียกค่าไถ่บนเอ็นไอเอสที เวอร์ชัน (Version) SP 800-82r2 ซึ่งเป็นเกี่ยวกับระบบควบคุมอุตสาหกรรมโดยเฉพาะ แต่อย่างไรก็ตามยังเป็นฉบับร่างอยู่ ดังนั้น รูปที่ 5.1 จึง

เป็นแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานที่ได้รวมองค์ประกอบของเทคโนโลยีเชิงปฏิบัติการ, ระบบควบคุมอุตสาหกรรมและเอ็นไอเอสทีเวอร์ชัน (Version) SP 800-82r3 เข้าด้วยกัน (Stouffer et al., 2023, pp.90-138)

5.2.2 การประยุกต์แนวทางที่นำเสนอกับระบบจริง

เพื่อเป็นการพิสูจน์ว่า แนวคิดที่นำเสนอในรูปที่ 5.1 สามารถนำมาประยุกต์ใช้งานจริงในการป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรม ดังนั้น ในรูปที่ 5.2 ได้แสดงโมเดล (Model) การนำไปใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม



รูปที่ 5.2 โมเดลการนำไปใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) กรณีศึกษาโรงงานอุตสาหกรรมขนาดใหญ่ ที่มีเงินทุนกว่า 200 ล้านบาท และคนงานกว่า 200 คนขึ้นไป ในเขตพื้นที่พระนครศรีอยุธยา

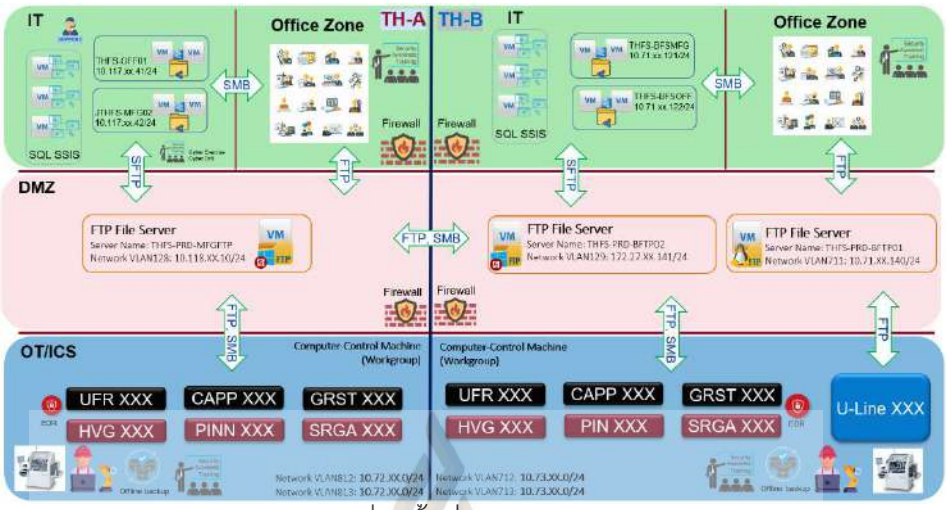
จากรูปที่ 5.2 แสดงถึงการป้องกัน ลดความเสี่ยง และจำกัดขอบเขตพื้นที่ได้รับความเสียหายจากการถูกโจมตีด้วยการแบ่งส่วนและการแยกเครือข่าย (Network Segmentation and Isolation) ได้พิจารณาใช้เพอร์ดูโมเดล (Purdue Model) เพื่อป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์จากมัลแวร์เรียกค่าไถ่ (Ransomware) โดยเป็นเชื่อมต่อระหว่างส่วนงานเทคโนโลยีสารสนเทศ (IT), ส่วนงานเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) ซึ่งเป็นกรณีศึกษาจริงในโรงงานอุตสาหกรรมขนาดใหญ่ในพื้นที่พระนครศรีอยุธยา ซึ่งให้ความสำคัญหัวข้อดังต่อไปนี้

5.2.2.1 การไหลของข้อมูล (Data Flow Model) ข้อมูลจากระบบควบคุมอุตสาหกรรม (ICS) ในรูปที่ 5.2 จากระดับชั้น 1 การนำข้อมูลออกในทิศทางเดียวเท่านั้นไปยังระดับชั้น 3.5 ฐานข้อมูลระดับย่อย (Database) และฐานข้อมูลระดับย่อยจะทำการรวมข้อมูลด้วยเอสคิวเอล เอสเอสไอเอส (SQL Server Integration Services: SSIS) ส่งผ่านในแต่ละระดับชั้นไปยังระดับชั้น 4 ฐานข้อมูลเอสคิวแอลหลักระบบคลังข้อมูล (Data Warehouse) โดยการกำหนดนโยบายเอซีเอล (ACLs) อนุญาตโปรโตคอลทีซีพีพอร์ต (TCP Ports) 1433, 4022, 135, 1434, และยูดีพีพอร์ต (UDP Port) 1434 เท่านั้น พร้อมมีการตรวจสอบและควบคุมการเข้าถึงข้อมูล ซึ่งมีเพียงผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1071 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) ในรูปที่ 4.1

5.2.2.2 การพิสูจน์ตัวตนของแต่ละระดับชั้น ในรูปที่ 5.1 ระหว่างระดับชั้น 3.5 กับระดับชั้น 4 และ 5 ซึ่งเป็นจุดอ่อนในปัจจุบัน จากรูปจะเห็นได้ว่าโมเดล (Model) นี้มุ่งเน้นไปที่การจัดการเครือข่าย และการพิสูจน์ตัวตน (Authentication) การป้องกันด้วยการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management) ระบบจะมีการยืนยันตัวตนที่มอบสิทธิ์ในการใช้งานแก่ผู้ใช้เข้าถึงระบบหรือข้อมูลที่จำเป็นได้เท่านั้น เพื่อเพิ่มความน่าเชื่อถือด้วยการกำหนดการเข้าถึงแอปพลิเคชัน (Application) ด้วยการยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication: MFA) การยืนยันตัวตนผู้ใช้จะต้องระบุข้อมูลจากอย่างน้อย 2 ปัจจัยที่แตกต่างกัน (2FA) เช่น ชื่อผู้ใช้พร้อมทั้งรหัสผ่านที่มีความซับซ้อนที่ปลอดภัยตามนโยบายกำหนด และป้อนรหัสโอทีพี (OTP) ยืนยันตัวตนจากแอปพลิเคชัน (Application) ที่สร้างรหัสโอทีพี (OTP) บนโทรศัพท์มือถือ เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1199 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) ในรูปที่ 4.1 ร่วมถึงการเข้าถึงระบบจากเครือข่ายเสมือนส่วนตัววีพีเอ็น (Virtual Private Network: VPN) เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1133 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) ในรูปที่ 4.1

5.2.2.3 การควบคุมการเข้าถึง (Access Control) และเพิ่มความปลอดภัยในระหว่างโซน ซึ่งได้ติดตั้งไฟร์วอลล์ (Firewall) เพื่อแยกส่วนในการควบคุมการเข้าถึงระหว่างเทคโนโลยีสารสนเทศ (IT), เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) โดยทำการกรองแพ็กเก็ต (Packet Filtering) จากไฟร์วอลล์ (Firewall) ตรวจจับสถานะ ป้องกันการโจมตี และลดความเสี่ยงการโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) โดยจัดการเครือข่าย (Network) นั้นได้กำหนดไดนามิควีแลนแอสซายเม้นท์ (Dynamic VLAN Assignment) และมีระบบพิสูจน์ตัวตนจากเรเดียสเซิร์ฟเวอร์ (Radius Server) ซึ่งจะทำงานร่วมกับกลุ่มผู้ใช้ในแอคทีฟไดเร็กทอรี (Active Directory: AD)

สามารถกำหนดนโยบายเน็ตเวิร์กในการเข้าถึงที่ปลอดภัยให้กับเครื่องไคลเอนต์ (Client) ในแต่ละระดับชั้นโดยให้ความสำคัญในส่วนระบบควบคุมอุตสาหกรรม ยึดตามหมายเลขวีแลน (VLAN) แต่ในส่วนของอุปกรณ์ระบบปฏิบัติการ หรือโปรแกรมที่ยังคงเป็นเวอร์ชันที่ล้าสมัย ที่ยังคงต้องการเชื่อมต่อเข้าในระบบเครือข่ายของเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม จะแยกคอมพิวเตอร์เครื่องเวอร์ชันที่ล้าสมัยดังกล่าว ออกจากการควบคุมของแอคทีฟไดเร็กทอรีโดเมน (Active Directory Domain) กลับไปเป็นคอมพิวเตอร์แบบสแตนด์อโลน (Standalone Computer) ที่ไม่ได้ขึ้นตรงกับเซิร์ฟเวอร์ (Server) ใด ๆ โดยกำหนดการอนุญาตหรือปฏิเสธการเข้าถึงระบบเครือข่ายด้วย (Media Access Control Address: MAC Address) ดังกล่าวข้างต้นเพื่อกำหนดนโยบาย (Dynamic Access Control List: ACL) พร้อมทำการกรองแพ็กเก็ต (Packet Filtering) และตรวจจับสถานะ ที่ส่งข้อมูลผ่านไฟร์วอลล์ให้เป็นไปตามเงื่อนไข ในรูปที่ 5.2 ระหว่างระดับชั้น 3.5 กับระดับชั้น 4 และ 5 โดยใช้นโยบายที่สร้างขึ้นมาเป็นเงื่อนไขเพื่อระบุสิทธิในการอนุญาตหรือปฏิเสธการเข้าถึงทรัพยากรข้อมูลระหว่างเครื่องคอมพิวเตอร์ หรือระหว่างระดับชั้นเครือข่าย พร้อมทั้งให้ความสำคัญอย่างละเอียดในการอนุญาตพอร์ตของโปรโตคอลทีซีพี (Transmission Control Protocol: TCP) และยูดีพี (User Datagram Protocol: UDP) ที่จำเป็นต้องใช้งานเชื่อมถึงกันในแต่ละระดับชั้นเครือข่าย ตัวอย่างเช่น ในรูปที่ 5.2 ระหว่างระดับชั้น 3 กับระดับชั้น 3.5 การเข้าถึงไฟล์ข้อมูลการอนุญาตเข้าถึงด้วยพอร์ตโปรโตคอลทีซีพีสำหรับการถ่ายโอนไฟล์ด้วย FTP พอร์ต 20 และ 21 ในแต่ส่วน ระหว่างระดับชั้น 3.5 กับระดับชั้น 4 และ 5 สำหรับการแชร์ไฟล์ด้วย SMB พอร์ต 445, 139, 138, และ 137 เท่านั้น ซึ่งแสดงรูปที่ 5.3 แสดงนำไปใช้จริงในการควบคุมการเข้าถึง โดยการแยกส่วนระบบปฏิบัติการและแอปพลิเคชันที่ล้าสมัย ออกจากส่วนอื่น ๆ ของเครือข่าย ด้วยการกำหนดนโยบายเอซีเอล (ACLs) ด้วยไฟร์วอลล์ (Firewall) ระหว่างโซน เพื่อป้องกันและลดความเสี่ยงพื้นที่การโจมตีจากจากมัลแวร์เรียกค่าไถ่ (Ransomware) และที่สำคัญในการถึงข้อมูลจากเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม เช่น ซีเอสวีไฟล์ (CSV) จากเครื่องมือวัดทั้งหมดดังกล่าว ตามความสำคัญของข้อมูลการอนุญาตหรือปฏิเสธการเข้าถึงในแต่ระดับชั้น โดยการกำหนดนโยบายเอซีเอล (ACLs) อย่างเคร่งครัด พร้อมทั้งสร้างความตระหนักรู้กับเจ้าหน้าที่ และสำรองแบบออฟไลน์ เพื่อป้องกันลดความเสี่ยงและพื้นที่การโจมตีจากจากมัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1071 และ T1486 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) ในรูปที่ 4.1



รูปที่ 5.3 แสดงการป้องกันและลดความเสี่ยงพื้นที่การโจมตีในส่วนของระบบปฏิบัติการและแอปพลิเคชันที่ล้าสมัยจากมัลแวร์เรียกค่าไถ่ใน OT/ICS

5.2.2.4 การตรวจจับภัยคุกคาม (Threat Detection) โดยใช้เครื่องมืออีดีอาร์ (Endpoint Detection and Response: EDR) ในรูปที่ 5.2 ในระดับชั้น 2 และ 3 ต้องมีการตรวจจับภัยคุกคามที่หลากหลาย (Threat Detection) และใช้นโยบายควบคุมอย่างเคร่งครัดของคอมพิวเตอร์ควบคุมเครื่องจักร (Computer-Controlled Machine) ในการควบคุมการเข้าถึงของพอร์ตยูเอสบีแฟลชไดรฟ์ (USB Flesh drive) และบลูทูธ (Bluetooth) เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1091 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโตล็อคเกอร์ (CryptoLocker) ตามรูปที่ 4.1

5.2.3 ความสัมพันธ์ระหว่างวัตถุประสงค์และประโยชน์งานวิจัย

จากรูปที่ 5.4 แสดงความสัมพันธ์ระหว่างวัตถุประสงค์และประโยชน์งานวิจัยจากความสัมพันธ์ระหว่างวัตถุประสงค์ในข้อที่ 1, ข้อที่ 2 และ ข้อที่ 3 ซึ่งได้ผลลัพธ์ของประโยชน์งานวิจัยในข้อที่ 1 และข้อที่ 2

รูปที่ 5.4 แสดงความสัมพันธ์ระหว่างวัตถุประสงค์ในข้อที่ 1, ข้อที่ 2 และ ข้อที่ 3 และประโยชน์งานวิจัยในข้อที่ 1 และ ข้อที่ 2

จากรูปที่ 5.5 แสดงความสัมพันธ์ระหว่างวัตถุประสงค์และประโยชน์งานวิจัยจากความสัมพันธ์ระหว่างวัตถุประสงค์ในข้อที่ 4 ซึ่งได้ผลลัพธ์ของประโยชน์งานวิจัยในข้อที่ 3

รูปที่ 5.5 แสดงความสัมพันธ์ระหว่างวัตถุประสงค์ในข้อที่ 4 และประโยชน์งานวิจัยในข้อที่ 3

5.3 ข้อเสนอแนะ

การศึกษาวิจัยในอนาคตควรจะมีกรณีศึกษาเพิ่มเติมจากการโจมตีด้วยมัลแวร์เรียกค่าไถ่ชนิดอื่น ซึ่งจะทำให้ได้มีการวิเคราะห์เทคนิคการโจมตีอื่นเพิ่มเติม เพื่อจะได้นำมาออกแบบโมเดล (Model) ในการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ได้ครอบคลุมมากยิ่งขึ้น นอกจากนี้การวิเคาระห์การโจมตีด้วยมัลแวร์เรียกค่าไถ่ควรจะใช้จากกรอบแนวคิดของเฟรมเวิร์กทูเอสเมทริกซ์ (2S Matrix for Ransomware Attack) ที่จัดทำโดย Chimmanee & Jantavongso (2024) ซึ่งวิเคราะห์การโจมตี จากมัลแวร์เรียกค่าไถ่ใหม่ล่าสุด

บรรณานุกรม

กิตติคุณ มีทองจันทร และ วงศ์ยศ เกิดศรี. (2564). ปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานคร และปริมณฑล. *วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์, 7*(2), 1-14.

คริชณะ ฉิมมณี และ มณีสุข โชติรุ่งรัตน์. (2564). แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในเขตพื้นที่พุทธสถาน กรณีศึกษาเมสแก๊ง. *วารสารมหาจุฬาวิชาการ , 8*(3), 1-24.

จันทกานต์ ผลพล. (2563). *ทำความรู้จักกับ Cyber Resilience สิ่งที่ทำให้ไปต่อได้ในทุกสถานการณ์.* สืบค้นจาก https://www.cyfence.com/article/what-is-cyber-resilience/

จิตสุภา ฤทธิผลิน. (2564). *กลยุทธ์การคืนสภาพได้ทางไซเบอร์ แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิตอล.* สืบค้นจาก http://awc.ac.th/storage/research/736.pdf

มุทิตา เอี่ยมทิพย์. (2565). *บทความวิชาการ การสนทนากลุ่มเทคนิคการเก็บข้อมูลเชิงคุณภาพ.* สืบค้นจาก https://so01.tci-thaijo.org/index.php/JLASI/article/view/250740

สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย. (2566). *Ransomware คืออะไร?* สืบค้นจาก https://www.it.chula.ac.th/ransomware-คืออะไร/

อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์. (2564). แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. *วารสารสถาบันวิชาการป้องกันประเทศ, 12*(1), 1-15.

Abrams, L. (2021). *DearCry ransomware attacks Microsoft Exchange with Proxylogon exploits.* Retrieved from https://www.bleepingcomputer.com/news/security/ /dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/

Alamri, A. (2022). *Dragos Industrial Ransomware Analysis: Q2 2022.* Retrieved from https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2022/

Anant, G. (2020). Ransomware Attacks: Impact, Symptoms, Working, Preventive Measures and Response. *International Journal of Engineering and Advanced Technology(IJEAT), 9*(6),188-191. doi:10.35940/ijeat.F1336.089620

Andrew, S. (2023). *Digital Forensics คืออะไร.* Retrieved from https://www.orionforensics. .com/th/tag/computer-forensics-คือ

บรรณานุกรม (ต่อ)

Antonina, F., Viktoria, R., Tetiana, S., Serhiy, B., Mykhailyna, F., & Oksana, B. (2021). Ransomware Attacks: Risks, Protection and Prevention Measures. In *2021 11th international conference on advanced computer information technologies (ACIT),* 473-478. doi:10.1109/ACIT52158.2021.9548507

Bill, F., Murugiah, S., William, C., & Barker, K. S. (2022). *Ransomware Risk Management: A Cybersecurity Framework Profile.* Retrieved from https://www.nist.gov /publications/ransomware-risk-management-cybersecurity-framework-profile

Bill, T. (2022). *Foxconn confirms ransomware attack disrupted production in Mexico.* Retrieved from https://www.bleepingcomputer.com/news/security/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/

Chimmanee, K., & Jantavongso, S. (2024). Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN. *Expert Systems with Applications*, *249*, 123652. doi: 10.1016/j.eswa.2024.123652

Christiaan, B. (2018). *What drives a ransomware criminal? CoinVault developers convicted*. Retrieved from https://www.mcafee.com/blogs/other-blogs/mcafee-labs/what-drives-a-ransomware-criminal-coinvault-developers-convicted-in-dutch-court/

Georgios, M. M., Constantinos, K., Georgios, K., Craig, R., & Jacob, B. (2021). Industrial and Critical Infrastructure Security: Technical Analysis of real-life security incidents. *Computers and Communications (ISCC), 9*, 165295-165325. doi: 10.1109/ACCESS.2021.3133348

Giorgio, V. S., Vincenzo, G. C., & Micro M. (2021). Analysis, prevention and detection of ransomware attacks on Industrial Control Systems. *Network Computing and Applications (NCA), 1-5* doi: 10.1109/NCA53618.2021.9685713

Helpransomware. (2022). *Twelve Versions Of CryptoLocker And Tools For The Removal.* Retrieved from https://helpransomware.com/cryptolocker-versions/#Conclusions

บรรณานุกรม (ต่อ)

Huang, Y., Debnath, J., Iorga, M., Kumar, A., & Xie, B. (2019). CSAT: a user-interactive cyber security architecture tool based on nist-compliance security controls for risk management. *Electronics & Mobile Communication Conference (UEMCON)*, 0697-0707. doi: 10.1109/UEMCON47517.2019.8993090

Ilker, K., & Murat, A. (2020). Cyber Fraud: Detection and Analysis of the Crypto-Ransomware. *Electronics & Mobile Communication Conference (UEMCON),* 0764-0769. doi: 10.1109/UEMCON51285.2020.9298128

Ivan, B. (2022). *The Destructive Reality of Ransomware Attacks.* Retrieved from https://www.avast.com/c-biggest-ransomware-attacks

Jackson, A. (2023). *Top 10 ransomware attacks.* Retrieved from https://cybermagazine.com/articles/top-10-ransomware-attacks

Jitti, A. A., & Susan, M. G. (2019). A Survey on Preventing Crypto Ransomware Using Machine Learning. *Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 1*, 259-263. doi: 10.1109/ICICICT46008.2019.8993137

Juan, A., Herrera, L. I., Barona, A. L., Valdivieso, & Myriam H. (2019). A Survey on Situational Awareness of Ransomware Attacks - Detection and Prevention Parameters. *Remote Sensing, 11,*10. doi: 10.3390/rs11101168

Kaspersky. (2021). *Ransomware attacks and types: How do locky, Petya and other ransomware differ?.* Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Kamalanathan, K., Sethuraman, S., Krishanshree, A., & Venkat, P. R. (2022). Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *Computing Communication and Networking Technologies*, *10*, 12345-12364. doi: 10.1109/ACCESS.2022.3145372

บรรณานุกรม (ต่อ)

Keith, S., Michael, P., Cheeyee T., Timothy, Z., Victoria, P., & Suzanne, L. (2022). *Guide to Operational Technology (OT) Security.* Retrieved from https://csrc.nist.gov /pubs/sp/800/82/r3/ipd

Kobialka, D. (2023). *Stellar Cyber now offers XDR for Operational Technology (OT) Environments*. Retrieved from https://www.msspalert.com/ news/stellar-cyber-now-offers-xdr-for-operational-technology-ot-environments

Lawrence, A. (2021). *Asteelflash electronics maker hit by REvil ransomware attack.* Retrieved from https://www.bleepingcomputer.com/news/security/asteelflash-electronics-maker-hit-by-revil-ransomware-attack/

Li, T., Feng, C., & Hankin, C. (2020). Scalable Approach to Enhancing ICS Resilience by Network Diversity. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),* 398-410. doi: 10.1109/DSN48063.2020.00055

Loana, R. (2019). *The impact of cybersecurity over the last 5 years.* Retrieved from. https://def.camp/impact-cybersecurity-five-years/

Marcel, M., Ventzislav, N., Joost, R., Tobias, S., & Nikita, V. (2021). Cyber resilience for self-monitoring IOT devices. *Cyber Security and Resilience (CSR)*, 160-167. doi: 10.1109/CSR51186.2021.9527995

Megan, R. (2021). *Lockbit 2.0: Ransomware attacks surge after successful affiliate recruitment.* Retrieved from https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/

Michael, B. (2022). *CryptoLocker: Everything You Need to Know.* Retrieved from https://www.varonis.com/blog/cryptolocker

Microsoft Security Response Center (MSRC). (2019). *Prevent a worm by updating Remote Desktop Services (CVE-2019-0708).* Retrieved from https://msrc. microsoft.com/blog/2019/05/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Microsoft 365 Defender Threat Intelligence Team. (2020). *Ransomware groups continue to target healthcare, critical services; here's how to reduce risk.* Retrieved from https://www.microsoft.com/en-us/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

Miller, C. (2021 *Throwback attack: Blackenergy attacks the Ukrainian Power Grid.* Retrieved from https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/

MITRE ATT&CK. (2022). Retrieved from https://attack.mitre.org

Nagaraja, S., & Fathima, R. (2020). Ransomware threats. *International Journal of Engineering Research & Technology (IJERT)*, *8*(15), 64–68. doi: 10.17577/IJERTCONV8IS15015

Nakhonthai, P., & Chimmanee, K. (2022). Digital forensic analysis of ransomware attacks on industrial control systems: A case study in factories. In *2022 6th International Conference on Information Technology (InCIT),* 416-421. doi: 10.1109/InCIT56086.2022.10067356

Ude, O., & Swar, B. (2021). Securing Remote Access Networks Using Malware Detection Tools for Industrial Control Systems. *In 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*, 166-171. doi: 10.1109/ICPS49255.2021.9468212

Robert, F. (2016). *Shamoon 2: Return of the Disttrack Wiper.* Retrieved from https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., … Thompson, M. (2023). *NIST SP 800-82r3 Guide to Operational Technology (OT) Security.* Retrieved from https://csrc.nist.gov/pubs/sp/800/82/r3/final.

Suwanradee, A. (2017). *ทำความรู้จักกับ Active Directory (แอคทีฟ ไดเรคทอรี่) ที่ช่วยจัดการทรัพยากรในระบบ.* Retrieved from https://www.mindphp.com/คู่มือ/73-คืออะไร%20/4948-what-is-active-directory.html#google_vignette

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Teri, R. (2022). *Attack on Panasonic Canada Shows Conti is Still Dangerous*. Retrieved from https://securityboulevard.com/2022/04/attack-on-panasonic-canada-shows-conti-is-still-dangerous/

Thaicyberdefense. (2020). *MITRE ATT&CK อธิบายกลยุทธ์ เทคนิค และกระบวนการทำงานของแฮกเกอร์.* Retrieved from https://www.thaicyberdefense.com/mitre-att-ck-cybersecurity

Trend Micro Research. (2021). *What We Know About Darkside Ransomware and the US Pipeline Attack.* Retrieved from https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

Urooj, U., Maarof, M. A. B., & Al-rimy, B. A. S. (2021). A proposed adaptive pre-encryption crypto-ransomware early detection model. In *2021 3rd International Cyber Resilience Conference (CRC),* 1-6. doi: 10.1109/CRC50527.2021.9392548

Wiboonrat, M. (2022). Cybersecurity in Industrial Control Systems: An integration of information technology and operational technology, In *IECON 2022–48th Annual Conference of the IEEE Industrial Electronics Society,* 1-6. doi: 10.1109/IECON49645.2022.9968468

With Ransomware like CryptoWall, CryptoLocker & Chimera what's in store for 2016. (2022). Retrieved from https://www.titanhq.com/blog/what-does-ransomware-including-cryptowall-cryptolocker-chimera-have-in-stor/

Worachat. (2016). *RDP อาร์ดีพี หรือ Remote Desktop Connection รีโมท เดสท็อป คอนเนคชั่น คืออะไร.* Retrieved from https://mindphp.com/

Zhang, Y., Li, M., Zhang, X., He, Y., & Li, Z. (2022). *Defeat magic with magic: A novel ransomware attack method to dynamically generate malicious payloads based on PLC control logic.* Retrieved from https://www.mdpi.com/2076-3417/12/17/8408/htm

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก ก

เอกสารรับรองโครงการวิจัย โดยคณะกรรมการจริยธรรมการวิจัยในคน

มหาวิทยาลัยรังสิต Rangsit University

COA. No. RSUERB2023-058

RSU-ERB

เอกสารรับรองโครงการวิจัย (Certificate of Approval)

โดย คณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต

เอกสารรับรองเลขที่	:	COA. No. RSUERB2023-058
ชื่อโครงการวิจัย	:	แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่อยุธยา กรณีศึกษาคริปโตล็อคเกอร์แรนซัมแวร์ A GUIDELINE FOR RANSOMWARE DETECTION AND PREVENTION ON INDUSTRIAL CONTROL SYSTEMS IN THE FACTORIES AYUTTHAYA: A CASE STUDY CRYPTOLOCKER RANSOMWARE
ชื่อหัวหน้าโครงการวิจัย	:	นายพิทยา นครไทย
ชื่อนักวิจัยร่วม	:	รศ.ดร. ศริชณะ ฉิมมณี
หน่วยงานที่สังกัด	:	วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต
วิธีทบทวน	:	พิจารณาจริยธรรมการวิจัยในคนแบบเร่งด่วน (Expedited Review)
เอกสารที่รับรอง	:	1. แบบเสนอโครงการวิจัย 2. เอกสารชี้แจงผู้เข้าร่วมการวิจัย 3. หนังสือแสดงเจตนายินยอมเข้าร่วมการวิจัย 4. แบบสอบถาม/แบบสัมภาษณ์
วันที่รับรอง	:	21 เมษายน 2566
วันที่หมดอายุ	:	21 เมษายน 2568

มหาวิทยาลัยรังสิต Rangsit University

คณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต ได้พิจารณาและมีมติรับรองเอกสาร ดังที่ระบุไว้ข้างต้น โดยยึดหลักจริยธรรม Declaration of Helsinki, The Belmont Report, CIOMS Guideline และ International Conference on Harmonization in Good Clinical Practice หรือ ICH-GCP

ลงนาม .....

(รองศาสตราจารย์ ดร. ปานันท์ กาญจนกุล)

ประธานคณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต

คณะกรรมการจริยธรรมการวิจัยในคน สำนักงานจริยธรรมการวิจัย ห้อง 504, ชั้น 5, อาคารอาทิตย์ อุไรรัตน์ (ตึก 1), มหาวิทยาลัยรังสิต
โทร. 0-2791-5728 Email: rsuethics@rsu.ac.th

COA. No. RSUERB2023-058

Certificate of Approval
By
Ethics Review Board of Rangsit University

COA. No.	COA. No. RSUERB2023-058
Protocol Title	A GUIDELINE FOR RANSOMWARE DETECTION AND PREVENTION ON INDUSTRIAL CONTROL SYSTEMS IN THE FACTORIES AYUTTHAYA: A CASE STUDY CRYPTOLOCKER RANSOMWARE
Principle Investigator	Mr. Phitaya Nakhonthai
Co-Investigator	Assoc. Prof. Dr. Krishna (Sanon) Chimmanee
Affiliation	College of Digital Innovation Technology, Rangsit University
How to review	Expedited Review
Approval includes	1. Project proposal 2. Information sheet 3. Informed consent form 4. Data collection form/Program or Activity plan
Date of Approval:	21 April 2023
Date of Expiration:	21 April 2025

The prior mentioned documents have been reviewed and approved by Ethics Review Board of Rangsit University based Declaration of Helsinki, The Belmont Report, CIOMS Guideline and International Conference on Harmonization in Good Clinical Practice or ICH-GCP

Signature.....

(Associate Professor Dr. Panan Kanchanaphum)
Chairman, Ethics Review Board for Human Research

Ethics Review Board of Rangsit University, 5th floor, Arthit Ourairat Building (Bldg.1) Rangsit University
Tel. 0-2791-5728 Email: rsuethics@rsu.ac.th

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก ข
ค่าดัชนีความสอดคล้องของข้อคำถามกับวัตถุประสงค์ของการวิจัย

มหาวิทยาลัยรังสิต Rangsit University

แบบประเมินความสอดคล้อง (IOC) ของผู้เชี่ยวชาญ

ข้อที่	ผู้ทรงคุณวุฒิ จำนวน 3 ท่าน คะแนน			รวม (Σ R)	IOC	สรุปผล	ข้อเสนอแนะ
	คนที่ 1	คนที่ 2	คนที่ 3				
ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม							
1	0	1	1	2	0.67	ใช้ได้	
2	1	1	1	3	1.0	ใช้ได้	
3	1	1	1	3	1.0	ใช้ได้	
4	1	1	1	3	1.0	ใช้ได้	
ส่วนที่ 2 แบบสอบถามสัมภาษณ์เชิงลึกอ้างอิงจากทฤษฎีของ NIST							
1	1	1	1	3	1.0	ใช้ได้	
2	1	1	1	3	1.0	ใช้ได้	
3	1	1	1	3	1.0	ใช้ได้	
4	1	1	1	3	1.0	ใช้ได้	
5	1	1	1	3	1.0	ใช้ได้	
6	1	1	1	3	1.0	ใช้ได้	
7	1	1	1	3	1.0	ใช้ได้	
8	1	1	1	3	1.0	ใช้ได้	
9	1	1	1	3	1.0	ใช้ได้	
ส่วนที่ 3 คำถามจากบทความวิชาการ Digital Forensic Analysis of Ransomware Attacks on Industrial Control Systems: A Case Study in Factories							
1	1	1	1	3	1.0	ใช้ได้	
2	1	1	1	3	1.0	ใช้ได้	
3	1	1	1	3	1.0	ใช้ได้	
ส่วนที่ 4 ท่านเคยมีประสบการณ์จากการถูกโจมตีจากมัลแวร์เรียกค่าไถ่ อย่างไร และมีแนวทางป้องกันอย่างไร							
1	0	1	1	2	0.67	ใช้ได้	

ประวัติผู้วิจัย

ชื่อ	พิทยา นครไทย
วัน เดือน ปี เกิด	28 เมษายน 2527
สถานที่เกิด	จังหวัดมุกดาหาร ประเทศไทย
ประวัติการศึกษา	มหาวิทยาลัยราชภัฏพระนคร ปริญญาหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์ โปรแกรมวิชาเทคโนโลยี อุตสาหกรรม แขนงเทคโนโลยีคอมพิวเตอร์ อุตสาหกรรม, 2552
ที่อยู่ปัจจุบัน	เลขที่ 88/105 หมู่ 7 หมู่บ้านเดอะริชทาวน์ ตำบลห้วยทราย อำเภอหนองแค สระบุรี
สถานที่ทำงาน	บริษัท แมกเนคอมพ์ พรีซิชั่น เทคโนโลยี จำกัด (มหาชน)
ตำแหน่งปัจจุบัน	Senior System Engineer

มหาวิทยาลัยรังสิต Rangsit University