การวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์ และเครื่องมือวิเคราะห์เฉพาะทาง

นายณัฐพงษ์ รุ่งพรมมา

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

การวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์ และเครื่องมือวิเคราะห์เฉพาะทาง

นายณัฐพงษ์ รุ่งพรมมา

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ใบรับรองโครงร่างการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์ และเครื่องมือวิเคราะห์เฉพาะทาง

โดย นายณัฐพงษ์ รุ่งพรมมา

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

.....

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี)

..... อาจารย์ที่ปรึกษา

(รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

ชื่อ : นายณัฐพงษ์ รุ่งพรมมา
ชื่อการค้นคว้าอิสระ : การวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์และเครื่องมือวิเคราะห์เฉพาะทาง
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : รองศาสตราจารย์ ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ
ปีการศึกษา : 2567

บทคัดย่อ

การค้นคว้าอิสระฉบับนี้มีวัตถุประสงค์เพื่อ ศึกษา วิเคราะห์ และตรวจจับการโจมตีของ LockBit Ransomware โดยการจำลองสถานการณ์การโจมตีภายใน สภาพแวดล้อมเสมือนจริง (Virtual Environment) เพื่อให้ใกล้เคียงกับสถานการณ์ที่อาจเกิดขึ้นจริงมากที่สุด การทดลองเน้นการศึกษาพฤติกรรมการทำงานของแรนซัมแวร์ การตรวจจับ และแนวทางการป้องกันที่มีประสิทธิภาพ

ในการดำเนินการ ผู้วิจัยได้ใช้เครื่องมือด้านความมั่นคงปลอดภัย เช่น ระบบระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM Security Information and Event Management) ในการตรวจสอบและวิเคราะห์เหตุการณ์แบบเรียลไทม์ รวมถึงใช้เครื่องมือเฉพาะทาง เช่น Redline และ Any.Run เป็นต้น สำหรับการวิเคราะห์พฤติกรรมของมัลแวร์ และ Wazuh สำหรับการตรวจจับแบบเชิงลึก

ผลการศึกษานี้จะช่วยให้เกิดความเข้าใจที่ชัดเจนเกี่ยวกับ กลไกการทำงานของ LockBit Ransomware พร้อมทั้งนำเสนอแนวทางการตรวจจับ และป้องกันที่สามารถประยุกต์ใช้ในองค์กรได้อย่างมีประสิทธิภาพ ซึ่งจะช่วยเสริมมาตรการด้านความมั้นคงปลอดภัยไซเบอร์ และลดความเสี่ยงจากภัยคุกคามในอนาคต

(มีจำนวนทั้งสิ้น 49 หน้า)

คำสำคัญ : แรนซัมแวร์ การตรวจจับการโจมตี ความมั่นคงปลอดภัยทางไซเบอร์ การตรวจจับภัยคุกคาม การวิเคราะห์มัลแวร์

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Nattapong Rungpromma
Independent Study Title : Analyzing and Detecting LockBit Ransomware Attacks with Event Logs and Tools
Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Associate Professor Dr. Pongpisit Wuttidittachotti
Academic Year : 2024

ABSTRACT

This independent study aims to investigate, detect, and prevent attacks from LockBit Ransomware by simulating a real-world attack scenario. The objective is to closely examine the behavior and operational patterns of the ransomware under a controlled virtual environment that mirrors real-world conditions as accurately as possible.

To achieve this, the study employs advanced cybersecurity tools, including a Security Information and Event Management (SIEM) system, to perform real-time monitoring and analysis of security events. Additionally, specialized forensic tools such as Redline and Any.Run are used to analyze malware behavior, while Wazuh is implemented to detect and correlate anomalous activities across the system.

The results of this study are expected to enhance the understanding of LockBit's attack mechanisms and provide effective detection and prevention strategies. These findings can assist organizations in strengthening their cybersecurity posture and reducing the risk of ransomware attacks in the future.

(Total 49 Pages)

Keywords: Ransomware, Attack Detection, Cybersecurity, Threat Detection, Malware Analysis

_____ Advisor

กิตติกรรมประกาศ

ข้าพเจ้าขอกราบขอบพระคุณ รองศาสตราจารย วาที่ร่อยตรี ดร.พงษพิสิฐ วุฒิดิษฐโชติ อาจารย์ที่ปรึกษาโครงงานวิจัย ผู้ให้คำปรึกษา แนะนำ และให้ความช่วยเหลือด้วยความเอื้อเฟื้ออย่างยิ่งตลอดระยะเวลาการดำเนินงานวิจัย ทำให้ข้าพเจ้าสามารถศึกษาค้นคว้าในหัวข้อ “การวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์และเครื่องมือวิเคราะห์เฉพาะทาง” ได้สำเร็จตามวัตถุประสงค์ที่ตั้งไว้ ข้าพเจ้าขอขอบคุณคณาจารย์ทุกท่านในหลักสูตร และคณะ ที่ได้ถ่ายทอดความรู้ และให้การสนับสนุนในการศึกษา รวมถึงขอขอบคุณครอบครัว และเพื่อน ๆ ที่คอยเป็นกำลังใจ และให้ความช่วยเหลือในทุกช่วงเวลา ตลอดจนขอบคุณทุกแหล่งข้อมูล และเครื่องมือที่นำมาใช้ในการวิจัย ซึ่งล้วนมีส่วนสำคัญทำให้งานชิ้นนี้เสร็จสมบูรณ์

ณัฐพงษ์ รุ่งพรมมา

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมา และความสำคัญของปัญหา

ในยุคที่เทคโนโลยีดิจิทัลพัฒนาอย่างรวดเร็วแรนซัมแวร์ได้กลายเป็นภัยคุกคามที่สำคัญต่อองค์กรทั้งภาครัฐ และเอกชนในประเทศไทย

เมื่อระบบถูกโจมตี มัลแวร์ชนิดนี้จะเข้ารหัสไฟล์ และเรียกค่าไถ่เพื่อปลดล็อคไฟล์เหล่านั้น [1] แรนซัมแวร์ได้พัฒนา และซับซ้อนมากขึ้นตามกาลเวลา เนื่องจากแฮกเกอร์คิดค้นวิธีการใหม่ ๆ เพื่อสร้างรายได้จากการโจมตีของพวกเขา ในอดีต แฮกเกอร์มักใช้บริการออนไลน์อย่าง MoneyPak หรือ Paysafecard เพื่อรับเงินค่าไถ่ เป็นต้น แต่การเกิดขึ้นของสกุลเงินดิจิทัลได้เปลี่ยนแปลงรูปแบบการชำระเงินนี้ ปัจจุบัน ผู้โจมตีที่ใช้แรนซัมแวร์นิยมรับเงินค่าไถ่ผ่านสกุลเงินดิจิทัลเช่น Ethereum หรือ Bitcoin เป็นต้น

ในช่วงไม่กี่ปีที่ผ่านมา การโจมตีด้วยแรนซัมแวร์ได้กลายเป็นหนึ่งในภัยคุกคามไซเบอร์ที่ส่งผลกระทบอย่างมีนัยสำคัญต่อองค์กรในประเทศไทย โดยเฉพาะอย่างยิ่งในด้านการให้บริการ เนื่องจากเมื่อระบบคอมพิวเตอร์ถูกโจมตี องค์กรจะไม่สามารถเข้าถึงข้อมูล หรือดำเนินงานตามปกติได้ ส่งผลทำให้งานบริการลูกค้าต้องหยุดชะงัก ตัวอย่างเช่น กรณีของโรงพยาบาลบางแห่งในประเทศที่ไม่สามารถเข้าถึงประวัติข้อมูลผู้ป่วยได้ ส่งผลกระทบต่อทั้งการรักษา และการดูแลผู้ป่วยอย่างต่อเนื่อง เป็นต้น

ในมุมของผลกระทบทางการเงิน องค์กรจำนวนมากจำเป็นต้องพิจารณาการจ่ายค่าไถ่เพื่อแลกกับการกู้คืนข้อมูล ซึ่งนอกจากจะมีค่าใช้จ่ายสูงแล้ว ยังไม่มีหลักประกันว่าข้อมูลที่ถูกเข้ารหัสจะสามารถกู้คืนได้จริง อีกทั้งยังมีภาระค่าใช้จ่ายเพิ่มเติมในการฟื้นฟูระบบ ปรับปรุงโครงสร้างความปลอดภัย และวางแผนป้องกันการโจมตีที่อาจเกิดขึ้นในอนาคต ซึ่งล้วนเป็นภาระทางการเงินที่หนักสำหรับองค์กร

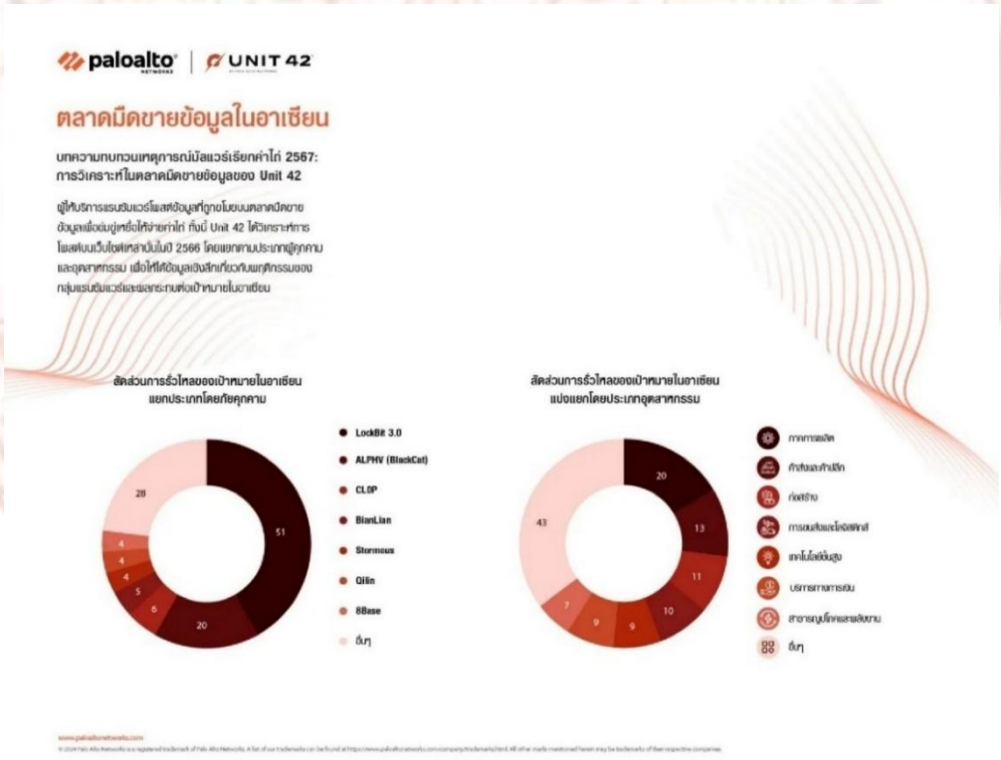
ด้านความเชื่อมั่นของผู้ใช้บริการก็เป็นอีกประเด็นที่ไม่ควรมองข้าม เมื่อเกิดเหตุการณ์ข้อมูลลูกค้าถูกเข้ารหัส หรือหลุดรั่วออกไป ไม่ว่าจะเป็นข้อมูลส่วนบุคคล หรือข้อมูลทางการเงิน เป็นต้น ย่อมส่งผลต่อความไว้วางใจของลูกค้า และบั่นทอนภาพลักษณ์ขององค์กรอย่างหลีกเลี่ยงไม่ได้ ความเสียหายนี้อาจส่งผลต่อความน่าเชื่อถือในระยะยาว และอาจส่งผลกระทบต่อความสัมพันธ์ระหว่างองค์กรกับผู้มีส่วนได้ส่วนเสีย

ท้ายที่สุด การโจมตีด้วยแรนซัมแวร์ยังส่งผลโดยตรงต่อการดำเนินธุรกิจโดยรวม เนื่องจากเมื่อระบบหยุดทำงาน องค์กรจะไม่สามารถดำเนินกิจกรรมทางธุรกิจได้ตามแผนอาทิ การจัดซื้อจัดจ้าง การให้บริการ หรือแม้แต่การทำธุรกรรมพื้นฐาน เป็นต้น ซึ่งในบางกรณีอาจนำไปสู่การสูญเสียลูกค้า และโอกาสทางธุรกิจในระยะยาว

Ransomware as a Service (RaaS) ถือเป็นการพัฒนาที่สำคัญในวงการแรนซัมแวร์ แนวคิดนี้ทำให้แฮกเกอร์ที่ไม่มีทักษะการเขียนโค้ดขั้นสูงสามารถเริ่มการโจมตีได้ง่ายขึ้น โดยให้บุคคลที่มีความสามารถทางเทคนิคเช่าแรนซัมแวร์ขั้นสูง [2] หนึ่งในแรนซัมแวร์ที่รู้จักกันดีของ RaaS คือ LockBit Ransomware ซึ่งมุ่งเป้าไปที่เซิร์ฟเวอร์ขององค์กร และเข้ารหัสข้อมูลสำคัญก่อนจะเข้ารหัสไฟล์เพิ่มเติมอย่างต่อเนื่อง ซึ่งอาจกระทบต่อระบบคอมพิวเตอร์ที่เชื่อมโยงกัน [3] ผลที่ได้คือผู้ใช้จะเห็นข้อความเรียกค่าไถ่บนหน้าจอของเครื่อง แจ้งว่าข้อมูลถูกเข้ารหัส และต้องชำระค่าไถ่เป็นสกุลเงินดิจิทัลเพื่อปลดล็อกไฟล์ ซึ่งแนวทางนี้ได้รับความนิยมจากแรนซัมแวร์อื่น เช่น REvil [4] เป็นต้น

ความรุนแรงของปัญหาไม่เพียงแต่สะท้อนให้เห็นถึงการเพิ่มขึ้นของจำนวนการโจมตี แต่ยังรวมถึงผลกระทบทางการเงิน และการดำเนินธุรกิจ ที่รุนแรง เช่น การหยุดชะงักของระบบ ส่งผลให้ไม่สามารถให้บริการลูกค้าได้ตามปกติ การสูญเสียข้อมูลสำคัญที่อาจถูกนำไปขายในตลาดมืด และความเชื่อมั่นของลูกค้าลดลง เป็นต้น เนื่องจากข้อมูลส่วนบุคคล และข้อมูลทางการเงินถูกละเมิด เป็นต้น [5], [6]

ด้วยเหตุนี้ การศึกษาปัญหาแรนซัมแวร์จึงมีความสำคัญอย่างยิ่ง เนื่องจากจะช่วยให้องค์กรต่าง ๆ สามารถวางมาตรการป้องกัน และตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ รวมถึงลดความเสียหายที่อาจเกิดขึ้นในอนาคต [7]



ภาพที่ 1-1 สถิติภัยคุกคามและเป้าหมายการโจมตีในอาเซียนในปี 2567 [17]

LockBit Ransomware เป็นหนึ่งในกลุ่มแรนซัมแวร์ที่มีอิทธิพลมากที่สุดในโลกไซเบอร์ในปัจจุบัน โดยเฉพาะในรูปแบบของ Ransomware-as-a-Service (RaaS) ซึ่งช่วยให้ผู้ที่ไม่มีทักษะการเขียนโค้ดขั้นสูง สามารถเช่าแรนซัมแวร์เพื่อโจมตีเป้าหมายได้ [2] กลุ่มนี้เริ่มปรากฏตัวครั้งแรกในปี 2019 และพัฒนาจนถึงเวอร์ชันล่าสุด LockBit 3.0 ซึ่งมีความสามารถในการหลบเลี่ยงการตรวจจับ และแพร่กระจายได้ดียิ่งขึ้น

LockBit Ransomware เป็นมัลแวร์เรียกค่าไถ่ที่มีคุณสมบัติเด่นหลายประการ โดยหนึ่งในคุณสมบัติหลักคือความสามารถในการเข้ารหัสข้อมูลอย่างรวดเร็ว LockBit Ransomware ใช้อัลกอริธึมการเข้ารหัสขั้นสูงในการเข้ารหัสไฟล์บนเซิร์ฟเวอร์ และคอมพิวเตอร์เป้าหมาย ส่งผลให้เหยื่อไม่สามารถเข้าถึงข้อมูลที่สำคัญได้ทันทีภายหลังการติดมัลแวร์ อีกทั้งยังมีลักษณะการโจมตีแบบ Double Extortion หรือการข่มขู่สองขั้น กล่าวคือ นอกจากการเรียกค่าไถ่เพื่อปลดล็อกไฟล์แล้ว ผู้โจมตียังข่มขู่ว่าจะเปิดเผยข้อมูลที่ขโมยไป หากเหยื่อไม่ยอมชำระเงินตามที่ร้องขอ วิธีการดังกล่าวช่วยเพิ่มแรงกดดันต่อเหยื่อในการตัดสินใจจ่ายค่าไถ่โดยเร็ว นอกจากนี้ LockBit Ransomware ยังมีการใช้สกุลเงินดิจิทัล เช่น Bitcoin หรือ Monero เป็นช่องทางหลักในการรับเงินค่าไถ่ เป็นต้น ซึ่งเป็นอีกกลยุทธ์หนึ่งที่ช่วยปกปิดตัวตนของผู้โจมตี และทำให้ยากต่อการติดตามเส้นทางทางการเงิน

1.2 วัตถุประสงค์

1.2.1 วิเคราะห์พฤติกรรมในกระบวนการทำงานของ LockBit Ransomware

1.2.2 พัฒนา และทดสอบโมเดลการตรวจจับ LockBit Ransomware โดยใช้การจำลองการโจมตีโดยแรนซัมแวร์ตัวจริง

1.3 ขอบเขตการวิจัย

1.3.1 ศึกษางานวิจัยที่เกี่ยวข้องกับการตรวจจับ และป้องกันแรนซัมแวร์ในแง่มุมต่าง ๆ เพื่อทำความเข้าใจแนวทาง วิธีการ หรือเทคนิคที่ถูกนำมาใช้ในงานที่ผ่านมา ทั้งในด้านการวิเคราะห์พฤติกรรม การตรวจสอบไฟล์ และการตอบสนองต่อเหตุการณ์ พร้อมทั้งศึกษาวิธีการใช้งานเครื่องมือ (Tools) หรือโปรแกรมที่เกี่ยวข้อง ซึ่งจะถูกนำมาใช้ในกระบวนการทดลอง หรือการเก็บข้อมูลในงานวิจัยนี้

1.3.2 ใช้ Tools Forensic Analysis ในการวิเคราะห์การทำงานของแรนซัมแวร์ Redline ในการวิเคราะห์หน่วยความจำ และไฟล์ในระบบ มีการใช้งานระบบ Sandbox ในการช่วยวิเคราะมัลแวร์เพิ่มเติม

1.3.3 ใช้ระบบระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM Security Information and Event Management) โดยเฉพาะเครื่องมือ Wazuh ถูกนำมาใช้เพื่อตรวจจับพฤติกรรมที่น่าสงสัยจากการโจมตีของ LockBit Ransomware

1.3.4 ดำเนินการประเมินผลการตรวจจับ และการตอบสนองโดยการประเมินผลนี้จะช่วยให้เห็นถึงข้อดี ข้อจำกัดของเทคนิค และเครื่องมือที่ใช้ในการตรวจจับ และตอบสนองต่อการโจมตีแรนซัมแวร์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ได้วิธีการตรวจจับ และป้องกันการโจมตีที่มีประสิทธิภาพมากขึ้น

1.4.2 เสริมสร้างความเข้าใจเกี่ยวกับพฤติกรรมของแรนซัมแวร์

1.5 เครื่องมือที่ใช้ในงานวิจัย

1.5.1 ฮาร์ดแวร์

1.5.1.1 CPU Intel Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz

1.5.1.2 Ram 32.00 GB

1.5.1.3 SSD 2 TB

1.5.2 ซอฟต์แวร์

1.5.2.1 ระบบปฏิบัติการ Windows 10 Pro 64-bit

1.5.2.2 ระบบปฏิบัติการ Windows Server 2022

1.5.2.3 ระบบปฏิบัติการ Linux Ubuntu 24.04

1.5.2.4 ระบบ pfsense firewall

1.5.2.5 ระบบ Wazuh SIEM

1.5.2.6 ไฟล์ตัวอย่างของ Lockbit Ransomware

1.5.2.7 Vmware workstation pro 17

บทที่ 2
ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในปัจจุบัน การโจมตีด้วยแรนซัมแวร์ (Ransomware) ได้กลายเป็นหนึ่งในภัยคุกคามที่รุนแรงและแพร่หลายมากที่สุดในโลกไซเบอร์ โดยเฉพาะในภาคธุรกิจ และองค์กรที่มีข้อมูลสำคัญเป็นทรัพยากรหลัก หนึ่งในสายพันธุ์ของแรนซัมแวร์ที่มีการแพร่ระบาดอย่างรวดเร็ว และสร้างความเสียหายอย่างรุนแรง คือ LockBit Ransomware [1] ซึ่งเป็นแรนซัมแวร์ที่มีความซับซ้อนสูง และมุ่งเน้นโจมตีองค์กรขนาดกลางถึงขนาดใหญ่โดยเฉพาะ LockBit Ransomware ใช้เทคนิคการเข้ารหัสไฟล์ร่วมกับการข่มขู่เรียกค่าไถ่ ส่งผลให้ข้อมูลสำคัญของเหยื่อไม่สามารถเข้าถึงได้ และต้องเผชิญกับความเสี่ยงในการสูญเสียข้อมูลถาวรหากไม่ชำระเงินตามที่ผู้โจมตีเรียกร้อง

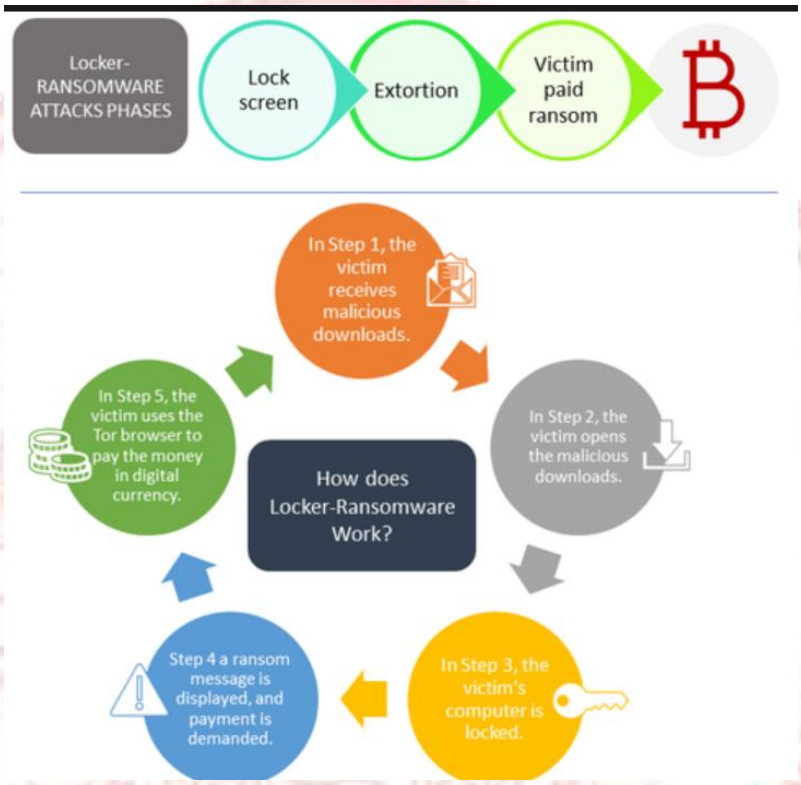
Lockbit Ransomware ยังมีคุณสมบัติเด่นในด้านการแพร่กระจายผ่านเครือข่าย และการใช้วิศวกรรมสังคม (Social Engineering) เพื่อหลอกล่อให้เหยื่อติดตั้งมัลแวร์ด้วยตนเอง งานวิจัยนี้มีจุดมุ่งหมายเพื่อศึกษารูปแบบการโจมตีของ Lockbit Ransomware และ นำเสนอวิธีการตรวจจับ และป้องกันการโจมตีดังกล่าว โดยหัวข้อที่จะกล่าวถึงมีดังนี้

2.1 แรนซัมแวร์ (Ransomware)
2.2 Lockbit Ransomware
2.3 MITRE ATT&CK
2.4 นิติวิทยาศาสตร์ดิจิทัล (Digital Forensic)
2.5 การตรวจสอบความสมบูรณ์ของไฟล์ (File Integrity Monitoring)
2.6 ระบบจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM)
2.7 งานวิจัยที่เกี่ยวข้อง

2.1 แรนซัมแวร์ (Ransomware)

แรนซัมแวร์หมายถึงมัลแวร์ประเภทหนึ่งที่ออกแบบมาเพื่อเข้ารหัสไฟล์ หรือจำกัดการเข้าถึงข้อมูลของเหยื่อ และเรียกร้องค่าไถ่เพื่อให้สามารถกู้คืนข้อมูล หรือเข้าถึงระบบได้ มักแพร่กระจายผ่านอีเมลฟิชชิ่ง, ลิงก์ที่เป็นอันตราย, หรือการโจมตีทางช่องโหว่ของซอฟต์แวร์ โดยแบ่งออกเป็น Locker Ransomware ซึ่งล็อกการเข้าถึงอุปกรณ์ และ Crypto Ransomware ซึ่งเข้ารหัสไฟล์ของเหยื่อแรนซัมแวร์ได้พัฒนาให้ซับซ้อนขึ้น ทำให้การป้องกัน และตรวจจับยากขึ้น ส่งผลให้เกิดความเสียหายต่อบุคคล และองค์กรทั่วโลก [3], [5]

2.1.1 Locker Ransomware คือมัลแวร์เรียกค่าไถ่ประเภทหนึ่งที่ล็อก หรือจำกัดการเข้าถึงอุปกรณ์ของเหยื่อ เช่น คอมพิวเตอร์ สมาร์ทโฟน หรือแท็บเล็ต เป็นต้น โดยไม่เข้ารหัสไฟล์ภายในเครื่อง แต่จะทำให้ผู้ใช้ไม่สามารถใช้งานระบบได้จนกว่าจะจ่ายค่าไถ่ มักแสดงหน้าจอแจ้งเตือนที่มีข้อความข่มขู่และวิธีการชำระ ตัวอย่างที่เคยพบ ได้แก่ WinLocker และ Police Ransomware ที่อ้างว่าเป็นหน่วยงานบังคับใช้กฎหมายเพื่อหลอกให้เหยื่อตกใจ และยอมจ่ายเงิน [3]

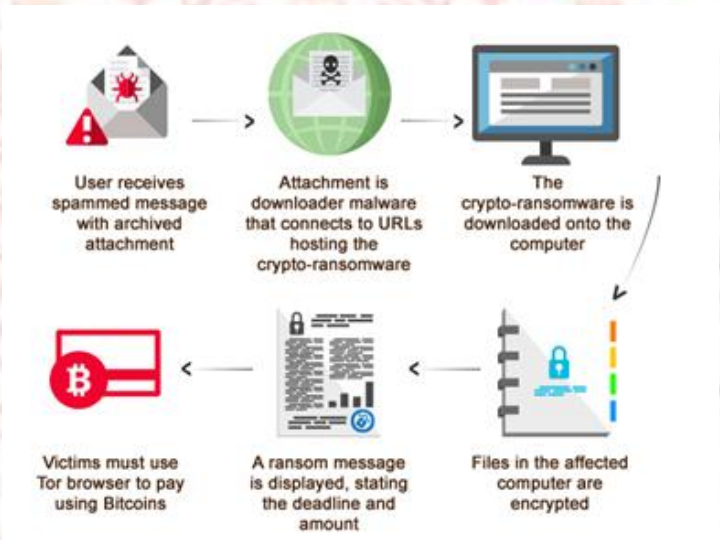


ภาพที่ 2-1 การทำงานของแรนซัมแวร์ประเภท Locker Ransomware [18]

กระบวนการทำงานของ Locker Ransomware โดยทั่วไปสามารถแบ่งออกได้เป็น 5 ขั้นตอนหลัก ดังแสดงในภาพที่ 2-1 เริ่มจากขั้นตอนแรก คือ เหยื่อได้รับไฟล์ที่เป็นอันตราย (Malicious Downloads) ซึ่งมักมาในรูปแบบของอีเมลฟิชชิ่ง (Phishing Email) หรือเว็บไซต์ที่ฝังลิงก์ดาวน์โหลดมัลแวร์ เมื่อเหยื่อเปิดไฟล์ดังกล่าว มัลแวร์จะเริ่มทำงานทันที โดยทำการล็อกระบบหรือจำกัดการเข้าถึงเครื่องคอมพิวเตอร์ของเหยื่อ ส่งผลให้ไม่สามารถใช้งานอุปกรณ์ได้ตามปกติ

ในขั้นตอนถัดมา มัลแวร์จะแสดงข้อความเรียกค่าไถ่ (Ransom Note) โดยระบุว่าเหยื่อต้องชำระเงินภายในระยะเวลาที่กำหนด มิฉะนั้นอาจไม่สามารถปลดล็อกระบบได้อีกต่อไป โดยช่องทางการชำระเงินมักกำหนดให้ดำเนินการผ่าน Tor Browser เพื่อเข้าสู่เว็บไซต์ของผู้โจมตี และชำระด้วยสกุลเงินดิจิทัล เช่น Bitcoin หรือ Cryptocurrency อื่น ๆ เป็นต้น ซึ่งเป็นวิธีที่ช่วยให้ผู้โจมตีสามารถปกปิดตัวตน และหลีกเลี่ยงการติดตามธุรกรรมได้อย่างมีประสิทธิภาพ

2.1.2 Crypto Ransomware คือมัลแวร์เรียกค่าไถ่ที่มุ่งเน้นการ เข้ารหัสไฟล์ ของเหยื่อ เช่น เอกสาร รูปภาพ วิดีโอ เป็นต้น ทำให้ไม่สามารถเปิดหรือใช้งานไฟล์เหล่านั้นได้ จากนั้นจะเรียกร้องค่าไถ่เพื่อแลกกับกุญแจถอดรหัส (decryption key) โดยอาจกำหนดระยะเวลาการจ่ายเงิน หากไม่จ่ายในเวลาที่กำหนดไฟล์อาจถูกลบ หรือเข้ารหัสถาวร ตัวอย่าง Crypto Ransomware ที่มีชื่อเสียง ได้แก่ WannaCry, Locky, CryptoLocker หรือ LockBit Ransomware ซึ่งใช้การเข้ารหัสที่ซับซ้อน เช่น AES, RSA หรือ ECC ทำให้การถอดรหัสทำได้ยาก หรือแทบเป็นไปไม่ได้หากไม่มีคีย์ เป็นต้น [4], [8]



ภาพที่ 2-2 การทำงานของแรนซัมแวร์ประเภท Crypto Ransomware [18]

กระบวนการโจมตีของ Crypto Ransomware โดยทั่วไปมีลำดับขั้นตอนที่ชัดเจน และเป็นระบบ เริ่มจากการที่เหยื่อได้รับอีเมลสแปม หรืออีเมลฟิชชิ่ง ซึ่งภายในแนบไฟล์ที่ถูกบีบอัดไว้ เช่น ไฟล์นามสกุล .zip หรือ .rar โดยซ่อนมัลแวร์ไว้ภายใน เมื่อเหยื่อหลงเชื่อ และเปิดไฟล์แนบมัลแวร์ภายในจะถูกเรียกใช้งาน เป็นต้น โดยเชื่อมต่อไปยัง URL หรือเซิร์ฟเวอร์ที่ใช้เป็นแหล่งแพร่กระจายของแรนซัมแวร์ เพื่อดาวน์โหลด และติดตั้ง Crypto Ransomware ลงในระบบของเหยื่อ

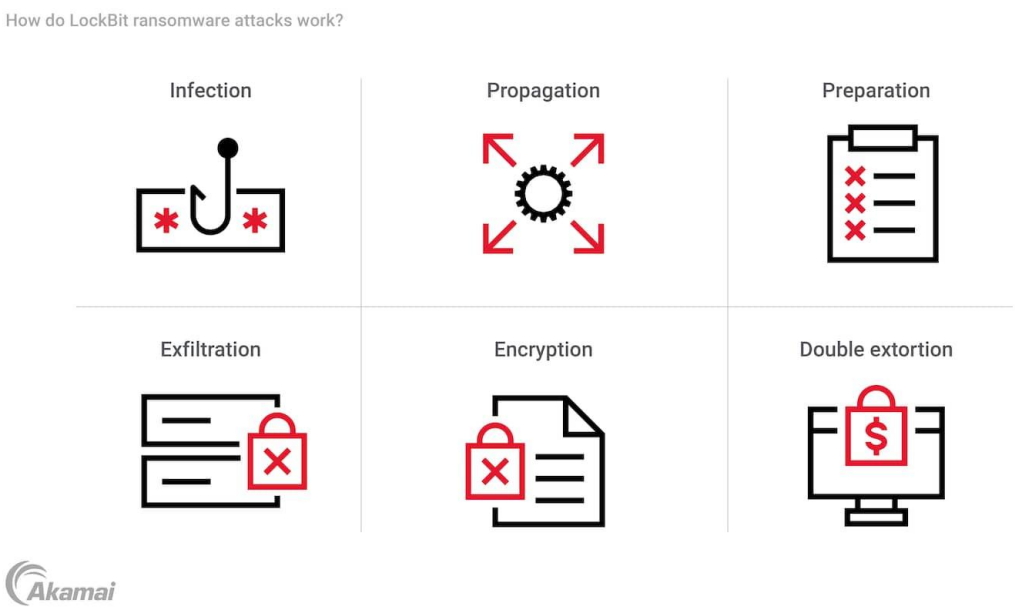
หลังจากติดตั้งเรียบร้อยแล้ว มัลแวร์จะเริ่มกระบวนการเข้ารหัสไฟล์สำคัญในคอมพิวเตอร์ของเหยื่อทันที ส่งผลให้ไฟล์ต่าง ๆ ไม่สามารถเปิดใช้งาน หรือเข้าถึงได้ กระบวนการนี้มักดำเนินการอย่างรวดเร็ว และเงียบเชียบ เพื่อหลีกเลี่ยงการตรวจจับจากโปรแกรมรักษาความปลอดภัย หลังจากเข้ารหัสเสร็จสิ้น มัลแวร์จะแสดงข้อความเรียกค่าไถ่ (Ransom Note) โดยแจ้งให้เหยื่อทราบว่าต้องชำระเงินเพื่อแลกกับการกู้คืนไฟล์ พร้อมทั้งระบุจำนวนเงิน และเวลาที่กำหนด

หากไม่ดำเนินการภายในเวลาที่กำหนด ข้อมูลอาจถูกทำลาย หรือไม่สามารถกู้คืนได้อีกต่อไปดังแสดงในภาพที่ 2-2

โดยปกติผู้โจมตีจะกำหนดให้เหยื่อติดต่อผ่านเครือข่ายที่ไม่สามารถติดตามได้ อย่าง Tor Browser และชำระเงินด้วยสกุลเงินดิจิทัล เช่น Bitcoin หรือสกุลเงินอื่นที่ไม่สามารถตรวจสอบเส้นทางธุรกรรมได้ง่าย เป็นต้น ซึ่งเป็นวิธีการที่ช่วยให้ผู้โจมตีปกปิดตัวตน และหลีกเลี่ยงการถูกติดตามจากหน่วยงานด้านความมั่นคงปลอดภัย

2.2 Lockbit Ransomware

LockBit คือแรนซัมแวร์ที่ถูกพัฒนาให้เป็น Ransomware-as-a-Service (RaaS) ซึ่งกลุ่มอาชญากรสามารถใช้เพื่อเจาะระบบ เป้าหมายหลักของ LockBit Ransomware คือองค์กรขนาดใหญ่และโครงสร้างพื้นฐานที่สำคัญ LockBit Ransomware ใช้เทคนิคที่ซับซ้อน เช่น การเข้าถึงโดยใช้บัญชีที่ถูกขโมย (Valid Accounts – T1078) การยกระดับสิทธิ์ (Privilege Escalation – T1068) และการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ (Data Encrypted for Impact – T1486) เพื่อสร้างความเสียหาย และเรียกร้องเงินจากเหยื่อ แรนซัมแวร์นี้ยังมีความสามารถในการปกปิดร่องรอย (Defense Evasion – T1027) และสามารถแพร่กระจายภายในเครือข่ายองค์กรได้อย่างรวดเร็ว เป็นต้น LockBit Ransomware ได้รับการพัฒนาอย่างต่อเนื่อง และมีการเปิดตัวเวอร์ชันใหม่ ๆ เช่น LockBit 2.0 และ LockBit 3.0 ซึ่งมีเทคนิคการโจมตีที่ซับซ้อนมากขึ้น ส่งผลให้มันกลายเป็นหนึ่งในแรนซัมแวร์ที่อันตรายที่สุดในปัจจุบัน [1], [9]

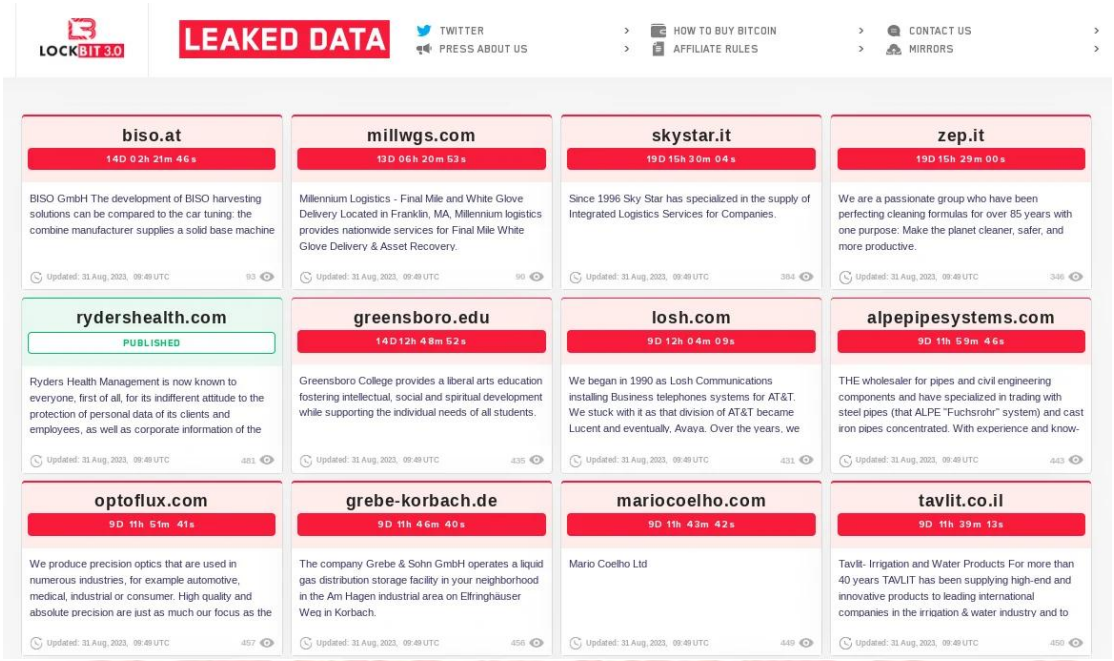


ภาพที่ 2-3 การทำงานของ Lockbit Ransomware [19]

กระบวนการโจมตีของ LockBit Ransomware (LockBit Ransomware Attack Lifecycle) สามารถแบ่งออกเป็น 6 ขั้นตอนหลัก โดยเริ่มจาก การติดเชื้อ (Infection) ซึ่งมัลแวร์จะเข้าสู่ระบบเป้าหมายโดยอาศัยเทคนิคต่าง ๆ เช่น การส่งอีเมลฟิชชิง (Phishing), การเจาะช่องโหว่ของระบบ (Exploiting Vulnerabilities) หรือการใช้ข้อมูลล็อกอินที่รั่วไหล (Leaked Credentials) เพื่อให้สามารถเข้าถึงระบบโดยไม่ได้รับอนุญาต เมื่อมัลแวร์สามารถแทรกซึมเข้าสู่ระบบได้แล้ว จะเข้าสู่ขั้นตอนถัดไปคือ การแพร่กระจาย (Propagation) ซึ่ง LockBit Ransomware จะดำเนินการเคลื่อนย้ายภายในระบบเครือข่าย (Lateral Movement) โดยใช้โปรโตคอลที่พบได้ทั่วไป เช่น Remote Desktop Protocol (RDP) และ Server Message Block (SMB) เป็นต้น เพื่อกระจายตัวไปยังอุปกรณ์อื่นในเครือข่ายเดียวกัน

หลังจากนั้นจะเข้าสู่ขั้นตอนที่สามคือ การเตรียมการ (Preparation) ซึ่ง LockBit Ransomware จะทำลายกลไกการป้องกันของระบบ โดยการปิดการทำงานของโปรแกรมแอนติไวรัส (Antivirus Software), หยุดการทำงานของบริการระบบ (System Services) และลบข้อมูลสำรอง (Shadow Copies) เพื่อป้องกันไม่ให้เหยื่อสามารถกู้คืนข้อมูลได้ จากนั้นมัลแวร์จะดำเนินการในขั้นตอนการขโมยข้อมูล (Exfiltration) โดยจะลักลอบขโมยข้อมูลสำคัญ (Sensitive Data) และส่งออกไปยังเซิร์ฟเวอร์ของผู้โจมตี (Attacker’s Server) เพื่อใช้ในการกดดันเหยื่อหากไม่ยอมจ่ายค่าไถ่ ดังแสดงในภาพที่ 2-3

ในขั้นตอนที่ห้าคือ การเข้ารหัสไฟล์ (Encryption) LockBit Ransomware จะเข้ารหัสไฟล์ทั้งหมดบนอุปกรณ์ของเหยื่อ (Encrypt Victim’s Files) พร้อมทั้งเปลี่ยนนามสกุลไฟล์ให้เป็นรูปแบบเฉพาะของ LockBit Ransomware ซึ่งทำให้ไฟล์ไม่สามารถเปิด หรือเข้าถึงได้อีก สุดท้ายคือขั้นตอนการขู่กรรโชกสองชั้น (Double Extortion) ซึ่งผู้โจมตีนอกจากจะเรียกค่าไถ่เพื่อแลกกับกุญแจถอดรหัสแล้ว ยังข่มขู่ว่าจะเปิดเผยข้อมูลที่ถูกขโมย (Data Leak) ต่อสาธารณชน หากเหยื่อไม่ยอมชำระเงินตามที่ร้องขอ กลยุทธ์นี้ช่วยเพิ่มแรงกดดัน และโอกาสที่เหยื่อจะยอมจ่ายค่าไถ่มากยิ่งขึ้น ดังแสดงในภาพที่ 2-4

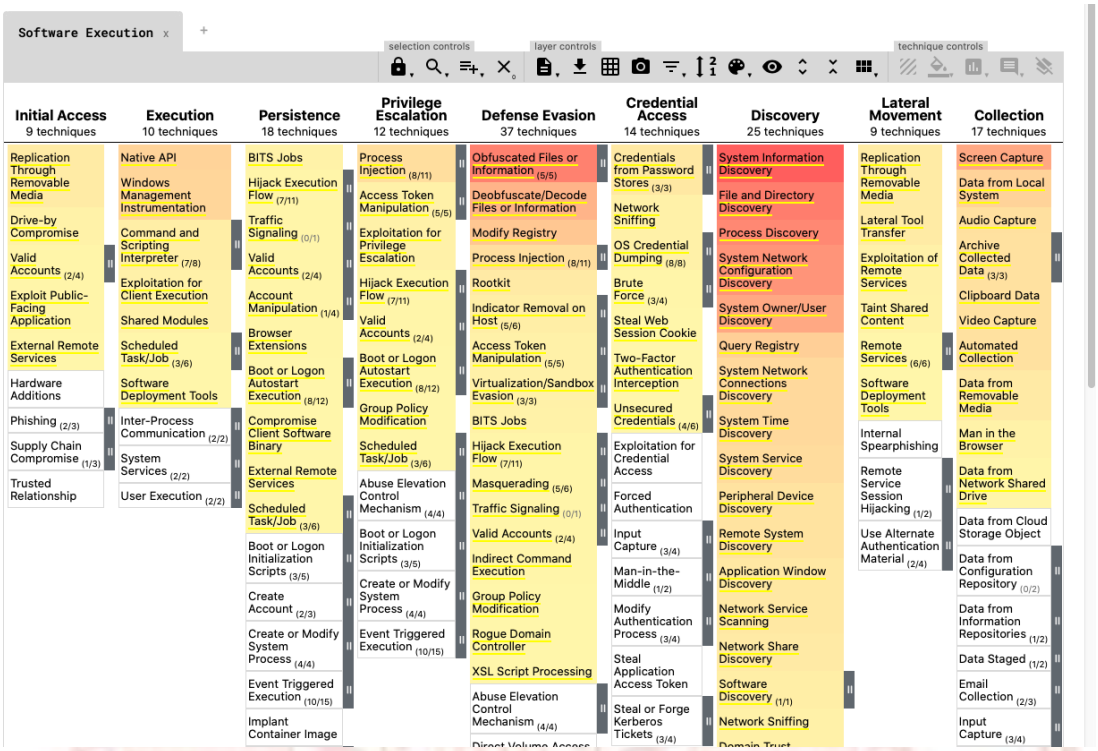


ภาพที่ 2-4 ข้อมูลจาก LockBit 3.0 Leak Site ซึ่งเป็นเว็บไซต์ของกลุ่มแรนซัมแวร์ที่ใช้เปิดเผยข้อมูลของเหยื่อ [19]

2.3 MITRE ATT&CK

MITRE ATT&CK หรือชื่อเต็มว่า Adversarial Tactics, Techniques, and Common Knowledge เป็นกรอบแนวคิดที่ถูกพัฒนาขึ้นโดยองค์กร MITRE Corporation เพื่อใช้ในการทำความเข้าใจและวิเคราะห์รูปแบบพฤติกรรมของผู้โจมตีในโลกไซเบอร์ โดยเน้นไปที่การอธิบายขั้นตอนต่าง ๆ ของการโจมตีตั้งแต่ช่วงที่เริ่มพยายามเข้าถึงระบบ จนถึงการควบคุม หรือทำลายข้อมูลที่อยู่ในระบบเป้าหมาย กรอบแนวคิดนี้ไม่เพียงแต่ช่วยให้นักวิเคราะห์สามารถระบุลักษณะของการโจมตีได้ดีขึ้นเท่านั้น แต่ยังสามารถนำไปประยุกต์ใช้เพื่อวางแนวทางในการป้องกัน ตรวจจับ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพอีกด้วยดังแสดงในภาพที่ 2-5 [9]

ความโดดเด่นของ MITRE ATT&CK คือการจัดแบ่งหมวดหมู่ของการโจมตีตามแพลตฟอร์มเป้าหมาย ซึ่งช่วยให้องค์กรสามารถเลือกใช้ข้อมูลให้ตรงกับสภาพแวดล้อมของตนเอง ปัจจุบัน ATT&CK Framework แบ่งออกเป็น 3 กลุ่มหลัก ได้แก่ Enterprise ATT&CK ที่ใช้สำหรับระบบ Windows, macOS, Linux, รวมถึงระบบ Cloud และ SaaS, Mobile ATT&CK สำหรับอุปกรณ์เคลื่อนที่ เช่น Android และ iOS ที่มีลักษณะเฉพาะของพฤติกรรมมัลแวร์บนอุปกรณ์พกพา และ ICS ATT&CK สำหรับระบบควบคุมอุตสาหกรรม (Industrial Control Systems) เช่น SCADA หรือ PLC เป็นต้น ซึ่งมักเป็นเป้าหมายของการโจมตีที่มุ่งเน้นสร้างความเสียหายต่อโครงสร้างพื้นฐานของประเทศ



ภาพที่ 2-5 MITRE ATT&CK Matrix แสดง Tactics (กลยุทธ์) และ Techniques (เทคนิค) ที่แฮกเกอร์ใช้ในกระบวนการโจมตีทางไซเบอร์ [20]

2.4 นิติวิทยาศาสตร์ดิจิทัล (Digital Forensic)

นิติวิทยาศาสตร์ดิจิทัล (Digital Forensic) คือ กระบวนการรวบรวม วิเคราะห์ และเก็บรักษาหลักฐานดิจิทัล ที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบต่อระบบคอมพิวเตอร์ และเครือข่าย จุดประสงค์หลักคือ การตรวจสอบ และระบุหลักฐานที่เชื่อถือได้ เพื่อนำไปใช้ในการวิเคราะห์เหตุการณ์ การกู้คืนข้อมูล หรือการสนับสนุนทางกฎหมาย [1], [3]

กระบวนการ Digital Forensic มีขั้นตอนหลัก 4 ขั้นตอนดังแสดงในภาพที่ 2-6 ได้แก่

2.4.1 การระบุข้อมูลหลักฐาน (Identification)

หลักฐานดิจิทัลเป็นสิ่งจำเป็นต่อการวิเคราะห์เหตุการณ์ หรือใช้เป็นข้อมูลเสนอในกระบวนการพิจารณาของศาล โดยข้อมูลหลักฐานที่จะนำมาใช้งานได้นั้น ต้องสามารถระบุแหล่งที่มาของข้อมูลหลักฐานได้ว่าข้อมูลดังกล่าวนั้นมาจากที่ใด มาจากประเภทอุปกรณ์ใด และใช้วิธีการอย่างไรในการได้มาซึ่งข้อมูลหลักฐานดังกล่าว ซึ่งนำไปเชื่อมโยงกับหลักฐานอื่น ๆ หรือบุคคลที่เกี่ยวข้องได้ ดังนั้นหลักฐานที่เก็บได้นั้นจะต้องมีการระบุที่มา และวิธีการได้มาของหลักฐานอย่างชัดเจนเพื่อให้สามารถตรวจสอบความถูกต้องได้

2.4.2 การรวบรวมข้อมูล (Collection)

หลักฐานดิจิทัลที่เกิดขึ้นต้องมีการพิจารณาว่าจะรวบรวมข้อมูลอย่างไร และมีปัจจัยใด ๆ ที่มีผลต่อการตัดสินใจอะไรบ้าง เช่น การเก็บข้อมูลหลักฐานทันทีเมื่อไฟดับเพราะข้อมูลหลักฐานเหล่านั้นจะหายไป เป็นต้น เพราะข้อมูลหลักฐานบางอย่างนั้นเป็นข้อมูลในหน่วยความจำชั่วคราว (RAM) ที่กำลังทำงานอยู่ ซึ่งเรียกว่าหลักฐานที่สูญสลายได้ (Volatile evidence) โดยเก็บจากข้อมูลที่สูญสลายได้เร็วที่สุดก่อน จากนั้น เก็บข้อมูลที่ยังคงมีอยู่ได้แม้ไม่มีไฟเลี้ยง เช่น ฮาร์ดไดรฟ์ เป็นต้น ซึ่งเรียกว่าหลักฐานที่ไม่สูญสลาย (Non-Volatile evidence)

2.4.3 การได้มาซึ่งข้อมูล (Acquisition)

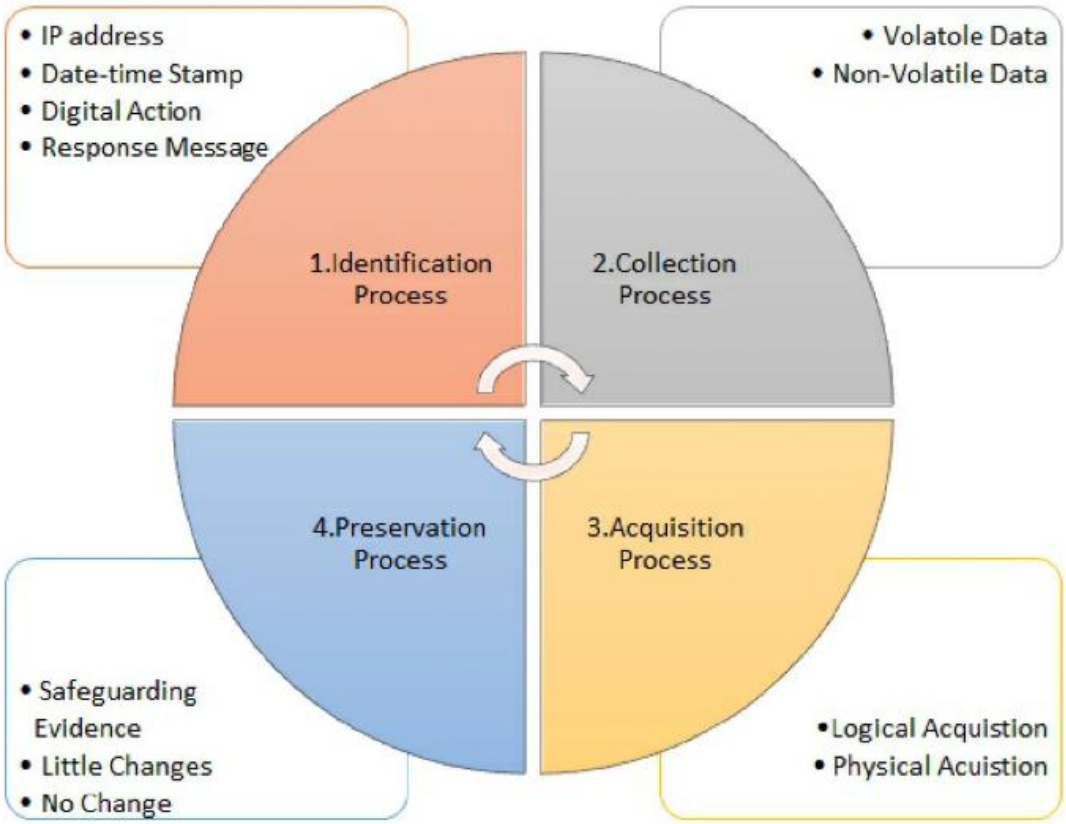
กระบวนการได้มาซึ่งหลักฐานต้นฉบับ (Original source evidence) ทั้งทางหลักฐานทางกายภาพ (Physical) และหลักฐานทางตรรกะ (Logical) ต้องมีการป้องกันหลักฐานดิจิทัลจากการถูกลบ ถูกเปลี่ยนแปลง แก้ไข โดยเมื่อได้หลักฐานต้นฉบับมาแล้วจะเก็บไว้ โดยไม่ให้มีการเข้าไปแตะต้องกับหลักฐานต้นฉบับ หากมีการขอหลักฐานไปใช้งาน จะทำการส่งสำเนาของหลักฐานต้นฉบับ (Digital evidence copy) ไปให้กับผู้ร้องขอ (เก็บหลักฐานต้นฉบับไว้ ไม่ให้มีการเปลี่ยนแปลง หรือแก้ไขได้) และต้องมีการบันทึกห่วงโซ่การครอบครองวัตถุพยาน (Chain of custody) ว่าหลักฐานมีการถูกเข้าถึงโดยใคร เมื่อไหร่ อย่างไร ด้วยเหตุผลอะไร

ในการสืบสวนทางกระบวนการพิสูจน์หลักฐานดิจิทัล การได้มาซึ่งข้อมูลอาจเป็นขั้นตอนที่สำคัญที่สุด และเกี่ยวข้องกับลำดับเหตุการณ์ ข้อมูล และหลักฐานที่ได้มาต้องมีรายละเอียดที่ครบถ้วนถูกต้อง ซึ่งต้องดำเนินด้วยวิธีการ กระบวน เครื่องมือ ข้อกำหนดของซอฟต์แวร์ และฮาร์ดแวร์ทั้งหมด รวมถึงสื่อคอมพิวเตอร์ ที่มีมาตรฐาน และเป็นที่ยอมรับไม่ขัดต่อข้อกำหนด และกฎหมายใด ๆ สำหรับการได้มาซึ่งหลักฐานดิจิทัล

2.4.4 ความสมบูรณ์ของข้อมูลหลักฐาน (Preservation)

ในการสอบสวน หรือการดำเนินคดี ข้อมูลหลักฐานถือเป็นองค์ประกอบที่มีความสำคัญอย่างยิ่ง เนื่องจากมีผลโดยตรงต่อความถูกต้อง และความน่าเชื่อถือของเหตุการณ์ หรือคดีนั้น ๆ ดังนั้นจึงจำเป็นต้องมีการปกป้องข้อมูลหลักฐานอย่างเหมาะสม ซึ่งรวมถึงการสำรองข้อมูล การจัดเก็บอย่างเป็นระบบ และการตรวจสอบความถูกต้อง เพื่อให้มั่นใจว่าข้อมูลหลักฐานยังคงความสมบูรณ์ ไม่ถูกแก้ไข ดัดแปลง หรือถูกปลอมแปลงในทุกกรณี

กระบวนการในการรวบรวม และจัดเก็บข้อมูลหลักฐานดิจิทัลจึงต้องดำเนินการด้วยความระมัดระวัง ภายใต้มาตรฐาน และขั้นตอนที่ได้รับการรับรอง ทั้งในด้านวิธีการ เครื่องมือที่ใช้ และบุคลากรผู้ดำเนินงาน เพื่อให้สามารถนำข้อมูลไปใช้ประกอบการดำเนินคดีได้อย่างมีประสิทธิภาพ อีกทั้งยังต้องสอดคล้องกับข้อกำหนดทางกฎหมายของประเทศนั้น ๆ ด้วย เพราะหากมีข้อบกพร่องในขั้นตอนดังกล่าว อาจส่งผลให้พยานหลักฐานขาดความน่าเชื่อถือ และไม่สามารถนำไปใช้เอาผิดผู้กระทำผิดได้อย่างถูกต้องตามกระบวนการยุติธรรม



ภาพที่ 2-6 กระบวนการ Digital Forensic [3]

2.5 การตรวจสอบความสมบูรณ์ของไฟล์ (File Integrity Monitoring)

การตรวจสอบความสมบูรณ์ของไฟล์ (File Integrity Monitoring หรือ FIM) คือกระบวนการในการเฝ้าระวัง และตรวจสอบความถูกต้องของไฟล์ในระบบ โดยเน้นการตรวจจับการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต เช่น การถูกแก้ไข ลบ หรือสร้างใหม่ โดยเฉพาะในระบบไฟล์ที่มีความสำคัญ เช่น ระบบปฏิบัติการ ฐานข้อมูล แอปพลิเคชัน และอุปกรณ์เครือข่าย เป็นต้น [10]

การทำงานของ FIM มักใช้เทคนิค การสร้างค่าฐาน (Baseline) ด้วยอัลกอริธึมการแฮช เช่น SHA-256 หรือ SHA-512 เพื่อเก็บสถานะของไฟล์ และเปรียบเทียบกับสถานะปัจจุบันทุกครั้งที่มีการตรวจสอบ หากพบความแตกต่างจะสามารถบ่งชี้ได้ว่าเกิดเหตุการณ์ที่อาจเกี่ยวข้องกับการบุกรุกหรือมัลแวร์

งานวิจัยของ Jukuntla และคณะ [10] ได้แสดงให้เห็นว่า การใช้สคริปต์ PowerShell ร่วมกับแนวคิด Hash Line และ Baseline สามารถเพิ่มความแม่นยำ และความยืดหยุ่นของระบบ FIM ได้ โดยสามารถตรวจจับการสร้าง (Created), การแก้ไข (Modified), และการลบ (Deleted) ไฟล์ได้แบบ Real-time พร้อมทั้งเสนอให้ใช้พื้นที่จัดเก็บที่มีความปลอดภัย เช่น OneDrive Vault เพื่อปกป้องค่าแฮชจากผู้ไม่หวังดี [10], [11]

2.6 ระบบจัดการข้อมูล และเหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM)

เป็นระบบที่ถูกออกแบบมาเพื่อช่วยในการ ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ในแบบเรียลไทม์อย่างอัตโนมัติ โดยทำหน้าที่รวบรวมข้อมูลจากแหล่งต่าง ๆ ภายในระบบสารสนเทศขององค์กร ไม่ว่าจะเป็น firewall, ระบบตรวจจับ และป้องกันการบุกรุก (IDS/IPS), โปรแกรมป้องกันไวรัส, ระบบรักษาความปลอดภัยของเครื่องลูกข่าย (endpoint security), บันทึกเหตุการณ์ของเซิร์ฟเวอร์ (server logs), ข้อมูลการรับส่งข้อมูลในเครือข่าย (network traffic logs) ตลอดจนข้อมูลจากอุปกรณ์รักษาความปลอดภัยประเภทอื่น ๆ SIEM ทำงานโดยใช้ 2 กระบวนการหลัก

2.6.2 การจัดการข้อมูลด้านความมั่นคงปลอดภัย (SIM Security Information Management)

การจัดการข้อมูลด้านความมั่นคงปลอดภัย (SIM) คือระบบ หรือกระบวนการที่เน้นการรวบรวม จัดเก็บ และวิเคราะห์ข้อมูลบันทึกเหตุการณ์ (Logs) จากแหล่งข้อมูลต่าง ๆ ภายในระบบเทคโนโลยีสารสนเทศ เช่น เซิร์ฟเวอร์ อุปกรณ์เครือข่าย เป็นต้น ระบบฐานข้อมูล หรืออุปกรณ์รักษาความปลอดภัย โดยข้อมูลเหล่านี้จะถูกนำมา วิเคราะห์ย้อนหลัง เพื่อระบุแนวโน้ม พฤติกรรม หรือรูปแบบของภัยคุกคามที่อาจเกิดขึ้นในอดีต

2.6.2 การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (SEM Security Event Management)

การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (SEM) คือระบบ หรือกระบวนการที่มุ่งเน้นการวิเคราะห์ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยแบบเรียลไทม์ (Real-time Analysis) โดยจะทำหน้าที่ตรวจจับกิจกรรมที่ผิดปกติ หรือเข้าข่ายเป็นภัยคุกคามจากข้อมูลที่ได้รับจากอุปกรณ์ความปลอดภัยต่าง ๆ เช่น Firewall, IDS/IPS, Endpoint Security และระบบอื่น ๆ ที่เชื่อมโยงอยู่ในเครือข่าย เป็นต้น

2.7 งานวิจัยที่เกี่ยวข้อง

งานวิจัยในด้านการตรวจจับและวิเคราะห์แรนซัมแวร์ได้มีการพัฒนาอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา โดยมีการประยุกต์ใช้ทั้งกรอบแนวคิด MITRE ATT&CK ระบบ SIEM (Security Information and Event Management) และเครื่องมือตรวจสอบความสมบูรณ์ของไฟล์ (File Integrity Monitoring: FIM) เพื่อวิเคราะห์พฤติกรรมของมัลแวร์อย่างเป็นระบบ Suk-on และคณะ [1] ศึกษาการโจมตีของ LockBit Ransomware บนระบบ Operational Technology (OT) โดยใช้ Joe Sandbox และ MITRE ATT&CK Framework เพื่อวิเคราะห์ลำดับขั้นตอนการโจมตี พบว่า LockBit สามารถใช้เทคนิค T1078, T1068 และ T1486 เพื่อฝังตัวและเข้ารหัสข้อมูลได้อย่างรวดเร็ว นอกจากนี้ Jukuntla และคณะ [10] ได้เสนอแนวทางพัฒนา FIM โดยใช้ PowerShell Script ผสานกับ Hash Line และ Baseline ร่วมกับ OneDrive Vault เพื่อป้องกันการแก้ไขไฟล์โดยไม่ได้รับอนุญาต ขณะที่ Suhendi และคณะ [11] ประยุกต์ใช้ Honeypot ร่วมกับ Wazuh SIEM เพื่อตรวจจับการสแกนพอร์ตและ brute-force attack ได้แบบ Real-time และสามารถเชื่อมโยงพฤติกรรมเข้ากับ ATT&CK Framework ได้อย่างครอบคลุม ในด้านของพฤติกรรมการพรางตัวของมัลแวร์ งานของ Lee และคณะ [4] นำเสนอแนวคิด “Hiding in the Crowd” โดย LockBit และ REvil ใช้ไฟล์ปลอม (Link File) และฝัง script ผ่าน explorer.exe เพื่อหลีกเลี่ยงการตรวจจับจาก SIEM และ EDR ส่วน Chen & Lin [7] ได้ศึกษาการแพร่เชื้อผ่าน Social Engineering และ RDP

ที่ไม่มีการเข้ารหัส ซึ่งนำไปสู่การปิด system restore และลบ event logs โดยอัตโนมัติ ภายหลังจากการติดตั้งมัลแวร์ ขณะที่ Sharma และคณะ [9] มุ่งเน้นไปที่การวิเคราะห์ Targeted Ransomware และเสนอให้ตรวจจับผ่าน Privilege Escalation เช่น “Special privileges assigned to new logon” และ “Command started by abnormal process” ที่สามารถระบุพฤติกรรมรุนแรงหลังล็อกอินระบบได้อย่างแม่นยำ อีกด้านหนึ่ง Verma & Tiwari [6] ได้นำเสนอพฤติกรรมของแรนซัมแวร์ระดับ Process และ I/O โดยพบว่า LockBit มักเรียกใช้ API เช่น CryptEncrypt, DeleteFile, WriteFile ผ่านโปรเซส powershell.exe, cmd.exe และ notepad.exe ซึ่งสะท้อนถึงกลไกการทำงานที่เจาะลึกไปถึงระดับระบบปฏิบัติการ

งานวิจัยของผู้วิจัยมีความสอดคล้องกับงานที่ผ่านมาหลายด้าน โดยได้จำลองสภาพแวดล้อมจริงบน Windows Server 2022 และ Windows 10 เพื่อศึกษาพฤติกรรมของ LockBit Ransomware โดยใช้เครื่องมือ Redline, Any.Run และ Wazuh ในการตรวจจับแบบ Real-time ซึ่งสามารถระบุเหตุการณ์ในกลุ่ม Execution, Discovery, Privilege Escalation, Impact และ Defense Evasion ได้อย่างแม่นยำ ข้อมูลที่ได้มีความลึกกว่าการตรวจจับด้วย Antivirus ทั่วไป และสามารถนำไปต่อยอดเป็น Dataset สำหรับพัฒนา Machine Learning Model ในอนาคต เพื่อเพิ่มความแม่นยำและลด False Positive โดยภาพรวมงานวิจัยนี้ผสมผสานการทดลองเชิงนิติวิทยาศาสตร์การใช้เครื่องมือจริง และการเชื่อมโยงพฤติกรรมกับ MITRE ATT&CK Framework ซึ่งแม้ยังไม่ได้ใช้เทคนิค AI/ML โดยตรง แต่ก็สามารถวิเคราะห์และรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ และสามารถนำไปพัฒนาต่อยอดเป็นระบบตอบสนองอัตโนมัติได้ในอนาคต

บทที่ 3
วิธีการดำเนินงาน

ในบทนี้จะกล่าวถึงขั้นตอนการดำเนินการวิจัยต่าง ๆ เพื่อให้การวิจัยดำเนินไปได้มีประสิทธิภาพและลุล่วง ผู้วิจัยจึงวางแผนขั้นตอนการวิจัยดังนี้

3.1 ออกแบบขั้นตอนการวิจัย

3.2 ดำเนินการวิจัย

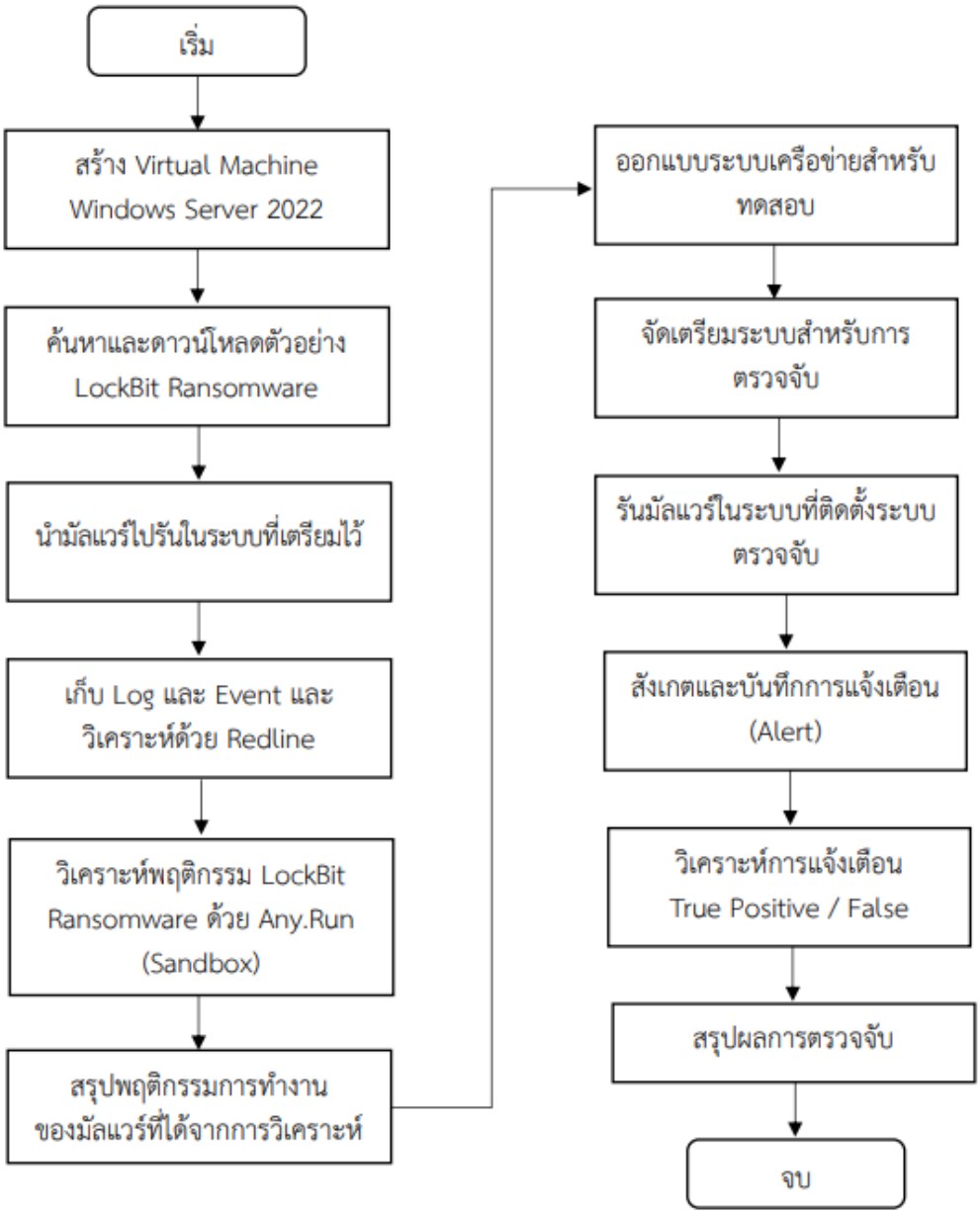
3.3 สรุปขั้นตอนการดำเนินการวิจัย

3.1 ออกแบบขั้นตอนการวิจัย

การวิจัยนี้จะแบ่งเป็นสองส่วนด้วยกันคือการวิเคราะห์ทางนิติวิทยาศาสตร์ และตรวจจับ ผู้วิจัยเริ่มต้นจากการออกแบบวิธีการวิเคราะห์ก่อนเป็นอันดับแรก เพื่อต้องการนาข้อมูลที่ได้จากการวิเคราะห์มัลแวร์ Lockbit Ransomware มาการรวบรวมข้อมูลเพื่อทำการการตรวจจับการทำงานของมัลแวร์ Lockbit Ransomware

ในส่วนแรกคือการวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) เพื่อวิเคราะห์พฤติกรรมการทำงานของมัลแวร์ LockBit Ransomware โดยขั้นแรกคือการจัดเตรียมสภาพแวดล้อมเพื่อทำการทดสอบมัลแวร์ เตรียมตัวอย่างมัลแวร์ โดยค้นหา และ ดาวน์โหลดตัวอย่างมัลแวร์จากแหล่งที่เชื่อถือได้ เมื่อได้ตัวอย่างมัลแวร์มาแล้วก็จะดำเนินการนำไฟล์มัลแวร์ไปวิเคราะห์ด้วย Sandbox เพื่อเก็บข้อมูลการทำงานในระดับเบื้องต้น โดยเน้นเก็บข้อมูลพฤติกรรม (Behavioral data) และ Indicator of Compromise (IOC) และ ทำการเปิดใช้งานมัลแวร์บนระบบปฏิบัติการที่ได้จัดเตรียมไว้ และนำข้อมูลพฤติกรรมการทำงานของมัลแวร์ไปทำการวิเคราะห์ด้วยเครื่องมือ Redline เพื่อทำการวิเคราะห์พฤติกรรมการทำงานของมัลแวร์เพื่อสรุปผล

ส่วนที่สองคือการนำผลจากการรวิเคราะห์พฤติกรรมการทำงานของมัลแวร์ นำมาประกอบกับการทดสอบระบบการตรวจจับจับมัลแวร์ (Malware Detection) โดยขั้นแรกคือการจัดเตรียมสภาพแวดล้อมทดสอบเพื่อทำการทดสอบตรวจจับมัลแวร์โดยการนำมัลแวร์ที่ทำการวิเคราะห์พฤติกรรมในส่วนแรกมาทำการรันบนสภาพแวดล้อมที่จัดเตรียมไว้เพื่อทดสอบว่าระบบตรวจจับที่จำลองขึ้นมานั้น สามารถตรวจจับมัลแวร์ตามกระบวนการทำงานที่ได้วิเคราะห์มา หรือไม่ และบันทึกผลการทดสอบ และนำไปสรุปผลเพื่อการปรับปรุง และพัฒนาระบบต่อไป ดังภาพที่ 3-1



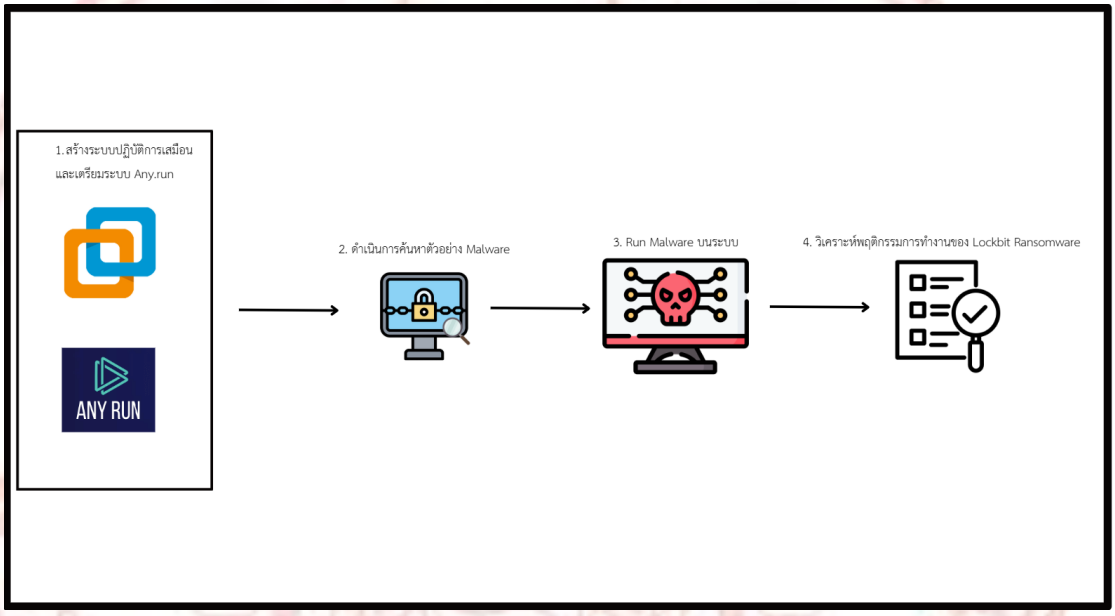
ภาพที่ 3-1 กระบวนการวิจัย

3.2 ดำเนินการวิจัย

ในส่วนของขั้นตอนการวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) ผู้วิจัยได้มีการจำลองสภาพแวดล้อมในการทดสอบมัลแวร์เพื่อวิเคราะห์การทำงานของ Lockbit Ransomware ในอันดับแรกโดยการ สร้างระบบปฏิบัติการเสมือน หรือ Virtual Machines ด้วยระบบปฏิบัติ

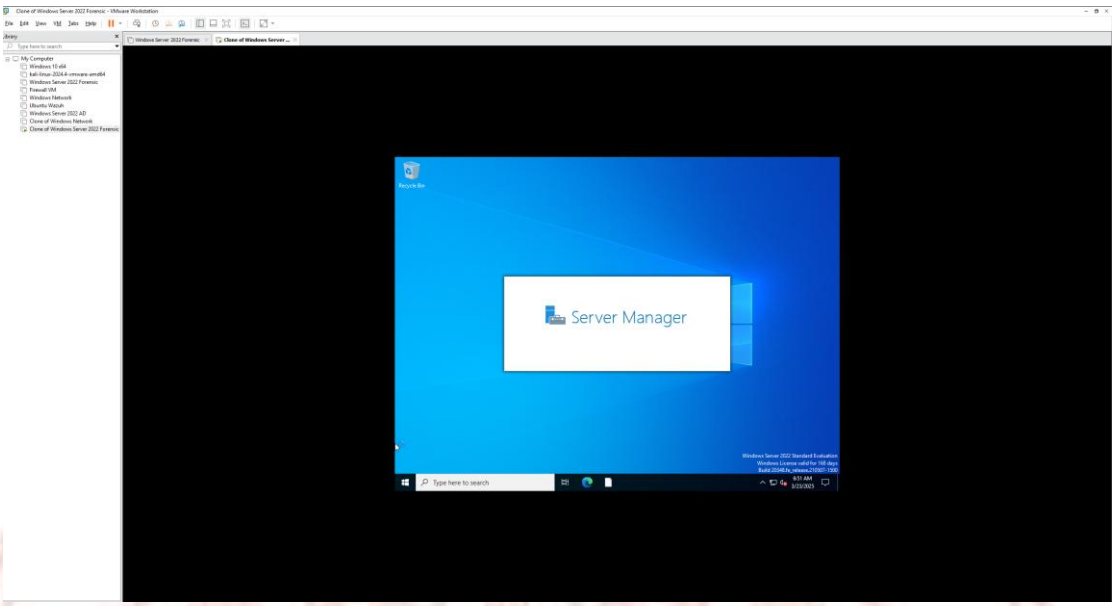
windows server 2022 ที่ได้ทำการลง Sysmon และได้ใช้เครื่องมืออย่าง Redline [4] เพื่อทำการวิเคราะห์และใช้ Sandbox [1] ร่วมวิเคราะห์ด้วย โดยมีขั้นตอน ดังภาพที่ 3-2

1. สร้างระบบปฏิบัติการเสมือน
2. ดำเนินการค้นหาตัวอย่างมัลแวร์
3. เตรียม Sanbox any.run
4. รันมัลแวร์บนระบบเสมือน
5. รันมัลแวร์บน any.run Sanbox
6. วิเคราะห์พฤติกรรมการทำงานของ Lockbit Ransomware



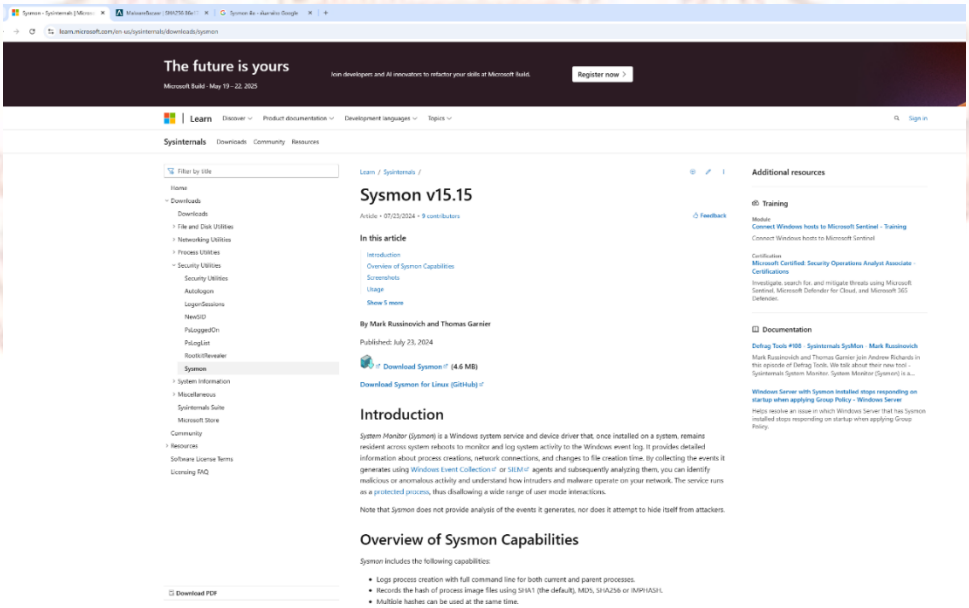
ภาพที่ 3-2 ขั้นตอนการเตรียมการ และวิเคราะห์พฤติกรรมการทำงานของ Lockbit Ransomware

ผู้วิจัยได้มีการจำลองสภาพแวดล้อมในการทดสอบมัลแวร์ โดยใช้โปรแกรม Vmware Workstation Pro มาช่วยสร้างระบบปฏิบัติการเสมือน เนื่องจาก Vmware Workstation Pro มีฟังก์ชันที่หลากหลาย รวมถึงรองรับ ระบบปฏิบัติการได้หลายแพลตฟอร์ม ในส่วนนี้ผู้วิจัยได้เลือกใช้ระบบปฏิบัติ windows server 2022 ในการจำลองสภาพแวดล้อมในการทดสอบมัลแวร์ ใช้เครื่องมือ Redline ในการวิเคราะห์มัลแวร์ ตามภาพที่ 3-3

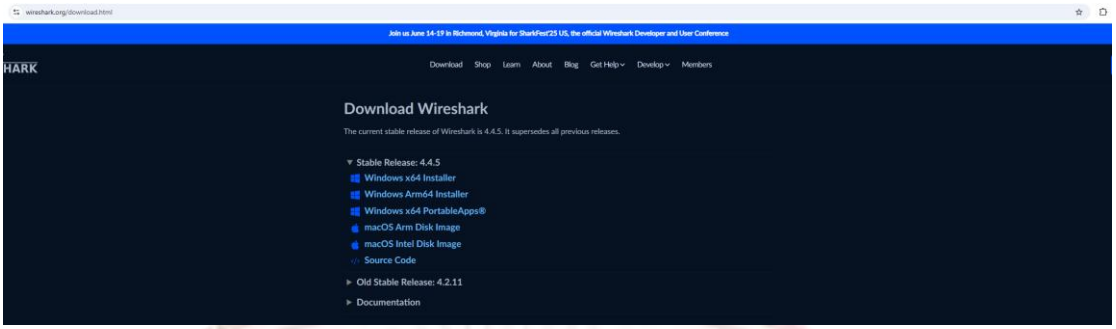


ภาพที่ 3-3 ระบบปฏิบัติ windows server 2022 ใน Vmware Workstation Pro

ต่อมาผู้วิจัยได้ทำการติดตั้งเครื่องมือ Sysmon และ wireshark เพิ่มเติมเพื่อต้องการดูพฤติกรรมการทำงานของ Lockbit Ransomware ในขณะทำการรันไฟล์มัลแวร์ ตามภาพที่ 3-4 และ 3-5

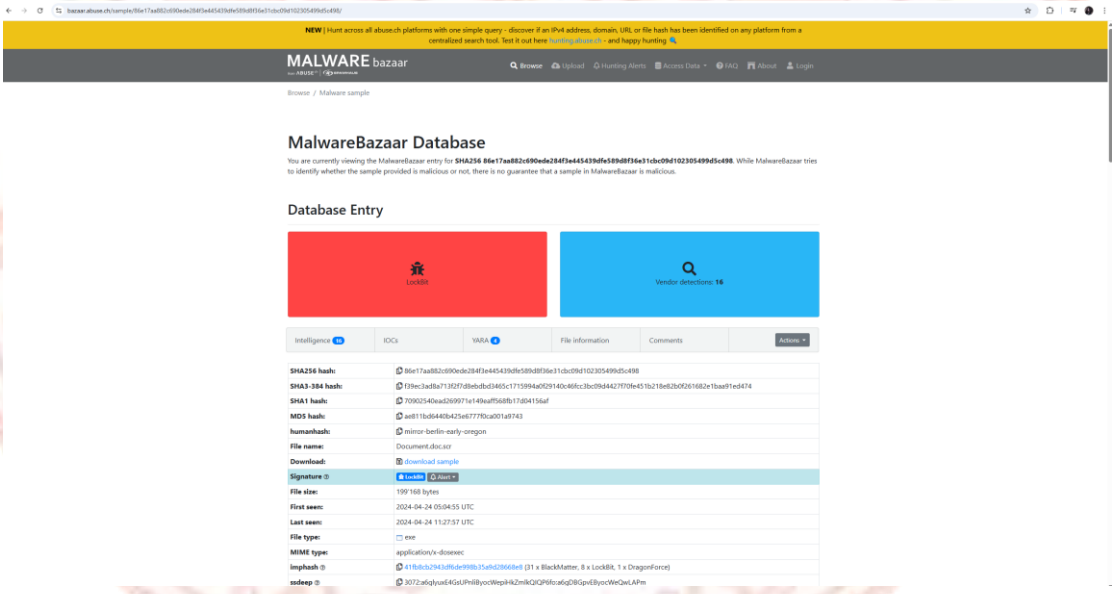


ภาพที่ 3-4 หน้าเว็บไซต์ Microsoft Learn สำหรับดาวน์โหลดเครื่องมือ Sysmon



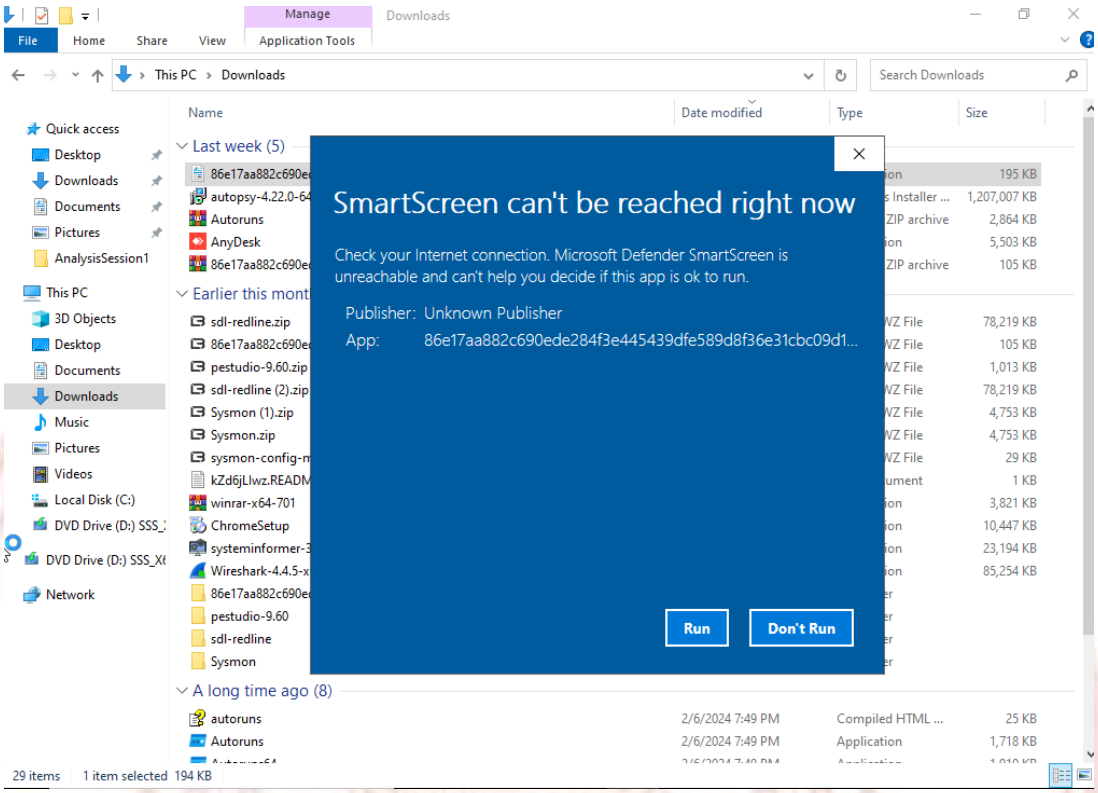
ภาพที่ 3-5 หน้าเว็บไซต์ทางการของ Wireshark แสดงหน้าดาวน์โหลดโปรแกรมเพื่อใช้งานด้านการดักจับและวิเคราะห์ข้อมูลเครือข่าย

ต่อมาผู้วิจัยได้ทำการจัดหาตัวอย่างมัลแวร์ที่เว็บไซต์ https://bazaar.abuse.ch แล้วเลือกใช้มัลแวร์ที่มีชื่อไฟล์ 86e17aa882c690ede284f3e445439dfe589d8f36e31cbc09d102305499d5c498.exe ในการทดสอบครั้งนี้ตามภาพ 3-6 และ ทำการทดสอบมัลแวร์บนระบบตามภาพ3-7 และ 3-8

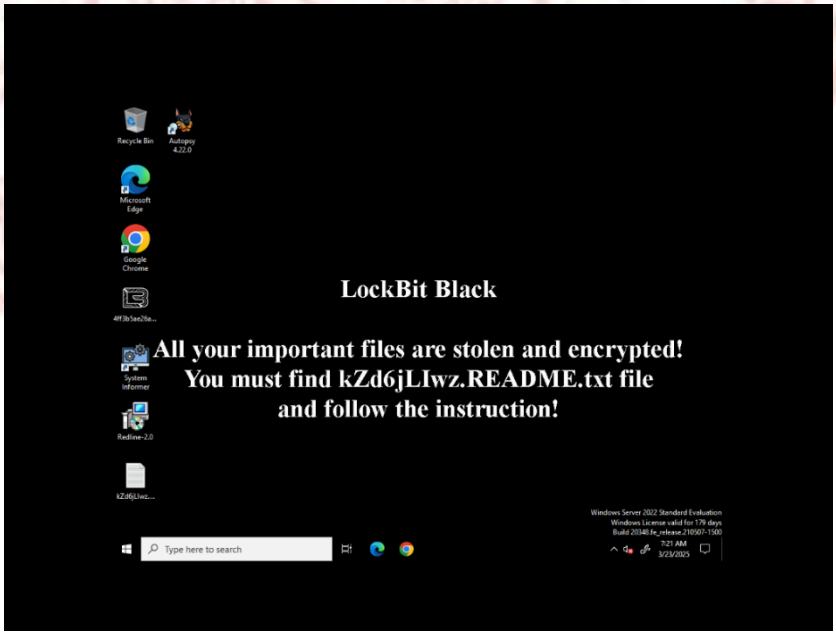


ภาพที่ 3-6 หน้าเว็บไซต์ MalwareBazaar แสดงตัวอย่างข้อมูลมัลแวร์ LockBit จากฐานข้อมูล

เมื่อได้ไฟล์มัลแวร์มาแล้วก็ทำการรันไฟล์บนระบบปฏิบัติการ

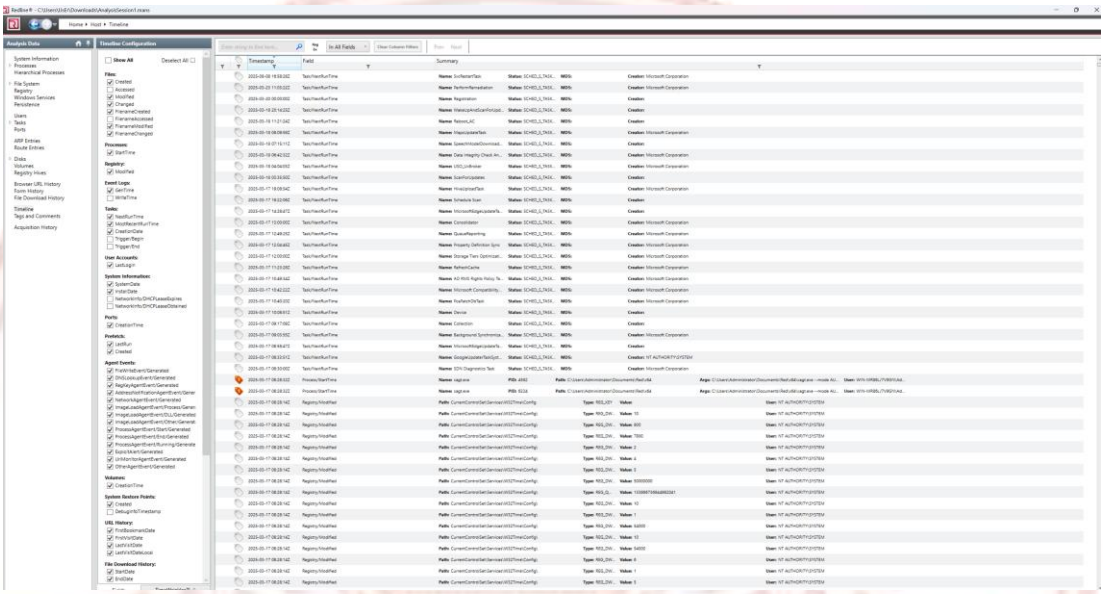


ภาพที่ 3-7 การรันไฟล์มัลแวร์บนระบบปฏิบัติการ

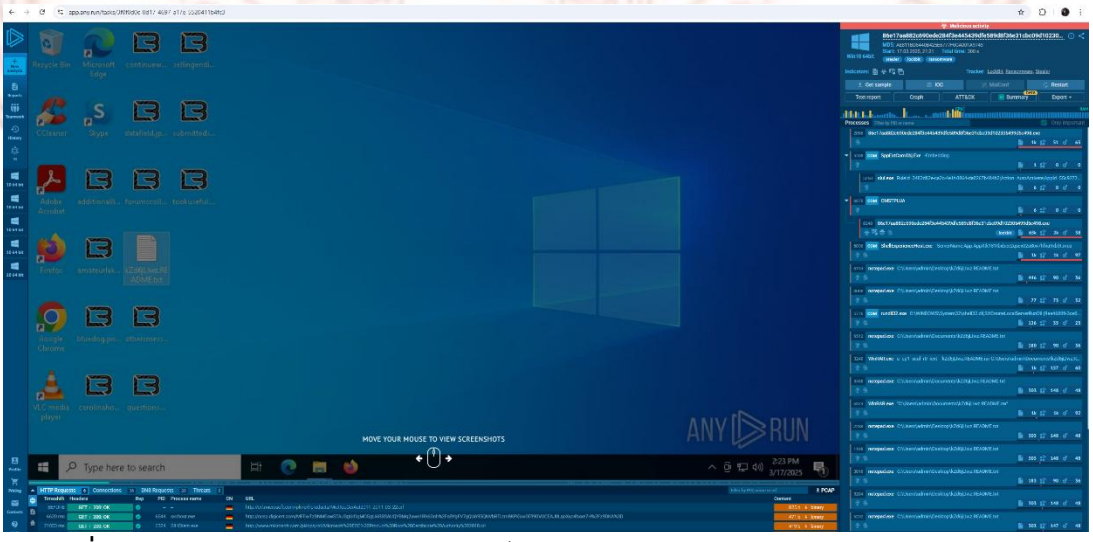


ภาพที่ 3-8 ระบบปฏิบัติการติด Lockbit Ransomware

เมื่อระบบปฏิบัติการติด Lockbit Ransomware แล้ว ผู้วิจัยได้ดำเนินการติดตั้ง ใช้งานเครื่องมือ Redline และ any.run ในการวิเคราะห์มัลแวร์ตามภาพที่ 3-9 และ 3-10

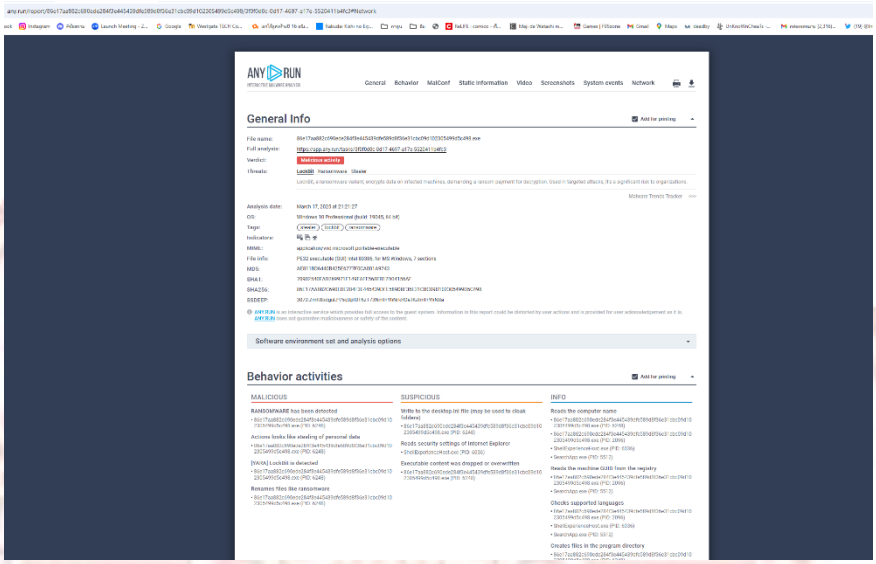


ภาพที่ 3-9 ข้อมูลที่ได้จากระบบปฏิบัติการที่ติด Lockbit Ransomware นำมาวิเคราะห์บนเครื่องมือ Redline



ภาพที่ 3-10 แสดงรายละเอียดการวิเคราะห์ไฟล์ตัวอย่างมัลแวร์ LockBit ผ่านระบบ Any.Run Sandbox พร้อมข้อมูลพฤติกรรมในระบบปฏิบัติการ

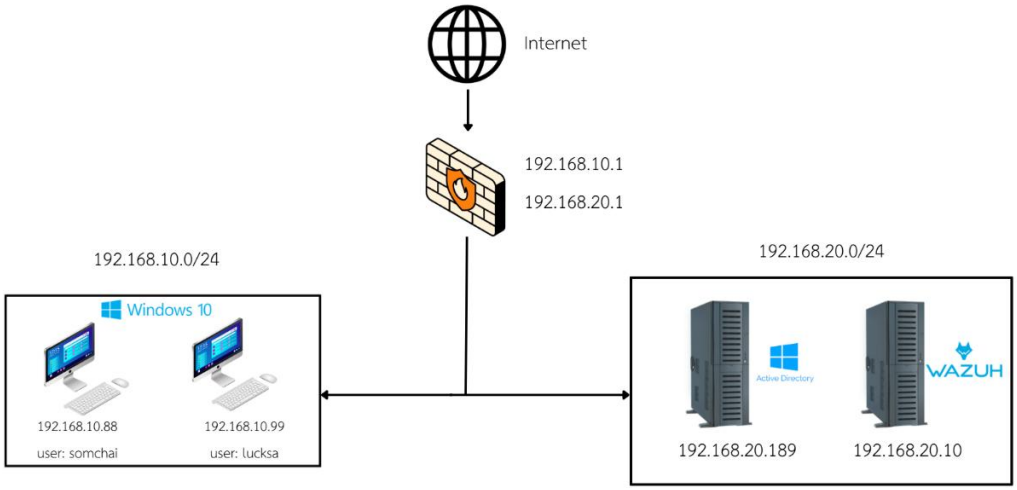
ในขั้นสุดท้ายในส่วนของการวิเคราะห์พฤติกรรมการทำงานของมัลแวร์ต้องทำผลที่ได้จากการวิเคราะห์ทางนิติวิทยาศาสตร์ มาทำการสรุปผล เพื่อนำข้อมูลมาประกอบในส่วนของการตรวจจับต่อไปตามภาพที่ 3-11



ภาพที่ 3-11 ข้อมูลรายงานผลการทดสอบจาก any.run

ในส่วนของขั้นตอนการทดสอบระบบตรวจจับมัลแวร์ (Malware Detection) หลังจากที่ได้ผลการวิเคราะห์พฤติกรรมมัลแวร์ในส่วนแรกแล้ว ผู้วิจัยนำข้อมูลที่ได้นั้นไปใช้ในการออกแบบการทดสอบระบบตรวจจับมัลแวร์มาทำการทดสอบโดยรันมัลแวร์บนสภาพแวดล้อมที่เตรียมไว้ โดยสร้างระบบปฏิบัติการเสมือน หรือ Virtual Machines เพื่อจำลองสภาพแวดล้อมเครือข่ายโดยประกอบด้วย Firewall pfsense ระบบ Wazuh ที่มีฟังก์ชันการตรวจจับ ตอบสนองแบบขยาย (XDR) และ การจัดการข้อมูล และเหตุการณ์ด้านความปลอดภัย (SIEM) ระบบปฏิบัติการ Windows Server 2022 จำนวน 1 เครื่องทำหน้าที่เป็น Active Directory (AD) และ ระบบปฏิบัติการ Windows 11 ทั้งหมดจำนวน 2 เครื่อง โดยมีขั้นตอน ดังนี้

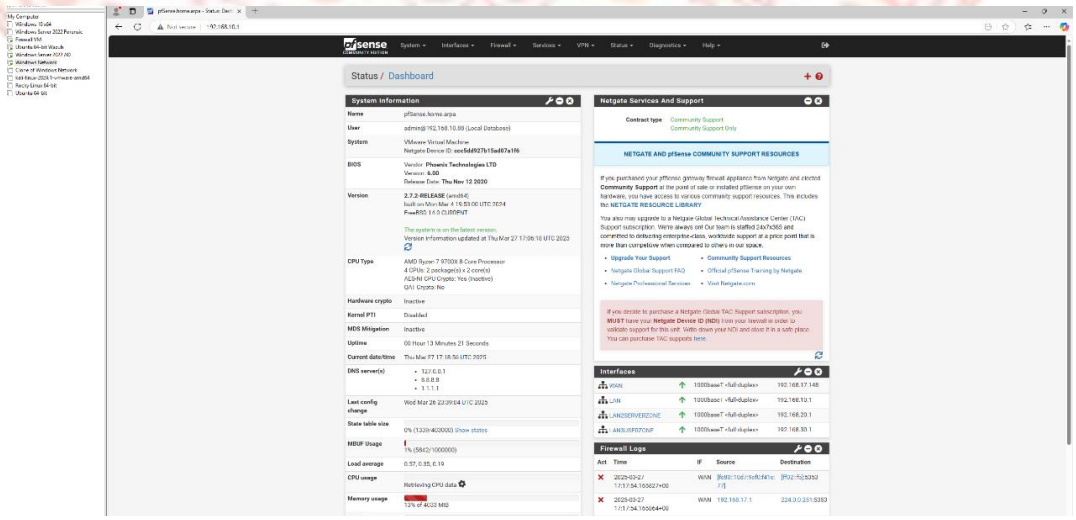
1. ออกแบบระบบเครือข่าย
2. สร้างระบบปฏิบัติการเสมือน
3. ทดสอบระบบตรวจจับมัลแวร์
4. รันมัลแวร์บนระบบเครือข่ายเสมือน
5. สรุปผลการทดสอบ



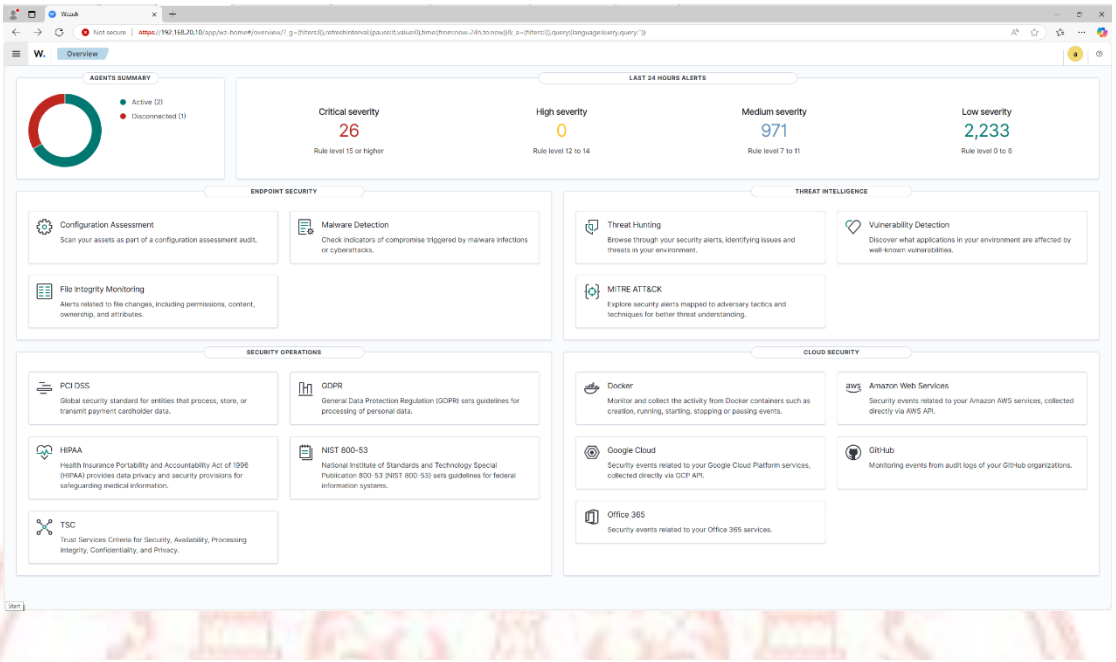
ภาพที่ 3-12 แผนภาพของสถาปัตยกรรมเครือข่าย

ผู้วิจัยได้มีการออกแบบเพื่อจำลองสภาพแวดล้อมเครือข่ายโดยมีแผนผังภาพของสถาปัตยกรรมเครือข่าย โดยมีรายระเอียดดังรูปภาพ 3-12

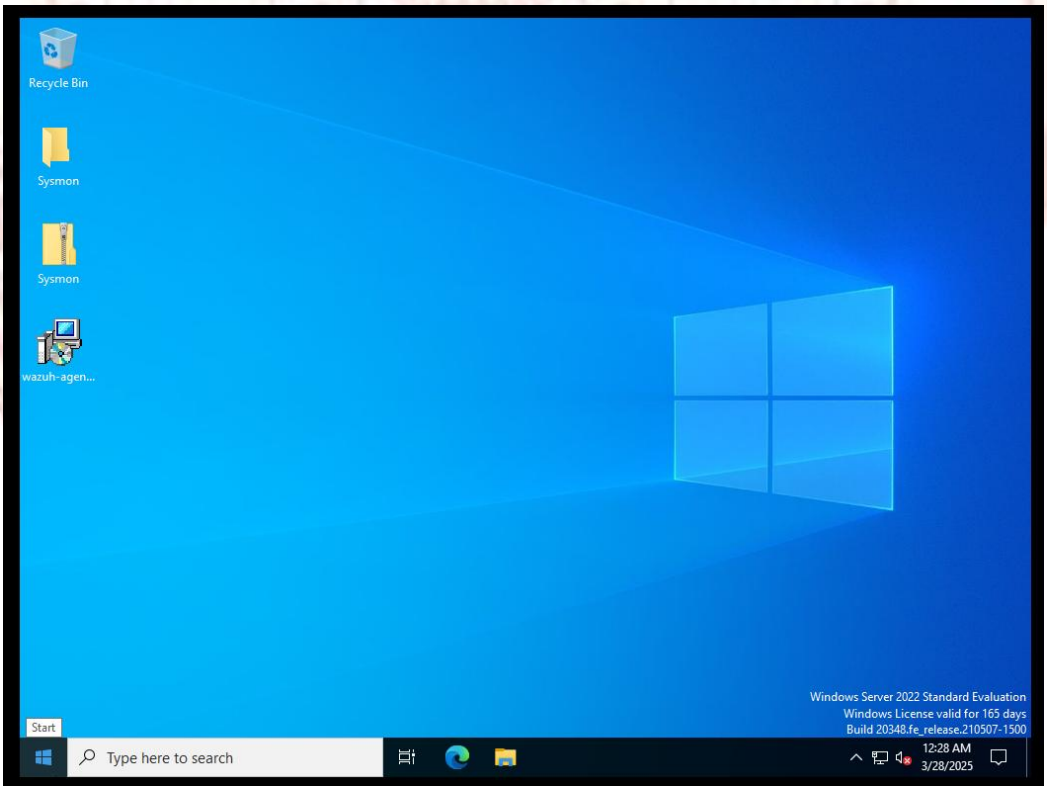
ผู้วิจัยได้มีการจำลองสภาพแวดล้อมเครือข่ายในการทดสอบมัลแวร์ โดยใช้โปรแกรม Vmware Workstation Pro มาช่วยสร้างระบบปฏิบัติการเสมือน เนื่องจาก Vmware Workstation Pro มีฟังก์ชันที่หลากหลาย รวมถึงรองรับ ระบบปฏิบัติการได้หลายแพลตฟอร์ม ในส่วนนี้ผู้วิจัยได้เลือกใช้ Firewall pfsense ระบบ Wazuh ที่มีฟังก์ชันการตรวจจับ และตอบสนองแบบขยาย (XDR) และการจัดการข้อมูล และเหตุการณ์ด้านความปลอดภัย (SIEM) ระบบปฏิบัติการ Windows Server 2022 จำนวน 1 เครื่อง ทำหน้าที่เป็น Active Directory (AD) และ ระบบปฏิบัติการ Windows 11 ทั้งหมด จำนวน 2 เครื่อง ตามภาพที่ 3-13 - 3-16



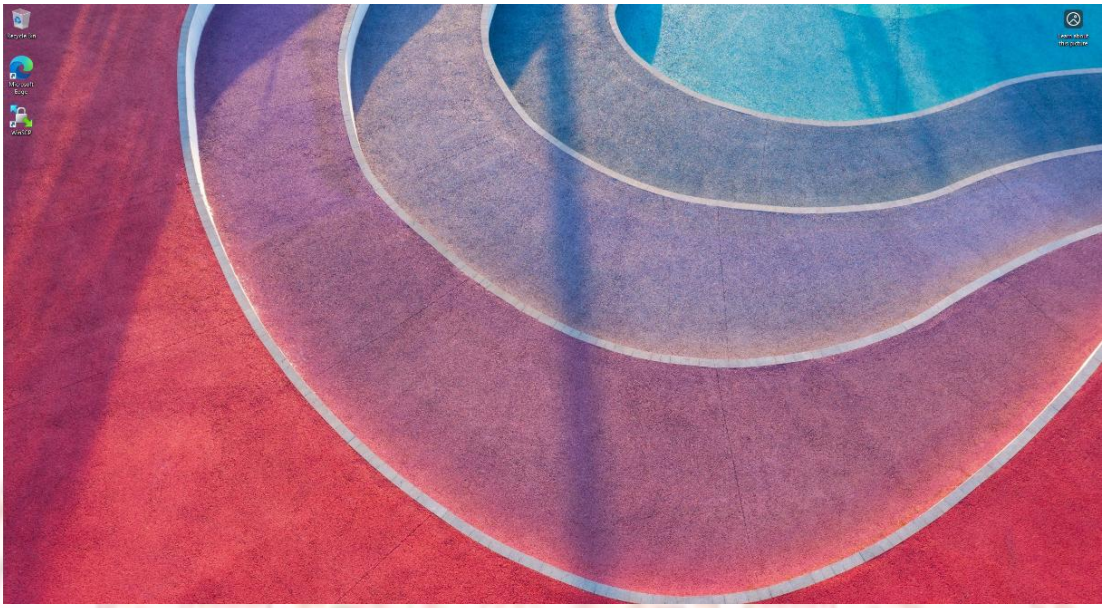
ภาพที่ 3-13 Firewall pfsense ใน Vmware Workstation Pro



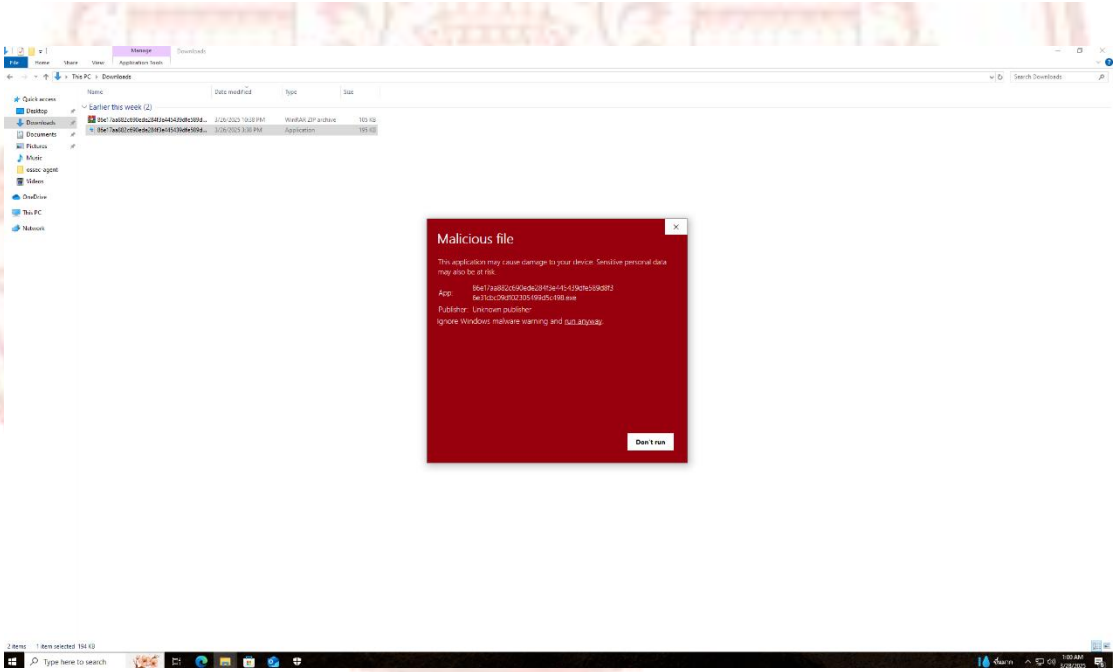
ภาพที่ 3-14 ระบบ Wazuh ใน Vmware Workstation Pro



ภาพที่ 3-15 Windows Server 2022 Active Directory (AD) ใน Vmware Workstation Pro

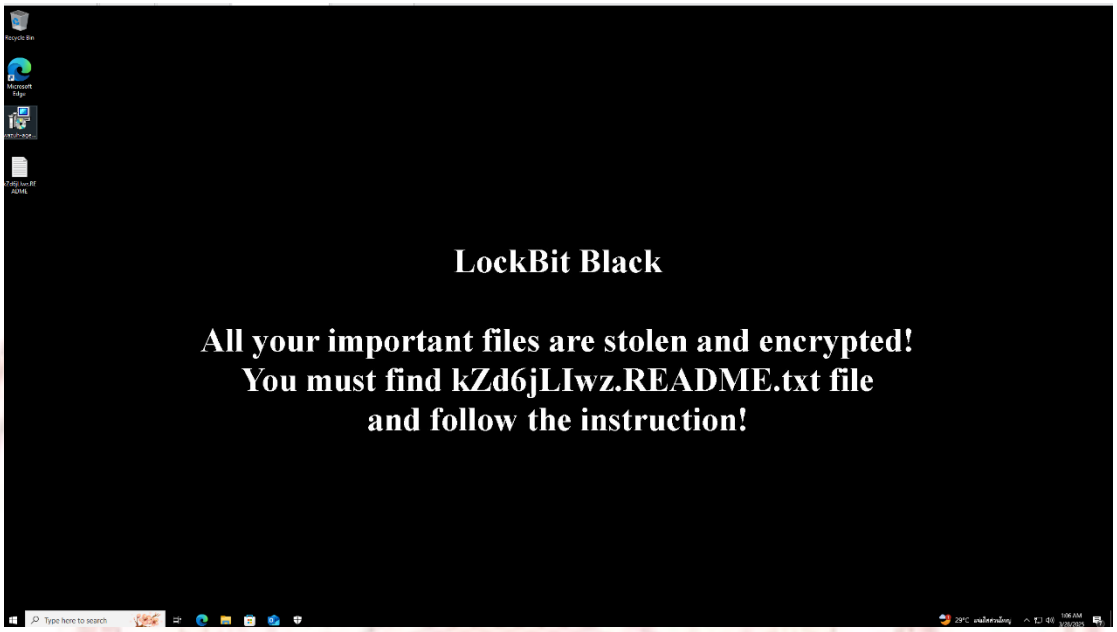


ภาพที่ 3-16 Windows 11 ใน Vmware Workstation Pro



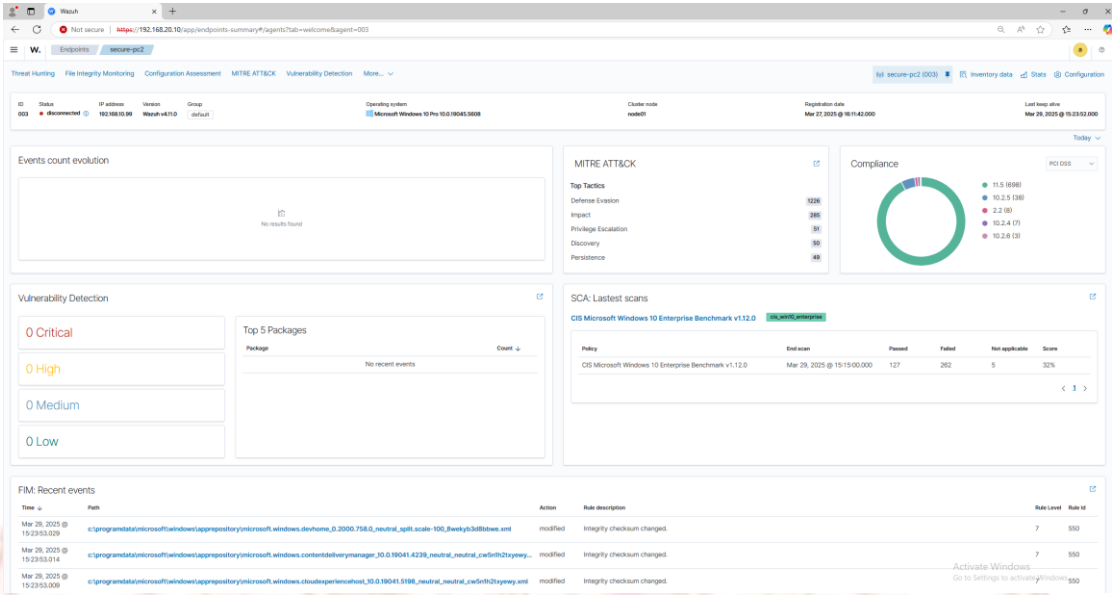
ภาพที่ 3-17 รันมัลแวร์ไฟล์บนระบบปฏิบัติการ บนระบบเครือข่ายเสมือน

ต่อมาผู้วิจัยได้ทำการนำไฟล์มัลแวร์ที่ได้ทำการวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) มาทดสอบรันบนสภาพแวดล้อมเครือข่ายที่ได้สร้างไว้ โดยรันมัลแวร์บนเครื่องระบบปฏิบัติการ Windows 11 IP Address: 192.168.10.99 ตามภาพที่ 3-17 และ 3-18



ภาพที่ 3-18 เครื่องระบบปฏิบัติการ Windows 11 IP Address: 192.168.10.99 ติดมัลแวร์รันมัลแวร์ไฟล์บนระบบปฏิบัติการ บนระบบเครือข่ายเสมือน

ในส่วนสุดท้ายทำการวิเคราะข้อมูลจาก Wazuh ที่สามารถตรวจจับระหว่างรันไฟล์ และ ดำเนินการสรุปผลการตรวจจับในบทที่ 4



ภาพที่ 3-19 ระบบ Wazuh ที่สามารถตรวจจับภัยคุกคามได้

3.3 สรุปขั้นตอนการดำเนินการวิจัย

ในการดำเนินงานวิจัยครั้งนี้ ผู้วิจัยแบ่งกระบวนการออกเป็นสองส่วนหลัก ได้แก่ การวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) และการตรวจจับมัลแวร์ (Malware Detection) โดยเริ่มจากการจำลองสภาพแวดล้อมด้วยเครื่องเสมือน (Virtual Machine) บนระบบปฏิบัติการ Windows Server 2022 เพื่อใช้ในการทดลองมัลแวร์ LockBit Ransomware ซึ่งได้จากแหล่งที่มาที่เชื่อถือได้ จากนั้นทำการวิเคราะห์เบื้องต้นด้วย Sandbox (Any.Run) เพื่อสังเกตพฤติกรรมของมัลแวร์ และรวบรวมข้อมูลเบื้องต้น เช่น Indicator of Compromise (IOC) พร้อมติดตั้งเครื่องมือสนับสนุนการวิเคราะห์ เช่น Sysmon และ Wireshark แล้วรันมัลแวร์ในสภาพแวดล้อมควบคุม และทำการวิเคราะห์เชิงลึกด้วยเครื่องมือ Redline เพื่อศึกษาพฤติกรรมที่เกิดขึ้นภายในระบบ เช่น การเข้ารหัสไฟล์ การลบ Shadow Copy และการเปลี่ยนแปลงรีจิสทรี เป็นต้น จากนั้นจึงนำข้อมูลพฤติกรรมที่ได้มาใช้ในการจำลองระบบตรวจจับ โดยสร้างระบบเครือข่ายเสมือนที่ประกอบด้วย pfSense Firewall, Wazuh SIEM/XDR, Windows Server และ Windows 11 เพื่อทำการทดสอบการตรวจจับ โดยรันมัลแวร์ในเครื่องเป้าหมาย และวิเคราะห์เหตุการณ์ผ่านระบบ Wazuh เพื่อประเมินประสิทธิภาพในการแจ้งเตือน และตรวจจับพฤติกรรมที่สอดคล้องกับการวิเคราะห์ก่อนหน้า พร้อมทั้งสรุปผลการตรวจจับ และแนวทางการพัฒนาเพิ่มเติม

บทที่ 4
ผลการวิจัย

จากการดำเนินงานการทดสอบการวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์ (Event Logs), เครื่องมือวิเคราะห์มัลแวร์ Any.Run และ Redline รวมถึงการจำลองสภาพแวดล้อมภายในระบบปฏิบัติการ Windows เพื่อสังเกตพฤติกรรมของมัลแวร์ พบหลักฐานสำคัญในเชิงปริมาณ และคุณภาพที่สามารถสรุปได้ดังนี้

4.1 ผลการวิเคราะห์ทางนิติวิทยาศาสตร์ด้วย Redline

การรันไฟล์มัลแวร์ LockBit Ransomware บน Windows Server 2022 และ วิเคราะห์ด้วย Redline พบว่า

4.1.1 มีไฟล์ถูกเข้ารหัสทั้งหมด 697 ไฟล์

4.1.2 มีการสร้างไฟล์ Ransom Note จำนวน 518 รายการ

4.1.3 พบการลบ บริการ Volume Shadow Copy (VSS) และไม่สามารถกู้คืนไฟล์จาก Previous Versions ได้

4.1.4 Event Logs ถูกลบ

4.1.5 Registry มีการเปลี่ยนแปลงจำนวนมากในเวลาที่ใกล้เคียงกับการรันมัลแวร์

4.2 ผลการจำลองพฤติกรรมมัลแวร์ด้วย Any.Run

ผลการวิเคราะห์บน Windows 10 ผ่านแพลตฟอร์ม Any.Run พบว่า

4.2.1 มี Process ใหม่ 166 รายการ โดย 28 รายการ เกี่ยวข้องกับมัลแวร์

4.2.2 ตรวจจับ Malicious Process ได้ 2 รายการ

4.2.3 พฤติกรรมสำคัญที่พบ ได้แก่:

4.2.1.1 เปิด Notepad พร้อมข้อความเรียกค่าไถ่

4.2.1.2 เข้ารหัสไฟล์ .doc, .jpg, .json, .txt

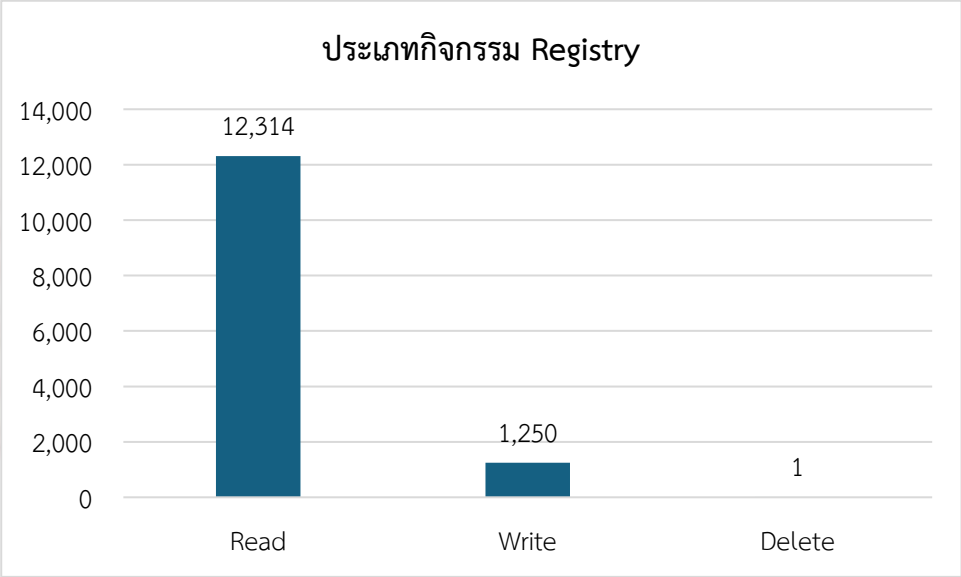
4.2.1.3 ลบ Shadow Copy ด้วย vssadmin delete shadows

4.2.4 กิจกรรมบน Registry ที่พบบน Any.Run

จากการวิเคราะห์ด้วยเครื่องมือ Any.Run พบว่าหลังการรันมัลแวร์ LockBit Ransomware มีการดำเนินกิจกรรมบน Registry จำนวนมาก โดยมีการอ่านค่า (Read) ถึง 12,314 รายการ เขียน หรือแก้ไขค่า (Write) จำนวน 1,250 รายการ และลบค่า (Delete) จำนวน 1 รายการ ซึ่งแสดงให้เห็นถึงความพยายามของมัลแวร์ในการตรวจสอบข้อมูลภายในระบบ และปรับแต่งค่าคอนฟิกบางอย่างเพื่อใช้ในการเข้ารหัสไฟล์ หรือฝังตัวในระบบอย่างแนบเนียน กิจกรรมเหล่านี้ถือเป็นหนึ่งในพฤติกรรมสำคัญที่สามารถใช้เป็นหลักฐานในการวิเคราะห์ทางนิติวิทยาศาสตร์ได้อย่างชัดเจน

ตารางที่ 4-1 ผลกิจกรรมบน Registry ที่พบบน Any.Run

ประเภทกิจกรรม Registry	จำนวนเหตุการณ์ที่ตรวจพบ
Read	12,314 รายการ
Write	1,250 รายการ
Delete	1 รายการ



ภาพที่ 4-1 สรุปผลกิจกรรมบน Registry ที่พบบน Any.Run

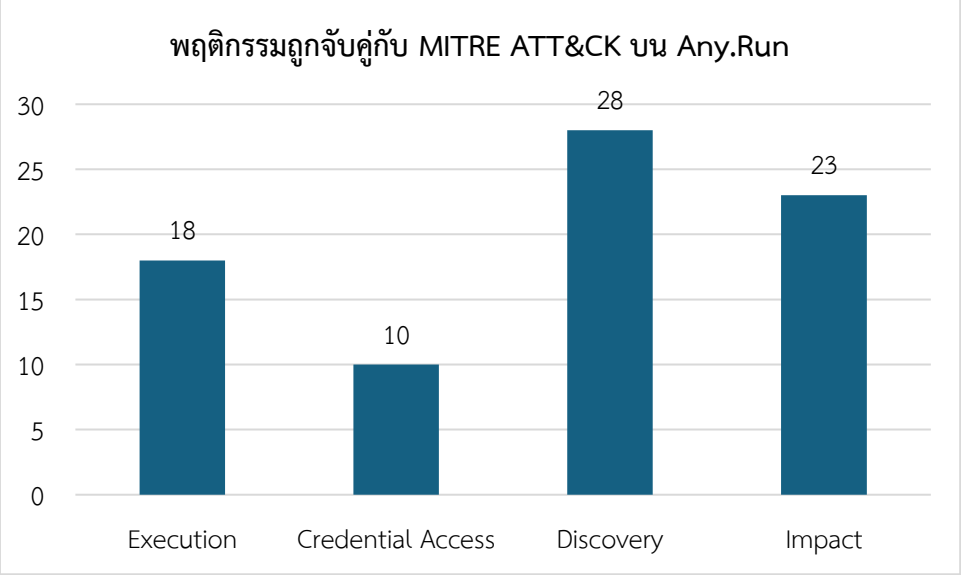
4.2.2 ผลพฤติกรรมถูกจับคู่กับ MITRE ATT&CK บน Any.Run

จากการวิเคราะห์พฤติกรรมของ LockBit Ransomware ผ่านแพลตฟอร์ม Any.Run พบว่าพฤติกรรมของมัลแวร์สามารถจับคู่กับกรอบการวิเคราะห์ MITRE ATT&CK ได้อย่างชัดเจนในหลายด้าน ได้แก่ กลยุทธ์ Execution โดยใช้เทคนิค User Execution จำนวน 18 เหตุการณ์ ซึ่งแสดงถึงการรันไฟล์มัลแวร์โดยผู้ใช้ หรือกระบวนการอัตโนมัติ ด้าน Credential Access พบการเข้าถึงข้อมูลรับรองใน

ไฟล์ (Credentials in Files) จำนวน 10 เหตุการณ์ กลยุทธ์ Discovery พบการค้นหาข้อมูลระบบผ่าน Query Registry จำนวน 28 เหตุการณ์ และสุดท้ายคือ Impact ซึ่งพบการเข้ารหัสข้อมูล (Data Encrypted for Impact) จำนวน 23 เหตุการณ์

ตารางที่ 4-2 ผลพฤติกรรมถูกจับคู่กับ MITRE ATT&CK บน Any.Run

Tactic	Technique	จำนวนเหตุการณ์
Execution	T1204 - User Execution	18
Credential Access	T1552 - Credentials in Files	10
Discovery	T1012 - Query Registry	28
Impact	T1486 - Data Encrypted for Impact	23



ภาพที่ 4-2 สรุปผลพฤติกรรมถูกจับคู่กับ MITRE ATT&CK บน Any.Run

4.3 ผลการตรวจจับเหตุการณ์ด้วย Wazuh

Wazuh ถูกใช้เพื่อวิเคราะห์การตรวจจับ และเฝ้าระวังแบบ Real-time และสามารถจับเหตุการณ์ที่เกี่ยวข้องกับ LockBit Ransomware ได้หลายรายการ ดังนี้

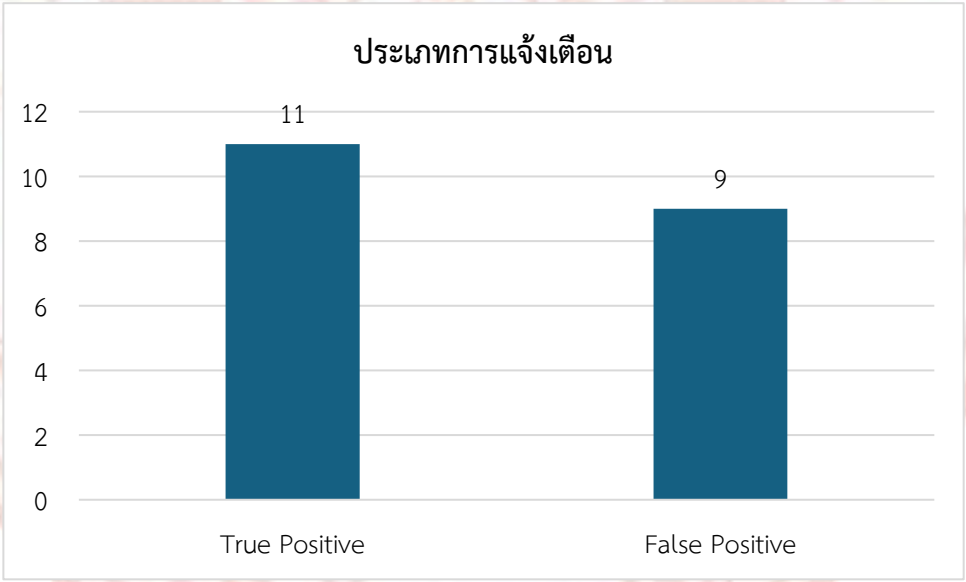
4.3.1 ประเภทของผลการแจ้งเตือนโดยรวม

จากการตรวจจับเหตุการณ์ด้วย Wazuh พบว่า มีการแจ้งเตือนที่เกี่ยวข้องกับพฤติกรรมของ LockBit Ransomware รวมทั้งหมด 20 ประเภท โดยในจำนวนนี้มี 11 ประเภทที่จัดเป็นเหตุการณ์

ประเภท True Positive ซึ่งสอดคล้องกับเทคนิคการโจมตีของมัลแวร์อย่างชัดเจน เช่น การเข้ารหัสไฟล์ การสร้าง service ในระบบ การลบ log การยกระดับสิทธิ์ผู้ใช้ และการตรวจสอบข้อมูลภายในระบบ ขณะที่อีก 9 เหตุการณ์จัดเป็น False Positive ซึ่งส่วนใหญ่เป็นกิจกรรมทั่วไปของระบบ เช่น การ Logon ของผู้ใช้ การแจ้งเตือนของ Windows และเหตุการณ์จาก VirusTotal ที่ไม่มีข้อมูล ทั้งนี้ Wazuh แสดงศักยภาพในการตรวจจับพฤติกรรมที่เป็นอันตรายได้อย่างครอบคลุมในแบบ Real-time โดยเฉพาะเมื่อใช้ร่วมกับการวิเคราะห์บริบท จะสามารถช่วยลดความคลาดเคลื่อนจาก False Positive และเสริมความแม่นยำในการวิเคราะห์ภัยคุกคามได้อย่างมีประสิทธิภาพ

ตารางที่ 4-3 ผลประเภทของผลการแจ้งเตือนโดยรวม

ประเภทการแจ้งเตือน	จำนวนเหตุการณ์
True Positive	11 เหตุการณ์
False Positive	9 เหตุการณ์



ภาพที่ 4-3 สรุปผลการแจ้งเตือนโดยรวม

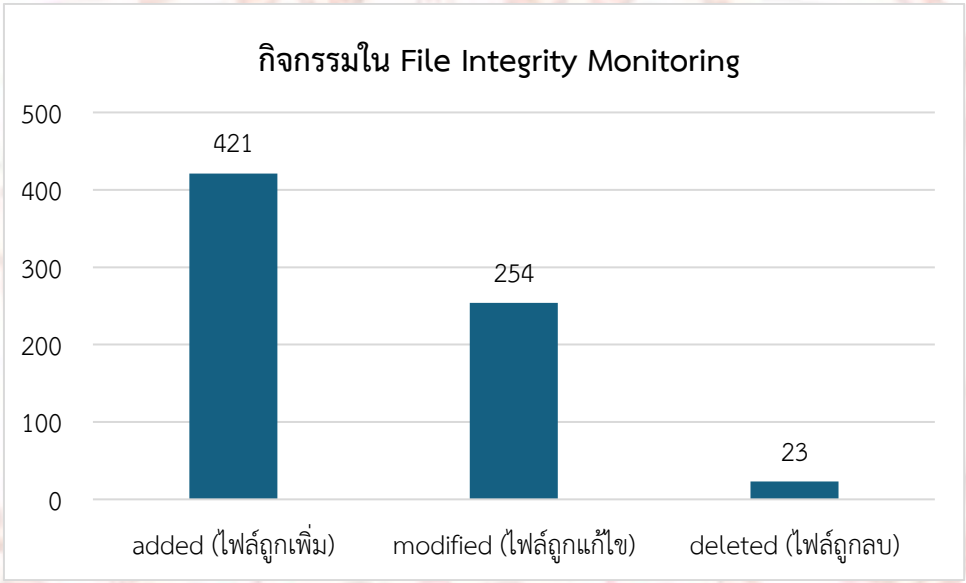
4.3.2 กิจกรรมใน File Integrity Monitoring ที่พบใน Wazuh

จากการตรวจสอบด้วยระบบ File Integrity Monitoring (FIM) ของ Wazuh หลังการรันมัลแวร์ LockBit Ransomware พบว่าเกิดการเปลี่ยนแปลงไฟล์ในระบบจำนวนมาก โดยมีไฟล์ที่ถูกเพิ่มใหม่ (added) จำนวน 421 รายการ ซึ่งส่วนใหญ่เป็นไฟล์เรียกค่าไถ่ (Ransom Note) ที่ถูกสร้างในหลายตำแหน่งของระบบ มีไฟล์ที่ถูกแก้ไข (modified) จำนวน 254 รายการ ซึ่งสอดคล้องกับพฤติกรรมการเข้ารหัสไฟล์ และพบไฟล์ที่ถูกลบ (deleted) จำนวน 23 รายการ ซึ่งอาจเป็นส่วนหนึ่งของการลบร่องรอย

หรือไฟล์สำคัญของระบบ ข้อมูลเหล่านี้สะท้อนให้เห็นถึงผลกระทบโดยตรงของมัลแวร์ที่สามารถตรวจจับผ่านฟีเจอร์ FIM ได้อย่างชัดเจน

ตารางที่ 4-4 ผลกิจกรรมใน File Integrity Monitoring ที่พบใน Wazuh

กิจกรรมใน File Integrity Monitoring	จำนวนเหตุการณ์
added (ไฟล์ถูกเพิ่ม)	421 รายการ
modified (ไฟล์ถูกแก้ไข)	254 รายการ
deleted (ไฟล์ถูกลบ)	23 รายการ



ภาพที่ 4-4 สรุปผลการแจ้งเตือนโดยรวมผลกิจกรรมใน File Integrity Monitoring ที่พบใน Wazuh

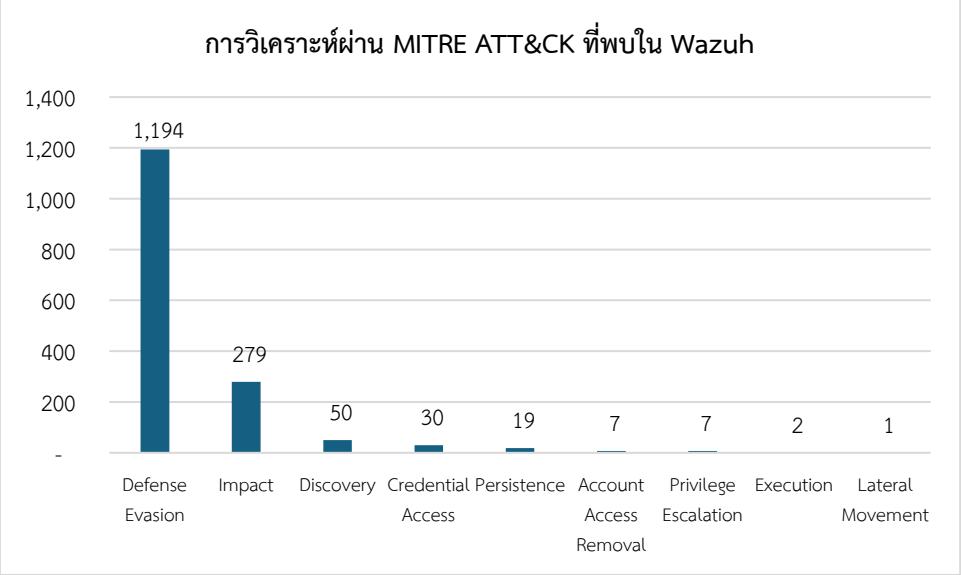
4.3.3 การวิเคราะห์ผ่าน MITRE ATT&CK ที่พบใน Wazuh

จากการตรวจจับเหตุการณ์ด้วย Wazuh พบว่าพฤติกรรมของ LockBit Ransomware สามารถจับคู่กับเทคนิคในกรอบ MITRE ATT&CK ได้อย่างชัดเจนในหลายกลยุทธ์ โดยกลยุทธ์ที่ตรวจพบมากที่สุดคือ Defense Evasion ผ่านเทคนิค T1070 - Indicator Removal จำนวน 1,170 เหตุการณ์ ซึ่งแสดงถึงความพยายามของมัลแวร์ในการลบ log และลบร่องรอยการโจมตี กลยุทธ์ด้าน Impact (T1485 - Data Destruction) ถูกตรวจพบ 23 เหตุการณ์ เป็นผลจากการเข้ารหัส และทำลายข้อมูล Discovery (T1087 - Account Discovery) มี 50 เหตุการณ์ บ่งชี้ถึงการสแกนข้อมูลผู้ใช้ และกลุ่มภายในระบบ Privilege Escalation (T1484 - Domain Policy Modification) และ Persistence (T1543.003 - Windows Service) ถูกตรวจพบ 7 และ 19 เหตุการณ์ตามลำดับ ซึ่งสะท้อนถึงการฝังตัว

และยกระดับสิทธิ์ของมัลแวร์เพื่อควบคุมระบบอย่างต่อเนื่อง พฤติกรรมเหล่านี้แสดงให้เห็นถึงรูปแบบการโจมตีที่ซับซ้อนของ LockBit Ransomware และสอดคล้องกับเทคนิคที่ใช้จริงในกรอบ MITRE ATT&CK

ตารางที่ 4-5 ผลการวิเคราะห์ผ่าน MITRE ATT&CK ที่พบใน Wazuh

Tactic	Technique	จำนวนเหตุการณ์
Defense Evasion	T1070-Indicator Removal	1,170
Impact	T1565.001-Stored Data Manipulation	254
Impact	T1485-Data Destruction	23
Defense Evasion	T1070.004-File Deletion	23
Discovery	T1087-Account Discovery	50
Privilege Escalation	T1484-Domain Policy Modification	7
Persistence	T1543.003-Windows Service	19
Execution	T1059.003-Windows Command Shell	2
Defense Evasion	T1562.001-Disable or Modify Tools	1
Impact	T1529-System Shutdown/Reboot	2
Credential Access	T1078-Valid Accounts	30
Account Access Removal	T1531-Account Access Removal	7
Lateral Movement	T1570-Lateral Tool Transfer	1



ภาพที่ 4-5 สรุปผลการวิเคราะห์ผ่าน MITRE ATT&CK ที่พบใน Wazuh

4.4 การเปรียบเทียบประสิทธิภาพของเครื่องมือที่ใช้

จากการเปรียบเทียบเครื่องมือที่ใช้ในการวิเคราะห์ LockBit Ransomware ได้แก่ Redline, Any.Run และ Wazuh พบว่าทั้งสามเครื่องมือล้วนสามารถใช้ในการวิเคราะห์ย้อนหลังได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ในด้านการตรวจจับแบบ Real-time มีเพียง Wazuh เท่านั้นที่รองรับได้จริง ขณะที่ Redline และ Any.Run จะเน้นการเก็บข้อมูลย้อนหลัง หรือในลักษณะ sandbox การตรวจจับ Process และการเปลี่ยนแปลงของ Registry ทั้งสามเครื่องมือสามารถทำได้ทั้งหมด ส่วนการตรวจจับ Log Event นั้น Redline ไม่รองรับโดยตรง แต่สามารถใช้ร่วมกับไฟล์จากแหล่งอื่นได้ ขณะที่ Any.Run และ Wazuh สามารถตรวจจับได้อย่างแม่นยำ โดยเฉพาะ Wazuh ที่เน้นการตรวจสอบ log แบบ Real-time นอกจากนี้ Any.Run และ Wazuh ยังสามารถเชื่อมโยงพฤติกรรมที่ตรวจพบกับกรอบ MITRE ATT&CK ได้โดยอัตโนมัติ ในขณะที่ Redline ไม่รองรับการเชื่อมโยงโดยตรง สะท้อนให้เห็นถึงข้อได้เปรียบของการใช้หลายเครื่องมือร่วมกันเพื่อการวิเคราะห์ที่ครอบคลุม

ตารางที่ 4-6 ผลการเปรียบเทียบความสามารถของแต่ละเครื่องมือ

ด้านที่เปรียบเทียบ	Redline	Any.Run	Wazuh
การวิเคราะห์ย้อนหลัง	ได้	ได้	ได้
ตรวจจับ Real-time	ไม่ได้	ไม่ได้	ได้
ตรวจจับ Process	ได้	ได้	ได้
ตรวจจับ Registry	ได้	ได้	ได้
ตรวจจับ Log Event	ไม่ได้	ได้	ได้
เชื่อมโยง MITRE ATT&CK	ไม่ได้	ได้	ได้

4.5 ข้อมูลเชิงคุณภาพ (Qualitative Findings)

4.5.1 พฤติกรรมของ LockBit Ransomware

เมื่อมีการรันไฟล์ชื่อ 86e17aa882c690ede284f3e445439dfe589d8f36e31cbc09d102305499d5c498.exe มัลแวร์จะเริ่มต้นกระบวนการเข้ารหัสไฟล์โดยอัตโนมัติทันที โดยทำการเปลี่ยนนามสกุลของไฟล์ที่ถูกเข้ารหัสเป็นนามสกุลเฉพาะ เช่น .kZd6jLlwz เป็นต้น เพื่อป้องกันไม่ให้ผู้ใช้สามารถเปิดใช้งานไฟล์เหล่านั้นได้ นอกจากนี้ มัลแวร์ยังสร้างไฟล์ข้อความเรียกค่าไถ่ หรือที่เรียกว่า Ransom Note ซึ่งอยู่ในรูปแบบไฟล์ README.txt และจะถูกสร้างไว้ในทุกไดเรกทอรีที่มีไฟล์ถูกเข้ารหัส พร้อมระบุข้อความเรียกค่าไถ่ วิธีการติดต่อ และขั้นตอนการชำระเงินเพื่อปลดล็อกข้อมูล อีกทั้งยังมีการเปลี่ยนภาพพื้นหลังของระบบ (Wallpaper) โดยอัตโนมัติเพื่อแสดงข้อความเรียกค่าไถ่เพิ่มเติม ทำให้ผู้ใช้ทราบว่าระบบของตนกำลังตกเป็นเหยื่อของการโจมตีจากแรนซัมแวร์

4.5.2 การลบร่องรอย และการหลบเลี่ยงการตรวจจับ

จากการวิเคราะห์ด้วยเครื่องมือ Redline พบว่าหลังจากมีการรันไฟล์มัลแวร์ ระบบมีพฤติกรรมการเปลี่ยนแปลงค่าภายในรีจิสทรี (Registry) อย่างต่อเนื่อง ซึ่งพฤติกรรมดังกล่าวอาจสะท้อนถึงความพยายามของมัลแวร์ในการสร้าง Persistence Mechanism หรือการฝังตัวเพื่อให้สามารถทำงานซ้ำได้ทุกครั้งที่ระบบถูกเปิดใช้งาน นอกจากนี้ยังอาจเป็นส่วนหนึ่งของกลไกการซ่อนตัว (Evasion) เพื่อหลีกเลี่ยงการตรวจจับจากซอฟต์แวร์ป้องกันภัยคุกคาม หรือผู้ดูแลระบบ

4.5.3 พฤติกรรมของ Process ที่สัมพันธ์กับมัลแวร์

จากการวิเคราะห์พฤติกรรมของมัลแวร์ LockBit Ransomware พบว่ามีการเรียกใช้งานโปรเซสของระบบหลายรายการที่สัมพันธ์กับการทำงานของมัลแวร์ โดยเฉพาะกระบวนการสำคัญที่เกี่ยวข้องกับการดำเนินกิจกรรมในระบบ เช่น cmd.exe, powershell.exe, vssadmin.exe และ wevtutil.exe เป็นต้น ซึ่งมักถูกใช้ในการลบ Shadow Copies, ปิดระบบบันทึกเหตุการณ์ และดำเนินคำสั่งอัตโนมัติผ่านสคริปต์ PowerShell อีกทั้งยังพบการใช้โปรเซส notepad.exe เพื่อเปิดข้อความเรียกค่าไถ่ (Ransom Note) ให้ผู้ใช้รับทราบถึงเงื่อนไขการชำระเงิน นอกจากนี้ยังมีการเรียกใช้ schtasks.exe และ explorer.exe ซึ่งอาจถูกใช้ในการสร้าง Scheduled Tasks หรือรันคำสั่งเบื้องหลัง (Background Execution) เพื่อให้มัลแวร์ยังคงทำงานต่อไปโดยไม่ถูกตรวจพบทันที พฤติกรรมเหล่านี้สะท้อนถึงกลยุทธ์การดำเนินงานของ LockBit ที่อาศัยเครื่องมือภายในระบบปฏิบัติการเพื่อเพิ่มความแนบเนียนในการโจมตี

4.5.4 ผลกระทบต่อระบบที่สังเกตได้

จากการสังเกตพฤติกรรมของมัลแวร์ LockBit Ransomware หลังการรันพบว่าระบบได้รับผลกระทบในหลายด้านที่ส่งผลต่อความสามารถในการทำงานของผู้ใช้ และการตรวจสอบเหตุการณ์ย้อนหลัง โดยหนึ่งในผลกระทบที่เด่นชัดคือ ไม่สามารถเปิดใช้งาน Event Viewer ได้ ซึ่งเกิดจากการที่มัลแวร์ดำเนินการล้างบันทึกเหตุการณ์ (Event Logs) ของระบบ ส่งผลให้ข้อมูลสำคัญที่ใช้ในการวิเคราะห์ย้อนหลังสูญหายไป นอกจากนี้ยังพบว่า ไม่สามารถใช้คุณสมบัติ Previous Versions ได้ เนื่องจากมัลแวร์ได้ลบ Shadow Copy ของระบบทั้งหมดเพื่อป้องกันไม่ให้ผู้ใช้สามารถกู้คืนไฟล์ที่ถูกเข้ารหัสได้

ในส่วนของการเข้ารหัสข้อมูล พบว่า LockBit Ransomware สามารถดำเนินการเข้ารหัสได้อย่างรวดเร็วภายในเวลาสั้น ๆ โดยครอบคลุมไฟล์ที่มีความสำคัญหลากหลายประเภท ไม่ว่าจะเป็นเอกสารงาน รหัสผ่านที่ถูกจัดเก็บไว้ในเว็บเบราว์เซอร์ และไฟล์ส่วนตัวของผู้ใช้งาน ทำให้เกิดผลกระทบโดยตรงต่อความพร้อมใช้งานของข้อมูล และสร้างแรงกดดันให้เหยื่อยอมจ่ายค่าไถ่เพื่อแลกกับการกู้คืนข้อมูลกลับคืนมา

4.5.5 มุมมองจากการตรวจจับโดย Wazuh

จากการติดตาม และตรวจสอบเหตุการณ์ด้วยระบบ Wazuh พบว่าสามารถตรวจจับพฤติกรรมที่เกี่ยวข้องกับ LockBit Ransomware ได้อย่างมีประสิทธิภาพ โดยเฉพาะผ่านฟีเจอร์ File Integrity Monitoring (FIM) ซึ่งสามารถระบุการเปลี่ยนแปลงของไฟล์จำนวนมากที่เกิดขึ้นภายในเวลาอันรวดเร็วทันทีหลังจากมัลแวร์เริ่มทำงาน ระบบสามารถแสดงรายการไฟล์ที่ถูก เพิ่ม แก้ไข

และลบ พร้อมกับแสดงชื่อผู้ใช้งานที่เกี่ยวข้องในการดำเนินการดังกล่าว เช่น lucksa หรือ SYSTEM ซึ่งเป็นข้อมูลสำคัญในการระบุจุดเริ่มต้นของการโจมตี และการกระทำของมัลแวร์ในระบบ

นอกจากนี้ Wazuh ยังสามารถวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยเชื่อมโยงกับ MITRE ATT&CK Framework ได้อย่างแม่นยำ เช่น เทคนิค T1070 – Indicator Removal on Host ที่แสดงถึงความพยายามของมัลแวร์ในการลบ Log หรือร่องรอยของการโจมตี, เทคนิค T1485 – Data Destruction ซึ่งสะท้อนถึงการทำลายข้อมูลผ่านการเข้ารหัส และเทคนิค T1543 – Create or Modify System Process ที่เกี่ยวข้องกับการสร้าง หรือเปลี่ยนแปลง service เพื่อรักษาการทำงานของมัลแวร์ในระบบอย่างต่อเนื่อง ข้อมูลจาก Wazuh จึงสามารถนำไปใช้วิเคราะห์เหตุการณ์เชิงลึก และเป็นแนวทางสำคัญในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ

4.6 ผลสรุป Attack Timeline ของ LockBit Ransomware โดยอ้างอิงจาก MITRE ATT&CK

จากการวิเคราะห์พฤติกรรมของ LockBit Ransomware โดยใช้การจับคู่กับกรอบแนวคิด MITRE ATT&CK Framework สามารถสรุปลำดับเหตุการณ์การโจมตีได้อย่างเป็นขั้นตอน (Attack Timeline) ดังนี้

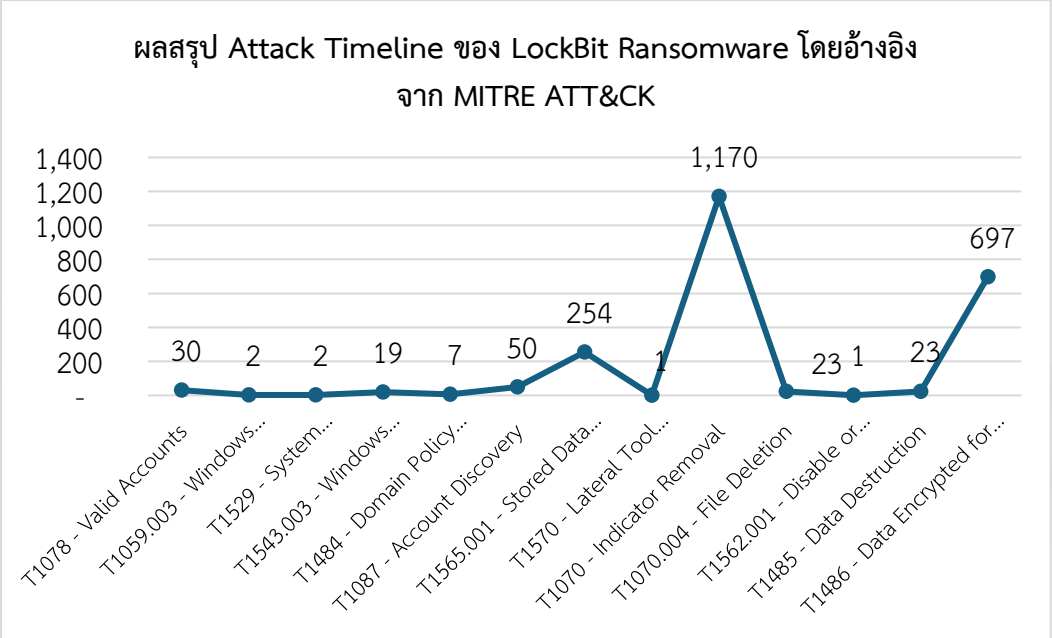
เริ่มจาก Initial Access พบว่าผู้โจมตีใช้บัญชีที่ถูกขโมย หรือเจาะเข้าสู่ระบบ (T1078 - Valid Accounts) จำนวน 30 เหตุการณ์ ซึ่งถือเป็นขั้นตอนเริ่มต้นของการแทรกซึมเข้าสู่ระบบเครือข่ายภายใน ต่อมาในขั้นตอน Execution มีการใช้ Windows Command Shell (T1059.003) จำนวน 2 เหตุการณ์ เพื่อดำเนินการรันคำสั่งมัลแวร์แบบอัตโนมัติ และยังพบการสั่ง Shutdown หรือ Reboot ระบบ (T1529) จำนวน 2 เหตุการณ์ ซึ่งอาจมีจุดประสงค์เพื่อโหลด payload หรือกลบข้อมูลบางส่วน

ในส่วนของ Persistence มีการสร้าง Windows Service ใหม่ (T1543.003) ถึง 19 เหตุการณ์ เพื่อให้มัลแวร์สามารถฝังตัวอยู่ในระบบอย่างต่อเนื่อง ส่วนการ Privilege Escalation พบเทคนิคการปรับเปลี่ยน Group Policy หรือ Domain Policy (T1484) จำนวน 7 เหตุการณ์ ซึ่งช่วยให้ผู้โจมตีสามารถยกระดับสิทธิ์ และควบคุมระบบได้มากขึ้น

ระหว่างการ Discovery มีการดำเนินการค้นหาข้อมูลภายในระบบอย่างเข้มข้น โดยเฉพาะ Account Discovery (T1087) จำนวน 50 เหตุการณ์ และ Stored Data Manipulation (T1565.001) จำนวน 254 เหตุการณ์ ซึ่งอาจเกี่ยวข้องกับการเปลี่ยนชื่อไฟล์หรือการปลอมแปลงข้อมูลในระหว่างการเข้ารหัส

สำหรับ Lateral Movement พบการใช้เทคนิค Lateral Tool Transfer (T1570) จำนวน 1 เหตุการณ์ ซึ่งบ่งชี้ถึงการส่งไฟล์ หรือ payload ไปยังเครื่องอื่นในเครือข่าย ด้าน Defense Evasion เป็นขั้นตอนที่เกิดขึ้นอย่างหนาแน่น โดยพบการลบร่องรอย และบันทึกเหตุการณ์ต่าง ๆ (T1070) มากถึง 1,170 เหตุการณ์ การลบไฟล์ระบบ (T1070.004) จำนวน 23 เหตุการณ์ และการปิด หรือปรับการทำงานของเครื่องมือป้องกันระบบ (T1562.001) อีก 1 เหตุการณ์

สุดท้ายในขั้นตอน Impact พบว่า LockBit Ransomware มุ่งเน้นสร้างความเสียหายโดยตรง ทั้งในรูปแบบของการทำลายข้อมูล (T1485) จำนวน 23 เหตุการณ์ และการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ (T1486) จำนวนสูงถึง 697 เหตุการณ์ ซึ่งถือเป็นจุดประสงค์หลักของการโจมตีโดยมัลแวร์ประเภทนี้



ภาพที่ 4-6 ผลสรุป Attack Timeline ของ LockBit Ransomware โดยอ้างอิงจาก MITRE ATT&CK

บทที่ 5
อภิปรายผล สรุปผล และข้อเสนอแนะ

จากการดำเนินงานการวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์ และเครื่องมือวิเคราะห์เฉพาะทางสามารถสรุปอภิปรายผลการวิจัย แบ่งได้เป็น 3 ส่วน ดังนี้

5.1 อภิปรายผลการวิจัย

5.2 สรุปผลการวิจัย

5.3 ข้อเสนอแนะ

5.1 อภิปรายผลการวิจัย

จากการศึกษาพฤติกรรมของ LockBit Ransomware โดยใช้เครื่องมือ Redline, Any.Run และ Wazuh ในสภาพแวดล้อมจำลองบนระบบปฏิบัติการ Windows พบว่า มัลแวร์มีพฤติกรรมที่สอดคล้องกับลักษณะของแรนซัมแวร์ขั้นสูง โดยสามารถเข้ารหัสไฟล์ได้รวดเร็ว สร้างไฟล์เรียกค่าไถ่ และลบข้อมูลสำรองพร้อมกับลบ log เหตุการณ์ของระบบเพื่อหลบเลี่ยงการตรวจจับ

ในเชิงปริมาณ พบว่า LockBit Ransomware เข้ารหัสไฟล์จำนวน 697 ไฟล์ สร้างไฟล์ Ransom Note 518 ไฟล์ มีการสร้าง Process ใหม่ 166 รายการ (เกี่ยวข้องกับมัลแวร์ 28 รายการ) และตรวจพบพฤติกรรมเปลี่ยนแปลง Registry ถึง 13,565 รายการ ขณะเดียวกัน Wazuh ตรวจจับเหตุการณ์ Integrity checksum changed ได้มากถึง 1,274 รายการ และจับคู่พฤติกรรมมัลแวร์ได้กับเทคนิค MITRE ATT&CK หลายรายการ เช่น T1070 (ลบ log), T1485 (ทำลายข้อมูล), และ T1543 (สร้าง service ฝังตัว)

ในเชิงคุณภาพ พบพฤติกรรมชัดเจนของมัลแวร์ เช่น การเปลี่ยน Wallpaper, การเปิด Notepad แสดงข้อความเรียกค่าไถ่, การลบ Shadow Copy และ การลบร่องรอย เป็นต้น ซึ่งเป็นเครื่องยืนยันถึงความสามารถในการโจมตี และหลบเลี่ยงการตรวจจับอย่างมีแบบแผน

5.2 สรุปการวิจัย

จากการทดลอง และวิเคราะห์พฤติกรรมของ LockBit Ransomware พบว่า มัลแวร์มีความสามารถในการดำเนินการโจมตีอย่างเป็นระบบ โดยเริ่มจากการเข้ารหัสไฟล์จำนวนมาก พร้อมสร้าง Ransom Note และลบร่องรอยสำคัญ เช่น Shadow Copy และ Event Logs ซึ่งเป็นพฤติกรรมที่ตรงกับเทคนิคในกรอบ MITRE ATT&CK อย่างชัดเจน เช่น T1070 (ลบร่องรอย), T1485 (ทำลายข้อมูล), และ T1543 (สร้างบริการฝังตัว)

การใช้เครื่องมือ Redline, Any.Run และ Wazuh ช่วยให้สามารถสังเกตพฤติกรรมของมัลแวร์ได้ในหลากหลายมิติ Redline ให้ข้อมูลเชิงลึกด้านไฟล์ ระบบ Registry และ Process ที่เปลี่ยนแปลงหลังการติดมัลแวร์ ส่วน Any.Run ช่วยให้เห็นพฤติกรรมแบบ sandbox ที่เกิดขึ้นในช่วงเวลาจริง และ

Wazuh ทำหน้าที่เฝ้าระวังเหตุการณ์แบบ Real-time พร้อมการจับคู่กับ MITRE ATT&CK ได้อย่างแม่นยำ

ข้อมูลเชิงปริมาณที่ได้จากการวิเคราะห์ เช่น ไฟล์ที่ถูกเข้ารหัส 697 ไฟล์, กิจกรรม Registry กว่า 13,000 รายการ และเหตุการณ์ File Integrity Monitoring รวมกว่า 698 เหตุการณ์ แสดงให้เห็นว่า LockBit Ransomware มีผลกระทบต่อระบบอย่างรุนแรง

แม้จะพบ False Positive บางส่วนจาก Wazuh เช่น การล็อกอินของผู้ใช้ หรือการทำงานของบริการ Windows ทั่วไป แต่ด้วยการวิเคราะห์บริบทของเหตุการณ์ และการตรวจสอบแบบสหวิธีผ่านหลายเครื่องมือ ก็สามารถแยกแยะพฤติกรรมของมัลแวร์ออกจากพฤติกรรมปกติได้อย่างแม่นยำ

จากผลที่ได้แสดงให้เห็นว่า การวิเคราะห์โดยใช้หลายเครื่องมือร่วมกันนั้นให้ประสิทธิภาพในการตรวจจับมัลแวร์ได้ดีกว่าการใช้เครื่องมือเดี่ยว ซึ่งเป็นแนวทางที่สามารถนำไปประยุกต์ใช้จริงในองค์กรเพื่อเพิ่มความมั่นคงปลอดภัยเชิงรุกได้อย่างมีประสิทธิภาพการทดลองซึ่งมีพื้นฐานความรู้ที่แตกต่างกัน มีการตอบสนองต่อการโจมตีด้วยฟิชชิงอีเมลในรูปแบบที่แตกต่างกัน ซึ่งสอดคล้องกับผลการทดลองในงานวิจัยนี้

5.3 ข้อเสนอแนะ

จากผลการวิจัย สามารถสรุปข้อเสนอแนะได้ดังนี้

5.1 ควรบูรณาการการใช้เครื่องมือทางนิติวิทยาศาสตร์ เช่น Redline, เครื่องมือจำลองพฤติกรรมแบบ Sandbox เช่น Any.Run และระบบตรวจจับเหตุการณ์แบบ Real-time เช่น Wazuh ร่วมกัน เพื่อเพิ่มประสิทธิภาพในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างครอบคลุมยิ่งขึ้น

5.2 ควรมีการปรับแต่งกฎการตรวจจับ (Detection Rules) ให้สอดคล้องกับบริบทขององค์กร รวมถึงการวางแผนกู้คืนระบบ (Disaster Recovery Plan) และสำรองข้อมูลสำคัญ เช่น Shadow Copy และ Log เพื่อให้สามารถฟื้นตัวจากการโจมตีได้อย่างรวดเร็ว

5.3 ควรพิจารณานำเทคโนโลยี Machine Learning (ML) และ Artificial Intelligence (AI) เข้ามาเสริมการวิเคราะห์พฤติกรรมที่ผิดปกติ เช่น การเรียนรู้พฤติกรรมการใช้งานผู้ใช้แต่ละราย และแจ้งเตือนเมื่อพบความเบี่ยงเบน (Anomaly Detection) เพื่อลด False Positive และเพิ่มความแม่นยำในการตรวจจับภัยคุกคามที่ไม่เคยพบมาก่อน รวมถึงวิเคราะห์ความสัมพันธ์ของข้อมูลหลายแหล่ง (Log Correlation) เพื่อจับเหตุการณ์ที่เกี่ยวข้องกับการโจมตีแบบ APT (Advanced Persistent Threat)

5.4 ในการศึกษาและวิเคราะห์ตัวอย่างมัลแวร์จริง เช่น LockBit Ransomware ควรดำเนินการในสภาพแวดล้อมที่จำลองขึ้น (Isolated Environment) เช่น ใช้ Virtual Machine ที่ไม่มีการเชื่อมต่อกับเครือข่ายภายนอก พร้อมตั้งค่า Snapshot และ Backup เพื่อป้องกันผลกระทบต่อระบบจริง

5.5 ควรเน้นย้ำแนวทางการวิเคราะห์เชิงรุก และการปฏิบัติตามแนวทางระบบการรักษาความปลอดภัยสารสนเทศที่ยอมรับในระดับสากล เพื่อหลีกเลี่ยงผลกระทบที่อาจเกิดขึ้นต่อระบบจริง

5.6 ในอนาคต งานวิจัยควรผสานการใช้เทคโนโลยี AI/ML ร่วมกับเครื่องมือวิเคราะห์ภัยคุกคาม เพื่อเพิ่มศักยภาพในการตรวจจับและตอบสนองต่อแรนซัมแวร์ได้อย่างชาญฉลาด ปลอดภัย และแม่นยำยิ่งขึ้น

บรรณานุกรม

1. N. Suk-on, N. Thiratitsakun, and K. Chimmanee, “Digital Forensic Analysis of Lockbit Ransomware Attack on Operational Technology,” in Proc. 8th Int. Conf. Information Technol. (InCIT), 2024, pp. 624–630.
2. A. A. M. A. Alwashali et al., “A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack,” in Proc. 14th Int. Conf. Developments in eSystems Eng. (DeSE), 2021.
3. N. A. Malik et al., “Behavior and Characteristics of Ransomware – A Survey,” in Proc. 2nd Int. Conf. Cyber Resilience (ICCR), 2024.
4. R. Ahmed et al., “REvil Ransomware: Analysis of One of the Most Sophisticated Malware Families,” in Proc. Int. Conf. Cybersecurity Trends (ICCT), 2023.
5. K. Khaliq et al., “Ransomware Attacks: Tools and Techniques for Detection,” in Proc. 2nd Int. Conf. Cyber Resilience (ICCR), 2024.
6. S. K. Verma and A. Tiwari, “Understanding the Behavior of Ransomware: An I/O Request-Based Analysis,” in Int. J. Info. Security & Privacy, vol. 18, no. 2, pp. 105–118, 2023.
7. L. Chen and W. Lin, “Social Engineering as an Attack Vector for Ransomware: Prevention Techniques,” in Cybersecurity Research and Practice, vol. 2, no. 1, 2023.
8. C. B. Asaju et al., “Development of a Machine Learning Model for Detecting and Classifying Ransomware,” in Proc. 1st Int. Conf. Multidisciplinary Eng. and Applied Sci. (ICMEAS), 2021.

9. D. K. Sharma et al., “Targeted Ransomware Attacks and Detection to Strengthen Enterprise Security,” in Proc. Int. Conf. Next-Gen Security (ICNS), 2023.

10. A. Jukuntla, G. Gutha, A. Palem, S. L. S. Kotaru, and R. Alavala, “Investigating the Effectiveness of Hash Line Baseline for File Integrity Monitoring,” in Proc. 5th Int. Conf. Image Process. Capsule Netw. (ICIPCN), 2024, pp. 901–906.

11. M. R. A. Suhendi et al., “Network Anomaly Detection Analysis using Artillery Honeypot and Wazuh SIEM,” in Proc. 9th Int. Conf. Computing, Eng. and Design (ICCED), 2023.

12. A. A. Khan and M. H. Miraz, “Ransomware Detection and Classification Using Machine Learning Algorithms,” in Proc. Int. Conf. Advanced Comp. Sci. and Info. Syst. (ICACSIS), 2023

13. S. Lee et al., “Hiding in the Crowd: Ransomware Protection by Adopting Camouflage and Hiding Strategy With the Link File,” IEEE Access, vol. 11, pp. 92693–92715, 2023.

14. L. Chen and W. Lin, “Social Engineering as an Attack Vector for Ransomware: Prevention Techniques,” in Cybersecurity Research and Practice, vol. 2, no. 1, 2023.

15. M. B. A. Al-Doori and E. I. Komotskiy, “Intrusion Detection and Prevention System AI Based Features with Random Forest,” in Proc. Int. Conf. on AI & Data Sci., 2024.

16. D. Dholariya, D. Panchal, and P. Singhal, “Dissection of Rorschach Ransomware,” in IEEE World AI IoT Congress (AIIoT), 2024.

17. Sanook Hitech, "รายงาน Palo Alto เผยกลุ่ม LockBit เล็งโจมตีภาคก่อสร้างไทย," Sanook.com, Apr. 26, 2024. [Online]. Available: https://www.sanook.com/hitech/1598491

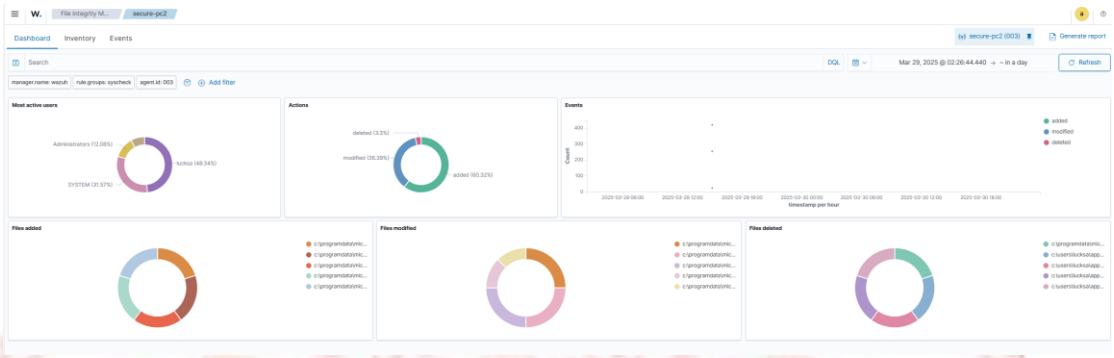
18. A. Alraizza and A. Algarni, "Ransomware: A Survey," ResearchGate, Aug. 2023. [Online]. Available: https://www.researchgate.net/figure/Locker-ransomware

19. Akamai, "What is LockBit Ransomware," Akamai, 2024. [Online]. Available: https://www.akamai.com/glossary/what-is-lockbit-ransomware. [Accessed: 27-Apr-2025].

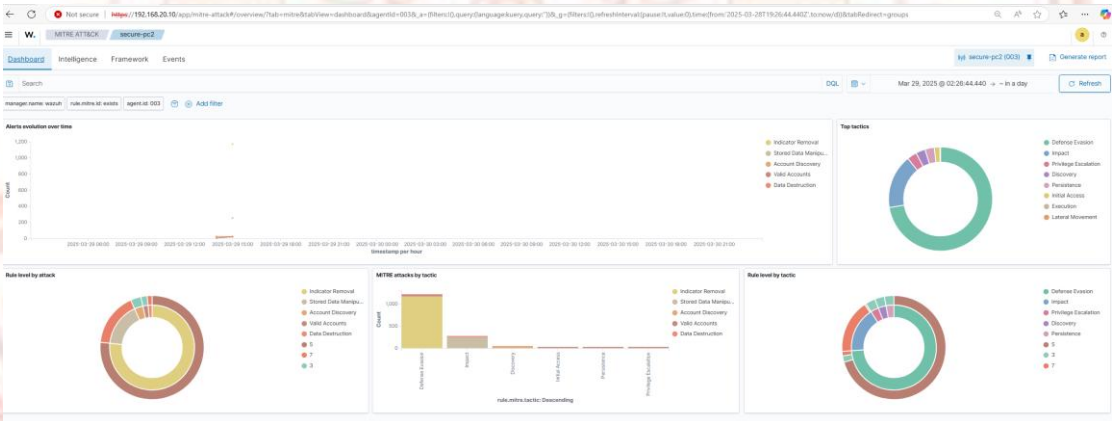
20. องค์การรักษาความปลอดภัยฝ่ายพลเรือน, "กระบวนการนิติวิทยาศาสตร์ทางดิจิทัล," 26 กันยายน 2021. [ออนไลน์]. Available: https://www.secnia.go.th/2021/09/กระบวนการนิติวิทยาศาสตร์ทางดิจิทัล/

ภาคผนวก ก

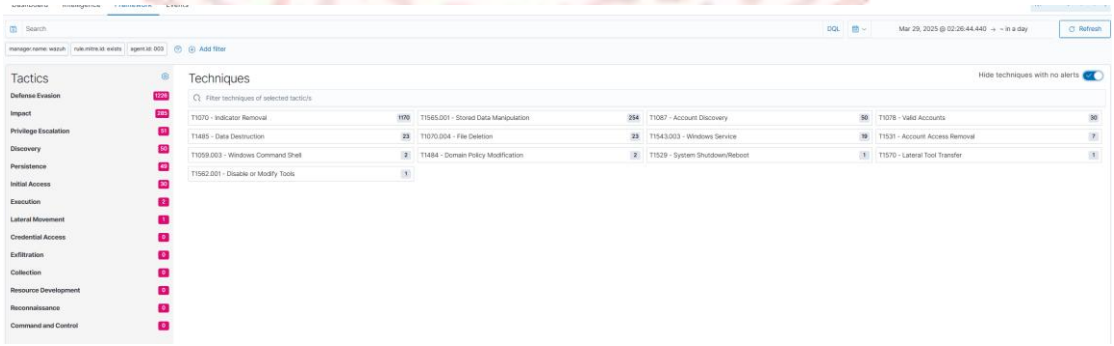
ข้อมูลดิบที่ได้จากการทดสอบ



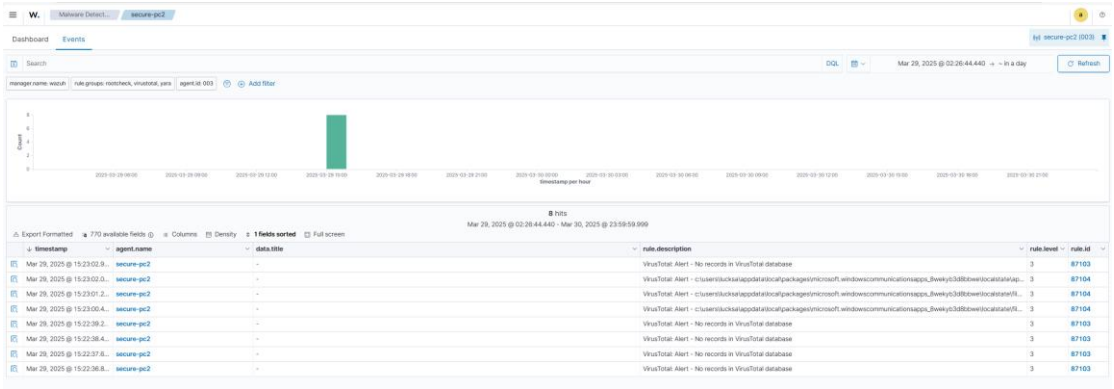
ภาพที่ ก-1 หน้าจอแสดงผลสรุปการตรวจสอบความสมบูรณ์ของไฟล์ในระบบ Wazuh



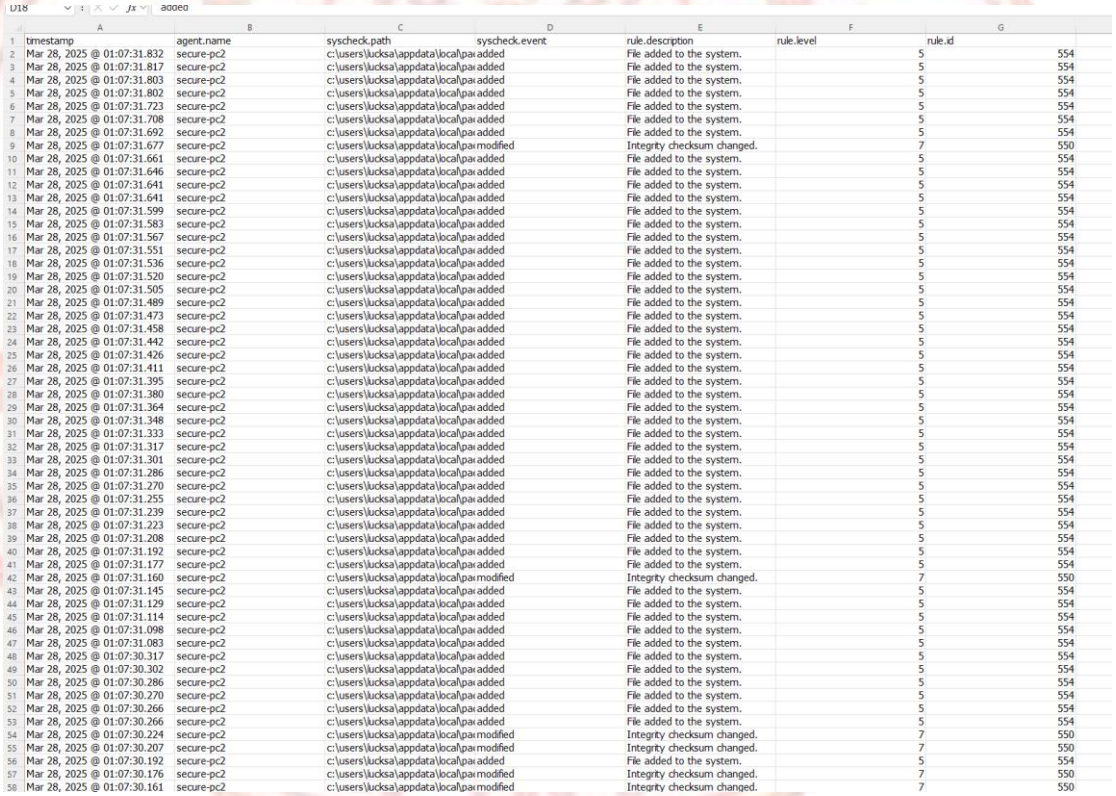
ภาพที่ ก-2 หน้าจอแสดงผลสรุป MITRE ATT&CK ในระบบ Wazuh



ภาพที่ ก-3 หน้าจอแสดงตาราง MITRE ATT&CK ในระบบ Wazuh



ภาพที่ ก-4 หน้าจอแสดงผลสรุปการตรวจจับมัลแวร์ในระบบ Wazuh

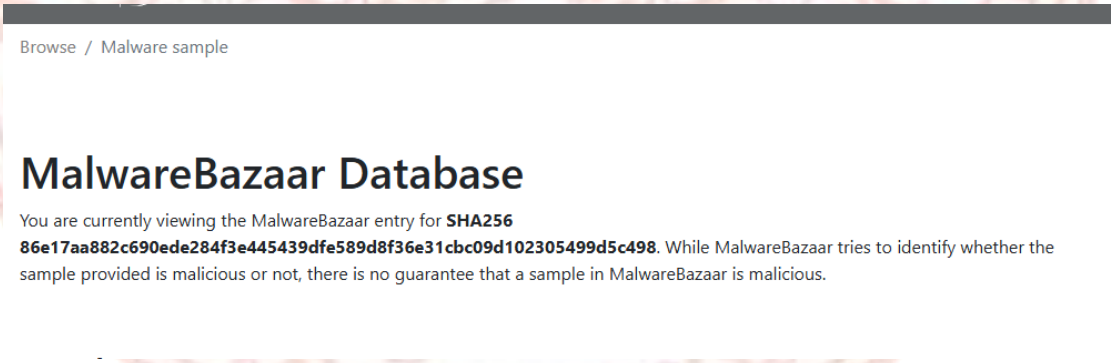


	A	B	C	D	E	F	G
1	timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
2	Mar 28, 2025 @ 01:07:31.832	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
3	Mar 28, 2025 @ 01:07:31.817	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
4	Mar 28, 2025 @ 01:07:31.803	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
5	Mar 28, 2025 @ 01:07:31.802	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
6	Mar 28, 2025 @ 01:07:31.723	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
7	Mar 28, 2025 @ 01:07:31.708	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
8	Mar 28, 2025 @ 01:07:31.692	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
9	Mar 28, 2025 @ 01:07:31.677	secure-pc2	c:\users\lucksa\appdata\local\pa	modified	Integrity checksum changed.	7	550
10	Mar 28, 2025 @ 01:07:31.661	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
11	Mar 28, 2025 @ 01:07:31.646	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
12	Mar 28, 2025 @ 01:07:31.641	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
13	Mar 28, 2025 @ 01:07:31.641	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
14	Mar 28, 2025 @ 01:07:31.599	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
15	Mar 28, 2025 @ 01:07:31.583	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
16	Mar 28, 2025 @ 01:07:31.567	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
17	Mar 28, 2025 @ 01:07:31.551	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
18	Mar 28, 2025 @ 01:07:31.536	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
19	Mar 28, 2025 @ 01:07:31.520	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
20	Mar 28, 2025 @ 01:07:31.505	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
21	Mar 28, 2025 @ 01:07:31.489	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
22	Mar 28, 2025 @ 01:07:31.473	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
23	Mar 28, 2025 @ 01:07:31.458	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
24	Mar 28, 2025 @ 01:07:31.442	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
25	Mar 28, 2025 @ 01:07:31.426	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
26	Mar 28, 2025 @ 01:07:31.411	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
27	Mar 28, 2025 @ 01:07:31.395	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
28	Mar 28, 2025 @ 01:07:31.380	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
29	Mar 28, 2025 @ 01:07:31.364	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
30	Mar 28, 2025 @ 01:07:31.348	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
31	Mar 28, 2025 @ 01:07:31.333	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
32	Mar 28, 2025 @ 01:07:31.317	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
33	Mar 28, 2025 @ 01:07:31.301	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
34	Mar 28, 2025 @ 01:07:31.286	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
35	Mar 28, 2025 @ 01:07:31.270	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
36	Mar 28, 2025 @ 01:07:31.255	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
37	Mar 28, 2025 @ 01:07:31.239	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
38	Mar 28, 2025 @ 01:07:31.223	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
39	Mar 28, 2025 @ 01:07:31.208	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
40	Mar 28, 2025 @ 01:07:31.192	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
41	Mar 28, 2025 @ 01:07:31.177	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
42	Mar 28, 2025 @ 01:07:31.160	secure-pc2	c:\users\lucksa\appdata\local\pa	modified	Integrity checksum changed.	7	550
43	Mar 28, 2025 @ 01:07:31.145	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
44	Mar 28, 2025 @ 01:07:31.129	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
45	Mar 28, 2025 @ 01:07:31.114	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
46	Mar 28, 2025 @ 01:07:31.098	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
47	Mar 28, 2025 @ 01:07:31.083	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
48	Mar 28, 2025 @ 01:07:30.317	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
49	Mar 28, 2025 @ 01:07:30.302	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
50	Mar 28, 2025 @ 01:07:30.286	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
51	Mar 28, 2025 @ 01:07:30.270	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
52	Mar 28, 2025 @ 01:07:30.266	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
53	Mar 28, 2025 @ 01:07:30.266	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
54	Mar 28, 2025 @ 01:07:30.224	secure-pc2	c:\users\lucksa\appdata\local\pa	modified	Integrity checksum changed.	7	550
55	Mar 28, 2025 @ 01:07:30.207	secure-pc2	c:\users\lucksa\appdata\local\pa	modified	Integrity checksum changed.	7	550
56	Mar 28, 2025 @ 01:07:30.192	secure-pc2	c:\users\lucksa\appdata\local\pa	added	File added to the system.	5	554
57	Mar 28, 2025 @ 01:07:30.176	secure-pc2	c:\users\lucksa\appdata\local\pa	modified	Integrity checksum changed.	7	550
58	Mar 28, 2025 @ 01:07:30.161	secure-pc2	c:\users\lucksa\appdata\local\pa	modified	Integrity checksum changed.	7	550

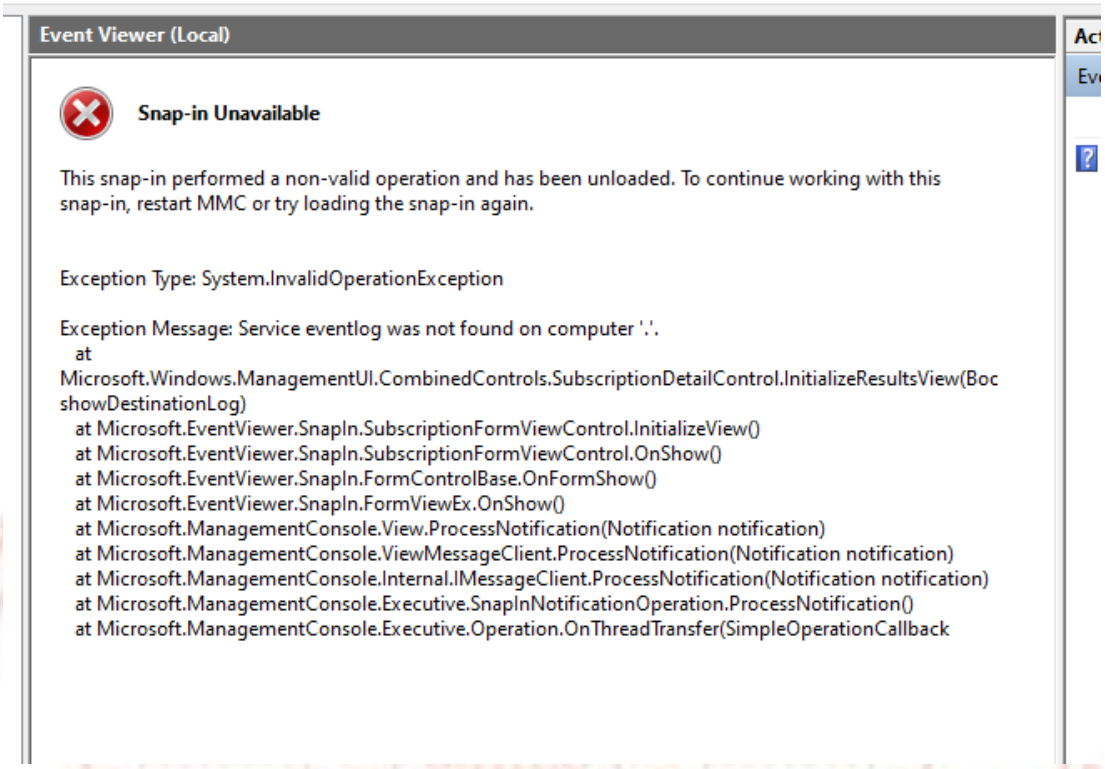
ภาพที่ ก-5 ข้อมูลดิบการตรวจสอบความสมบูรณ์ของไฟล์ในระบบ Wazuh

	A	B	C	D	E	F	G	H
1	timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id	
2	Mar 28, 2025 @ 01:07:31.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
3	Mar 28, 2025 @ 01:07:31.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
4	Mar 28, 2025 @ 01:07:30.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
5	Mar 28, 2025 @ 01:07:30.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
6	Mar 28, 2025 @ 01:07:30.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
7	Mar 28, 2025 @ 01:07:30.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
8	Mar 28, 2025 @ 01:07:30.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
9	Mar 28, 2025 @ 01:07:30.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
10	Mar 28, 2025 @ 01:07:29.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
11	Mar 28, 2025 @ 01:07:29.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
12	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
13	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
14	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
15	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
16	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
17	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
18	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
19	Mar 28, 2025 @ 01:07:27.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
20	Mar 28, 2025 @ 01:07:26.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
21	Mar 28, 2025 @ 01:07:26.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
22	Mar 28, 2025 @ 01:07:26.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
23	Mar 28, 2025 @ 01:07:26.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
24	Mar 28, 2025 @ 01:07:26.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
25	Mar 28, 2025 @ 01:07:26.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
26	Mar 28, 2025 @ 01:07:25.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
27	Mar 28, 2025 @ 01:07:25.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
28	Mar 28, 2025 @ 01:07:25.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
29	Mar 28, 2025 @ 01:07:20.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
30	Mar 28, 2025 @ 01:07:20.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
31	Mar 28, 2025 @ 01:07:20.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
32	Mar 28, 2025 @ 01:07:20.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
33	Mar 28, 2025 @ 01:07:19.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
34	Mar 28, 2025 @ 01:07:19.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
35	Mar 28, 2025 @ 01:07:19.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
36	Mar 28, 2025 @ 01:07:18.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
37	Mar 28, 2025 @ 01:07:17.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
38	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
39	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
40	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
41	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
42	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
43	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
44	Mar 28, 2025 @ 01:07:16.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
45	Mar 28, 2025 @ 01:07:15.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
46	Mar 28, 2025 @ 01:07:15.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
47	Mar 28, 2025 @ 01:07:15.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
48	Mar 28, 2025 @ 01:07:02.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
49	Mar 28, 2025 @ 01:07:00.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
50	Mar 28, 2025 @ 01:07:00.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
51	Mar 28, 2025 @ 01:06:59.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
52	Mar 28, 2025 @ 01:06:59.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
53	Mar 28, 2025 @ 01:06:59.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
54	Mar 28, 2025 @ 01:06:59.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
55	Mar 28, 2025 @ 01:06:59.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
56	Mar 28, 2025 @ 01:06:57.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
57	Mar 28, 2025 @ 01:06:57.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	
58	Mar 28, 2025 @ 01:06:57.	secure-pc2	["T1565.001"]	["Impact"]	Integrity checksum changed.	7	550	

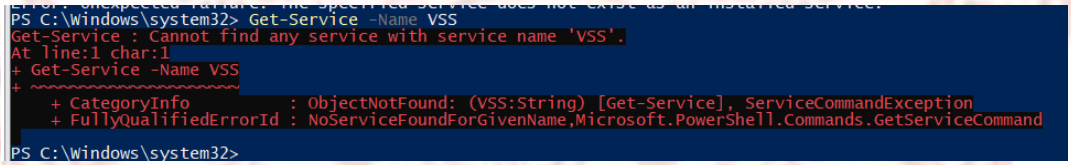
ภาพที่ ก-6 ข้อมูลดิบ MITRE ATT&CK ในระบบ Wazuh



ภาพที่ ก-7 ภาพเว็บไซต์ของหน้าดาวน์โหลดตัวอย่าง Lockbit Ransomware ที่เว็บไซต์ Malware Bazaar



ภาพที่ ก-8 ภาพหน้าจอ Event viewer ที่ log ถูกมัลแวร์ลบ



ภาพที่ ก-9 ภาพหน้าจอ Powershell ที่ใช้คำสั่งค้นหา shadow copy

ประวัติผู้เขียน

ชื่อ นายณัฐพงษ์ รุ่งพรมมา

ชื่อการค้นคว้าอิสระ การวิเคราะห์ทางนิติวิทยาศาสตร์ และการตรวจจับการโจมตีของ LockBit Ransomware โดยใช้บันทึกเหตุการณ์ และเครื่องมือวิเคราะห์เฉพาะทาง

สาขาวิชา การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประวัติ

ประวัติการศึกษา

สำเร็จการศึกษาระดับปริญญาตรี สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา

ประวัติการทำงาน

พ.ศ. 2563 – ปัจจุบัน ทำงานบริษัท โซ ซีเคียว จำกัด ตำแหน่ง Cybersecurity Engineer

สถานที่ติดต่อปัจจุบัน

4/84 ถ.พระรามสอง แสมดำ บางขุนเทียน กทม 10150