การวิเคราะห์แนวโน้มการโจมตีทางไซเบอร์และแนวทางการป้องกันเชิงรุกจากข้อมูลระบบป้องกันแอปพลิเคชันเว็บ

Analysis of Cyberattack Trends and Proactive Defense Approaches Using Web Application Firewall Data

อมร เจือตี๋

Amorn Juatee

สาขาวิชาเทคโนโลยี คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏกาญจนบุรี

Department of Technology, Faculty of Science and Technology, Kanchanaburi Rajabhat University

E-Mail : amorn@kru.ac.th

(Received : November 2, 2024; Revised : December 23, 2025; Accepted : December 24, 2025)

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) วิเคราะห์แนวโน้มและลักษณะของการโจมตีทางไซเบอร์จากข้อมูลเหตุการณ์จริงที่บันทึกโดย ระบบป้องกันแอปพลิเคชันเว็บ (Web Application Firewall: WAF) 2) ประเมินระดับความเสี่ยงและจัดลำดับความสำคัญของ ภัยคุกคามทางไซเบอร์ ที่ส่งผลกระทบต่อระบบแอปพลิเคชันเว็บ และ 3) เสนอแนวทางการป้องกันเชิงรุกที่สอดคล้องกับระดับความเสี่ยงของภัยคุกคาม โดยใช้ข้อมูลบันทึกเหตุการณ์การโจมตีที่ตรวจพบจากระบบป้องกันแอปพลิเคชันเว็บของมหาวิทยาลัยราชภัฏกาญจนบุรี ระหว่างเดือนกันยายนถึงธันวาคม พ.ศ. 2568 ซึ่งครอบคลุมเหตุการณ์การโจมตีจำนวน 40,934 เหตุการณ์ในมิติของประเภทการโจมตี และ 58,777 เหตุการณ์ในมิติของสถานะความมั่นคงปลอดภัยของระบบ การวิเคราะห์ข้อมูลดำเนินการด้วย สถิติเชิงพรรณนา และ การวิเคราะห์แนวโน้ม เพื่อศึกษาความถี่ สัดส่วน ลักษณะของการโจมตี และผลกระทบที่เกิดขึ้นต่อระบบ

ผลการวิจัยพบว่า การโจมตีประเภท การแทรกคำสั่ง SQL (SQL Injection) เป็นรูปแบบที่พบมากที่สุด คิดเป็นร้อยละ 31.42 ของเหตุการณ์ทั้งหมด รองลงมาคือ การอัปโหลดเว็บเชลล์ (WebShell) และ การโจมตีคำสั่งระบบ ขณะที่การวิเคราะห์สถานะความมั่นคงปลอดภัยของระบบพบว่า เหตุการณ์ส่วนใหญ่อยู่ในสถานะ ถูกโจมตี (Attacked) อย่างไรก็ตาม ยังตรวจพบเหตุการณ์ในสถานะ ระบบถูกเจาะ (Compromised) ระบบติดมัลแวร์ (Infected) และ ระบบถูกควบคุมโดยบอต (Bot-controlled) ซึ่งแม้มีจำนวนเหตุการณ์น้อยกว่า แต่ก่อให้เกิดผลกระทบต่อระบบในระดับที่รุนแรงกว่าอย่างมีนัยสำคัญ ผลการศึกษาชี้ให้เห็นว่าการประเมินภัยคุกคามทางไซเบอร์ควรพิจารณาองค์ประกอบหลายมิติร่วมกัน ได้แก่ จำนวนเหตุการณ์ สถานะของการโจมตี จำนวนระบบที่ได้รับผลกระทบ และระดับความรุนแรงของผลกระทบ เพื่อสนับสนุนการกำหนดแนวทางการป้องกันภัยทางไซเบอร์เชิงรุกที่สอดคล้องกับบริบทการใช้งานจริงขององค์กร และยกระดับการบริหารจัดการความมั่นคงปลอดภัยของระบบแอปพลิเคชันเว็บอย่างเป็นระบบและมีประสิทธิภาพ

คำสำคัญ : การโจมตีทางไซเบอร์, การวิเคราะห์แนวโน้ม, ระบบป้องกันแอปพลิเคชันเว็บ, ความมั่นคงปลอดภัยไซเบอร์

ABSTRACT

This study aimed to 1) analyze the trends and characteristics of cyberattacks based on real incident data recorded by a Web Application Firewall (WAF); 2) assess risk levels and prioritize cyber threats affecting web application systems; and 3) propose proactive defense strategies aligned with the assessed risk levels. The dataset consisted of cyberattack logs collected from the WAF deployed at Kanchanaburi Rajabhat University between September and December 2025,

comprising 40,934 attack events categorized by attack type and 58,777 events categorized by system security status. Descriptive statistics and trend analysis were employed to examine attack frequency, distribution, patterns, and their impacts on the system.

The results indicated that SQL injection was the most prevalent attack type, accounting for 31.42% of all incidents, followed by web shell uploads and system command attacks. Analysis of system security status revealed that most events were classified as attacked; however, incidents categorized as compromised, infected, and bot-controlled, although fewer in number, caused substantially more severe impacts on the system. The findings suggest that effective cyber threat assessment should adopt a multidimensional perspective, taking into account the number of incidents, attack status, number of affected systems, and impact severity. Such an approach supports the design of proactive cyber defense strategies that are aligned with the organization's operational context and enhances the systematic and effective management of web application security

Keywords : Cyberattacks, Trend Analysis, Web Application Firewall (WAF), Cybersecurity

บทนำ

ในปัจจุบัน ระบบสารสนเทศและแอปพลิเคชันเว็บมีบทบาทสำคัญต่อการดำเนินงานขององค์กรทั้งภาครัฐและเอกชน โดยเฉพาะสถาบันการศึกษา ซึ่งให้บริการด้านการเรียนการสอน การบริหารจัดการ และการให้บริการข้อมูลผ่านระบบออนไลน์อย่างต่อเนื่อง การพึ่งพาแอปพลิเคชันเว็บในระดับสูงส่งผลให้ระบบดังกล่าวกลายเป็นโครงสร้างพื้นฐานที่มีความสำคัญต่อภารกิจขององค์กร อย่างไรก็ตาม การขยายตัวของการใช้งานแอปพลิเคชันเว็บได้เพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากภัยคุกคามมีความหลากหลายและซับซ้อนมากขึ้น ส่งผลให้ระบบแอปพลิเคชันเว็บตกเป็นเป้าหมายของการโจมตีอย่างต่อเนื่อง [1]

มหาวิทยาลัยฯ ได้นำระบบป้องกันแอปพลิเคชันเว็บมาใช้เพื่อสนับสนุนการตรวจจับและป้องกันการโจมตีในระดับแอปพลิเคชัน อย่างไรก็ตาม จากการใช้งานจริงยังพบเหตุการณ์การโจมตีทางไซเบอร์เกิดขึ้นอย่างต่อเนื่อง ทั้งในรูปแบบของความพยายามโจมตีที่ยังไม่สำเร็จ การเข้าถึงทรัพยากรโดยมิชอบ และเหตุการณ์ที่ส่งผลกระทบต่อระบบในเชิงระบบและการแพร่กระจายภายในเครือข่าย สถานการณ์ดังกล่าวสะท้อนให้เห็นว่าการป้องกันภัยทางไซเบอร์ไม่สามารถพิจารณาเพียงการมีหรือไม่มีระบบป้องกันเท่านั้น แต่จำเป็นต้องอาศัยการวิเคราะห์ข้อมูลเหตุการณ์ที่ตรวจพบจริงจากระบบป้องกัน เพื่อทำความเข้าใจแนวโน้ม ลักษณะ และระดับความเสี่ยงของภัยคุกคาม

จากการทบทวนงานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยส่วนใหญ่มุ่งเน้นการพัฒนาเทคนิคหรือเครื่องมือด้านความมั่นคงปลอดภัยในเชิงเทคนิคเป็นหลัก ขณะที่การนำข้อมูลเหตุการณ์จริงที่บันทึกจากระบบป้องกันแอปพลิเคชันเว็บมาใช้ในการวิเคราะห์แนวโน้มการโจมตี การประเมินระดับความเสี่ยง และการสังเคราะห์แนวทางการป้องกันเชิงรุกที่สอดคล้องกับบริบทการใช้งานจริงขององค์กรยังมีอยู่อย่างจำกัด โดยเฉพาะในสภาพแวดล้อมของสถาบันการศึกษา ส่งผลให้การบริหารจัดการความมั่นคงปลอดภัยของระบบแอปพลิเคชันเว็บยังขาดข้อมูลเชิงประจักษ์ที่สามารถนำมาใช้ประกอบการตัดสินใจเชิงกลยุทธ์ได้อย่างเป็นระบบ

ด้วยเหตุนี้ งานวิจัยนี้จึงมุ่งวิเคราะห์แนวโน้มและลักษณะของการโจมตีทางไซเบอร์จากข้อมูลเหตุการณ์จริงที่บันทึกโดยระบบป้องกันแอปพลิเคชันเว็บ ประเมินระดับความเสี่ยงและจัดลำดับความสำคัญของภัยคุกคาม และนำผลการวิเคราะห์ดังกล่าวมาใช้ในการเสนอแนวทางการป้องกันเชิงรุกที่สอดคล้องกับระดับความเสี่ยงของภัยคุกคาม เพื่อสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยของระบบแอปพลิเคชันเว็บอย่างเป็นระบบและเหมาะสมกับบริบทการใช้งานจริงขององค์กร [2]

1. วัตถุประสงค์การวิจัย

1.1 เพื่อวิเคราะห์แนวโน้มและลักษณะของการโจมตีทางไซเบอร์ โดยอาศัยข้อมูลเหตุการณ์จริงที่บันทึกจากระบบป้องกันแอปพลิเคชันเว็บ

1.2 เพื่อประเมินระดับความเสี่ยงและจัดลำดับความสำคัญของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบแอปพลิเคชันเว็บ

1.3 เพื่อเสนอแนวทางการป้องกันเชิงรุกที่สอดคล้องกับระดับความเสี่ยงของภัยคุกคามจากข้อมูลระบบป้องกันแอปพลิเคชันเว็บ

2. งานวิจัยที่เกี่ยวข้อง

Rathod et al. [3] ศึกษาภัยคุกคามจากการโจมตีแบบสคริปต์ข้ามไซต์ (Cross-Site Scripting: XSS) ซึ่งเป็นช่องโหว่ที่มีความรุนแรงและส่งผลกระทบโดยตรงต่อระบบเว็บแอปพลิเคชัน โดยมุ่งแทรกโค้ดที่เป็นอันตรายเพื่อเข้าถึงข้อมูลสำคัญภายในระบบ งานวิจัยได้ทบทวนรูปแบบการโจมตี XSS อย่างครอบคลุม ได้แก่ Reflected, Persistent, DOM-based, Blind และ Self-XSS พร้อมนำเสนอแนวทางการป้องกัน เช่น การพัฒนาแอปพลิเคชันอย่างปลอดภัย การตรวจสอบข้อมูลนำเข้า การกรองและการเข้ารหัสข้อมูล รวมถึงการประยุกต์ใช้ระบบป้องกันแอปพลิเคชันเว็บ ผลการศึกษาชี้ให้เห็นว่า ช่องโหว่ XSS ยังคงเกิดขึ้นจากการขาดมาตรการด้านความมั่นคงปลอดภัยที่เพียงพอในกระบวนการพัฒนาแอปพลิเคชัน จึงจำเป็นต้องมีการวางแผนความมั่นคงปลอดภัยที่รัดกุมควบคู่กับความเข้าใจเชิงลึกเกี่ยวกับลักษณะของการโจมตี

Babaey & Ravindran [4] ได้นำเสนอกรอบการทำงาน GenXSS เพื่อยกระดับประสิทธิภาพของระบบป้องกันแอปพลิเคชันเว็บในการตรวจจับและบรรเทาการโจมตีแบบสคริปต์ข้ามไซต์ โดยอาศัยปัญญาประดิษฐ์และแบบจำลองภาษาขนาดใหญ่ (Large Language Models: LLMs) งานวิจัยชี้ให้เห็นว่าการขยายตัวของบริการผ่านเว็บส่งผลให้การโจมตี XSS มีความถี่และความซับซ้อนเพิ่มขึ้น ขณะที่ระบบดั้งเดิมยังมีข้อจำกัดจากการพึ่งพาการปรับปรุงกฎด้วยตนเอง กรอบการทำงานดังกล่าวสามารถสร้างและทดสอบเพย์โหลด XSS เพื่อระบุรูปแบบการโจมตีที่หลบเลี่ยงการป้องกันเดิมได้ พร้อมสนับสนุนการสร้างกฎความปลอดภัยใหม่โดยอัตโนมัติ ผลการทดลองโดยใช้ GPT-4o แสดงให้เห็นว่าสามารถสร้างเพย์โหลด XSS ได้ 264 รายการ โดยร้อยละ 83 ผ่านการตรวจสอบความถูกต้อง และการเพิ่มกฎใหม่เพียง 15 กฎ สามารถลดการโจมตีที่เคยสำเร็จได้ถึงร้อยละ 86 ซึ่งสะท้อนศักยภาพของ LLMs ในการเสริมประสิทธิภาพระบบป้องกันแอปพลิเคชันเว็บอย่างมีนัยสำคัญ

Yelkoti [5] ได้นำเสนอการศึกษาที่ชี้ให้เห็นถึงข้อจำกัดของระบบป้องกันแอปพลิเคชันเว็บแบบดั้งเดิมในการรับมือกับการโจมตีที่มุ่งเป้าไปยัง Application Programming Interface (API) ซึ่งมีความซับซ้อน โดยเฉพาะการโจมตีที่เกี่ยวข้องกับช่องโหว่ด้านตรรกะทางธุรกิจและการควบคุมการเข้าถึงข้อมูล งานวิจัยเสนอการประยุกต์ใช้การวิเคราะห์พฤติกรรม (Behavioral Analytics) เพื่อการตรวจจับภัยคุกคามขั้นสูง ผ่านการสร้างรูปแบบการใช้งาน API ที่ถูกต้องและการตรวจจับความเบี่ยงเบนด้วยเทคนิคการเรียนรู้ของเครื่องแบบเรียลไทม์ พร้อมระบบแจ้งเตือนเชิงบริบท นอกจากนี้ แนวทางดังกล่าวยังสนับสนุนการค้นหา API ที่ซ่อนอยู่ การจำแนกการไหลของข้อมูลที่มีความอ่อนไหว การปกป้องข้อมูลระหว่างการรับส่ง และการบูรณาการกับระบบจัดการเหตุการณ์และข้อมูลความมั่นคงปลอดภัย (SIEM) ซึ่งช่วยยกระดับการป้องกัน API จากแนวทางเชิงรับไปสู่การเฝ้าระวังเชิงรุกบนพื้นฐานของพฤติกรรมได้อย่างมีประสิทธิภาพ

Leka et al. [6] ได้นำเสนอแนวทางการพัฒนาระบบป้องกันแอปพลิเคชันเว็บรูปแบบใหม่ โดยผสานเทคโนโลยีการเรียนรู้ของเครื่อง (Machine Learning: ML) และบล็อกเชน เพื่อเพิ่มประสิทธิภาพในการตรวจจับและบรรเทาการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (Distributed Denial of Service: DDoS) ที่อาศัยเครือข่ายบอตเน็ต งานวิจัยชี้ให้เห็นว่าระบบรักษาความมั่นคงปลอดภัยแบบดั้งเดิมมีข้อจำกัดในการรับมือกับการโจมตีที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว โดยกรอบแนวคิดที่เสนอใช้ ML ในการวิเคราะห์พฤติกรรมและตรวจจับความผิดปกติของทราฟฟิก ควบคู่กับการใช้บล็อกเชนเพื่อสนับสนุนการแลกเปลี่ยนข้อมูลภัยคุกคามอย่าง

น่าเชื่อถือ ซึ่งช่วยยกระดับประสิทธิภาพของระบบป้องกันแอปพลิเคชันเว็บและรองรับการพัฒนากลยุทธ์ความมั่นคงปลอดภัยที่สามารถปรับตัวต่อภัยคุกคามในอนาคตได้อย่างเหมาะสม

Annas, Adek & Afrillia [7] ได้นำเสนอการพัฒนาระบบป้องกันแอปพลิเคชันเว็บโดยประยุกต์ใช้ ModSecurity ร่วมกับชุดกฎมาตรฐาน OWASP Core Rule Set เพื่อป้องกันการโจมตีประเภท SQL Injection และ Cross-Site Scripting (XSS) งานวิจัยใช้แบบจำลอง UML ในการวิเคราะห์ระบบและทดสอบประสิทธิภาพกับ Damn Vulnerable Web Application (DVWA) และ WordPress ผลการทดลองพบว่าสามารถตรวจจับการโจมตีแบบ SQL Injection ได้ร้อยละ 100 และ XSS ได้ร้อยละ 99.8 พร้อมรองรับการบันทึกเหตุการณ์การโจมตีแบบเรียลไทม์ ผลการศึกษาชี้ให้เห็นว่าการบูรณาการระบบป้องกันแอปพลิเคชันเว็บเข้ากับกลไกความมั่นคงปลอดภัยของเว็บแอปพลิเคชันช่วยเพิ่มความแข็งแกร่งในการออกแบบระบบและยกระดับความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอย่างต่อเนื่อง

Yaddala & Sunkara [8] ได้นำเสนอการสำรวจเชิงวิชาการเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยของเว็บในปี ค.ศ. 2024 โดยครอบคลุมทั้งช่องโหว่แบบดั้งเดิมและความเสี่ยงรูปแบบใหม่จากวิวัฒนาการของเทคโนโลยีและกลยุทธ์การโจมตีที่ซับซ้อนขึ้น งานวิจัยวิเคราะห์ภัยคุกคามในระดับแอปพลิเคชัน เครือข่าย และด้านความเป็นส่วนตัวของข้อมูล โดยอาศัยข้อมูลจากรายงานอุตสาหกรรม งานวิจัยทางวิชาการ และมาตรฐานจากองค์กรชั้นนำ ผลการศึกษาชี้ให้เห็นถึงความจำเป็นของการใช้กลไกการป้องกันเชิงรุกและการตรวจจับภัยคุกคามอย่างมีประสิทธิภาพ เพื่อปกป้องทรัพยากรบนเว็บ และทำหน้าที่เป็นแหล่งอ้างอิงสำคัญสำหรับการพัฒนามาตรการรับมือภัยคุกคามในปัจจุบัน

วิธีดำเนินการวิจัย

1. เครื่องมือในการวิจัย

การวิจัยนี้ใช้เครื่องมือในการเก็บรวบรวม วิเคราะห์ และสรุปผลข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นกับระบบแอปพลิเคชันเว็บขององค์กร โดยเครื่องมือที่ใช้ในการวิจัยสามารถจำแนกออกเป็น 3 ประเภทหลัก ดังนี้

1. ระบบป้องกันแอปพลิเคชันเว็บ ผู้วิจัยใช้ระบบป้องกันแอปพลิเคชันเว็บ ซึ่งติดตั้งและใช้งาน ณ ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี เป็นแหล่งข้อมูลหลักในการเก็บรวบรวมบันทึกเหตุการณ์การโจมตีทางไซเบอร์ในระดับแอปพลิเคชันเว็บ โดยทำการดึงข้อมูลเหตุการณ์ที่ระบบตรวจจับและบันทึกไว้ในช่วงเวลาที่กำหนดในการศึกษา ข้อมูลดังกล่าวครอบคลุมเหตุการณ์การโจมตีหลายประเภท ทั้งการโจมตีในระดับแอปพลิเคชันและความผิดปกติของการร้องขอข้อมูล [7], [9], [10]

2. เครื่องมือวิเคราะห์ข้อมูล หลังการเก็บรวบรวมข้อมูลเหตุการณ์การโจมตีทางไซเบอร์จากระบบป้องกันแอปพลิเคชันเว็บ ผู้วิจัยได้ตรวจสอบ คัดกรอง และจัดระเบียบข้อมูลเพื่อเตรียมความพร้อมสำหรับการวิเคราะห์เชิงพรรณนา โดยใช้เครื่องมือวิเคราะห์ภายในระบบป้องกันแอปพลิเคชันเว็บร่วมกับโปรแกรมไมโครซอฟท์ เอ็กเซลในการจัดกลุ่มข้อมูลและคำนวณสถิติเชิงพรรณนา ได้แก่ ความถี่ ร้อยละ และค่าเฉลี่ย พร้อมสรุปผลในรูปแบบตารางเพื่อแสดงลักษณะและแนวโน้มของเหตุการณ์การโจมตีทางไซเบอร์อย่างเป็นระบบ โปร่งใส และสามารถตรวจสอบได้ ทั้งนี้ การวิเคราะห์ดังกล่าวสอดคล้องกับวัตถุประสงค์ของการวิจัยที่มุ่งใช้ข้อมูลเชิงประจักษ์จากเหตุการณ์จริงที่ตรวจพบโดยระบบป้องกันแอปพลิเคชันเว็บ

3. ระบบรายงานความปลอดภัย ผู้วิจัยใช้ข้อมูลจากรายงานความมั่นคงปลอดภัยเป็นเครื่องมือสนับสนุนในการรวบรวมและสรุปข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่บันทึกโดยระบบป้องกันแอปพลิเคชันเว็บ โดยนำข้อมูลมาใช้ในการวิเคราะห์ภาพรวมสถานการณ์ภัยคุกคาม สัดส่วนและแนวโน้มของการโจมตีในแต่ละประเภท รวมถึงการเปรียบเทียบข้อมูลตามช่วงเวลา ทั้งนี้ ข้อมูลดังกล่าวถูกใช้ประกอบการวิเคราะห์เชิงพรรณนาและเป็นฐานข้อมูลสำคัญในการสังเคราะห์แนวทางการป้องกันภัยทางไซเบอร์เชิงรุกให้สอดคล้องกับบริบทการใช้งานจริงขององค์กร [11]

2. กลุ่มเป้าหมาย

กลุ่มเป้าหมายของการวิจัยครั้งนี้ คือ ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นกับระบบแอปพลิเคชันเว็บของศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี ซึ่งถูกบันทึกโดยระบบป้องกันแอปพลิเคชันเว็บ ข้อมูลดังกล่าวเป็นข้อมูลเชิงประจักษ์จากการให้บริการแอปพลิเคชันเว็บและไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้ใช้งาน ผู้วิจัยได้คัดเลือกข้อมูลเหตุการณ์ที่ตรวจจับได้ในช่วงเวลาที่กำหนด เพื่อนำมาวิเคราะห์แนวโน้ม ลักษณะ และประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบแอปพลิเคชันเว็บตามวัตถุประสงค์ของการวิจัย

3. ขั้นตอนการดำเนินการวิจัย

การวิจัยครั้งนี้ดำเนินการอย่างเป็นระบบ โดยมุ่งวิเคราะห์ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นจริงกับระบบแอปพลิเคชันเว็บของสถาบันการศึกษา เพื่อวิเคราะห์แนวโน้มและลักษณะของการโจมตี ประเมินระดับความเสี่ยงของภัยคุกคาม และสังเคราะห์แนวทางการป้องกันเชิงรุกที่สอดคล้องกับบริบทการใช้งานจริงขององค์กร โดยมีขั้นตอนการดำเนินการวิจัยดังนี้

ขั้นตอนที่ 1 การเก็บรวบรวมข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ ผู้วิจัยเก็บรวบรวมข้อมูลเหตุการณ์การโจมตีทางไซเบอร์จากระบบป้องกันแอปพลิเคชันเว็บ โดยใช้ข้อมูลบันทึกเหตุการณ์การโจมตีและความผิดปกติของการร้องขอข้อมูลในระดับแอปพลิเคชันเว็บที่ระบบตรวจจับได้ในช่วงวันที่ 1 กันยายน ถึง 20 ธันวาคม พ.ศ. 2568 ข้อมูลดังกล่าวถูกรวบรวมและสรุปในรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบป้องกันแอปพลิเคชันเว็บ ซึ่งเป็นข้อมูลเชิงประจักษ์ที่สะท้อนสถานการณ์ภัยคุกคามที่เกิดขึ้นจริง และถูกใช้เป็นแหล่งข้อมูลหลักในการดำเนินการวิจัยครั้งนี้

ขั้นตอนที่ 2 การตรวจสอบความถูกต้องและการจัดระเบียบข้อมูล หลังการเก็บรวบรวมข้อมูลเหตุการณ์การโจมตีทางไซเบอร์จากระบบป้องกันแอปพลิเคชันเว็บ ผู้วิจัยได้ตรวจสอบความครบถ้วนและความถูกต้องของข้อมูล โดยพิจารณาความสมบูรณ์ของรายการข้อมูล ความซ้ำซ้อนของเหตุการณ์ และความสอดคล้องของรูปแบบข้อมูล จากนั้นจึงคัดกรองเหตุการณ์ที่มีข้อมูลไม่ครบถ้วนหรือซ้ำซ้อนออก และจัดเตรียมข้อมูลให้อยู่ในรูปแบบมาตรฐานเดียวกัน พร้อมจัดหมวดหมู่เหตุการณ์ตามประเภทการโจมตี เพื่อให้ข้อมูลมีความเป็นระบบและพร้อมสำหรับการวิเคราะห์เชิงพรรณนาในขั้นตอนถัดไป

ขั้นตอนที่ 3 การวิเคราะห์แนวโน้มและลักษณะของการโจมตีทางไซเบอร์ ผู้วิจัยนำข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่ผ่านการตรวจสอบและจัดระเบียบแล้วมาดำเนินการวิเคราะห์เชิงพรรณนา โดยศึกษาความถี่ สัดส่วน และลักษณะของการโจมตีในแต่ละประเภท รวมถึงการเปลี่ยนแปลงของจำนวนเหตุการณ์ตามช่วงเวลาที่ศึกษา เพื่อสะท้อนรูปแบบและพฤติกรรมของการโจมตีที่เกิดขึ้นจริงกับระบบแอปพลิเคชันเว็บ ผลการวิเคราะห์ดังกล่าวถูกใช้เป็นข้อมูลพื้นฐานในการทำความเข้าใจภัยคุกคาม และเป็นฐานข้อมูลเชิงประจักษ์สำหรับการประเมินระดับความเสี่ยงและการจัดลำดับความสำคัญของภัยคุกคามในขั้นตอนถัดไป

ขั้นตอนที่ 4 การประเมินความเสี่ยงและการจัดลำดับความสำคัญของภัยคุกคาม จากผลการวิเคราะห์ลักษณะและรูปแบบของการโจมตีทางไซเบอร์ในขั้นตอนก่อนหน้า ผู้วิจัยดำเนินการประเมินระดับความเสี่ยงของภัยคุกคามโดยอาศัยข้อมูลเหตุการณ์จริงจากระบบป้องกันแอปพลิเคชันเว็บ โดยพิจารณาความถี่ ประเภทการโจมตี และระดับผลกระทบที่เกิดขึ้นหรืออาจเกิดขึ้นต่อระบบแอปพลิเคชันเว็บ ผลการประเมินถูกนำมาใช้ในการจัดลำดับความสำคัญของภัยคุกคาม เพื่อระบุภัยคุกคามที่มีความเสี่ยงสูงและควรได้รับการจัดการในลำดับเร่งด่วน ทั้งนี้ เพื่อสนับสนุนการกำหนดแนวทางการป้องกันเชิงรุกที่สอดคล้องกับระดับความเสี่ยงและบริบทการใช้งานจริงขององค์กร

ขั้นตอนที่ 5 การสังเคราะห์แนวทางการป้องกันภัยทางไซเบอร์เชิงรุก ผู้วิจัยนำผลการวิเคราะห์แนวโน้มการโจมตีและการประเมินระดับความเสี่ยงจากข้อมูลระบบป้องกันแอปพลิเคชันเว็บ มาสังเคราะห์เป็นแนวทางการป้องกันเชิงรุก โดยเชื่อมโยงลักษณะเหตุการณ์ สถานะการโจมตี และระดับผลกระทบกับการกำหนดมาตรการป้องกันที่เหมาะสมในระดับแอปพลิเคชันเว็บ แนวทางดังกล่าวครอบคลุมการจัดลำดับความสำคัญของมาตรการตาม

ระดับความเสี่ยง การปรับปรุงนโยบายและการตั้งค่าด้านความมั่นคงปลอดภัย ตลอดจนการวางแผนเฝ้าระวังและการรับมือเหตุการณ์อย่างเป็นระบบ เพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับบริบทการใช้งานจริงขององค์กร

4. สถิติที่ใช้งานการวิจัย

การวิจัยครั้งนี้ใช้สถิติเชิงพรรณนาในการวิเคราะห์ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่บันทึกโดยระบบป้องกันแอปพลิเคชันเว็บ ซึ่งเป็นข้อมูลเหตุการณ์จริงในช่วงเวลาที่ศึกษา โดยมีวัตถุประสงค์เพื่ออธิบายลักษณะ แนวโน้ม และรูปแบบของการโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อระบบแอปพลิเคชันเว็บ ทั้งนี้ สถิติที่ใช้ในการวิเคราะห์สามารถสรุปรายละเอียดได้ดังต่อไปนี้

4.1 ค่าความถี่ ใช้ในการนับจำนวนเหตุการณ์การโจมตีทางไซเบอร์ในแต่ละประเภท เพื่อแสดงความถี่ของรูปแบบการโจมตีที่ตรวจพบ และสะท้อนแนวโน้มของภัยคุกคามที่ส่งผลกระทบต่อระบบแอปพลิเคชันเว็บในช่วงเวลาที่ศึกษา

4.2 ค่าร้อยละ ใช้ในการแสดงสัดส่วนของเหตุการณ์การโจมตีในแต่ละประเภทเมื่อเปรียบเทียบกับจำนวนเหตุการณ์ทั้งหมดที่ตรวจพบในช่วงเวลาที่ศึกษา เพื่อเปรียบเทียบระดับความสำคัญและความรุนแรงเชิงปริมาณของภัยคุกคามแต่ละประเภท

4.3 การวิเคราะห์แนวโน้มตามช่วงเวลา ใช้ในการวิเคราะห์การเปลี่ยนแปลงของจำนวนเหตุการณ์การโจมตีทางไซเบอร์ตามช่วงเวลาที่ปรากฏในรายงานของระบบป้องกันแอปพลิเคชันเว็บ เพื่อแสดงรูปแบบการเพิ่มขึ้นหรือลดลงของเหตุการณ์การโจมตี และอธิบายพฤติกรรมของภัยคุกคามที่เกิดขึ้นจริงกับระบบแอปพลิเคชันเว็บในช่วงเวลาที่ศึกษา

4.4 การจัดอันดับภัยคุกคาม ใช้ในการจัดลำดับความสำคัญของภัยคุกคามทางไซเบอร์ โดยอาศัยข้อมูลความถี่และสัดส่วนของเหตุการณ์การโจมตีในแต่ละประเภทที่ตรวจพบจากระบบป้องกันแอปพลิเคชันเว็บ เพื่อสนับสนุนการประเมินระดับความเสี่ยงของภัยคุกคาม และเป็นข้อมูลประกอบในการเสนอแนวทางการป้องกันเชิงรุกให้สอดคล้องกับระดับความสำคัญของภัยคุกคามที่เกิดขึ้น

4.5 ค่าเฉลี่ยต่อช่วงเวลา หมายถึง จำนวนเหตุการณ์การโจมตีทางไซเบอร์เฉลี่ยที่ตรวจพบในหนึ่งช่วงเวลาการรายงาน โดยคำนวณจากจำนวนเหตุการณ์ทั้งหมดหารด้วยจำนวนช่วงเวลาที่ใช้ในการวิเคราะห์ ทั้งนี้ ค่าเฉลี่ยดังกล่าวใช้เพื่อสะท้อนความถี่ของการโจมตีในเชิงเวลา และสนับสนุนการเปรียบเทียบความเข้มข้นของภัยคุกคามระหว่างประเภทการโจมตีต่าง ๆ

ผลการวิจัย

ผลการวิจัยในส่วนนี้นำเสนอผลการวิเคราะห์ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่บันทึกโดยระบบป้องกันแอปพลิเคชันเว็บในช่วงเวลาที่ศึกษา โดยมุ่งสะท้อนภาพรวมของแนวโน้ม ลักษณะ และรูปแบบของการโจมตีที่เกิดขึ้นจริงกับระบบแอปพลิเคชันเว็บขององค์กร เพื่อสนับสนุนการวิเคราะห์เชิงสถิติและการแปลผลตามวัตถุประสงค์การวิจัย ดังนี้

1. ผลการวิเคราะห์แนวโน้มและลักษณะของการโจมตีทางไซเบอร์ โดยอาศัยข้อมูลเหตุการณ์จริงที่บันทึกจากระบบป้องกันแอปพลิเคชันเว็บ

จากการวิเคราะห์ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่ตรวจพบโดยระบบป้องกันแอปพลิเคชันเว็บในช่วงเวลาที่ศึกษา พบว่าเหตุการณ์การโจมตีมีความหลากหลายทั้งในด้านรูปแบบและระดับผลกระทบต่อระบบแอปพลิเคชันเว็บ เพื่อสะท้อนภาพรวมของลักษณะการโจมตีที่เกิดขึ้นจริง งานวิจัยนี้นำเสนอผลการวิเคราะห์เชิงพรรณนาโดยจำแนกเหตุการณ์ตามประเภทการโจมตี พร้อมแสดงจำนวนเหตุการณ์ สัดส่วนร้อยละ ค่าเฉลี่ยต่อช่วงเวลา และสถานะของระบบที่ตรวจพบการโจมตี ดังแสดงในตารางที่ 1

ตารางที่ 1 แนวโน้มและลักษณะการโจมตีทางไซเบอร์จากระบบป้องกันแอปพลิเคชันเว็บ

ประเภทการโจมตี	จำนวนเหตุการณ์	สัดส่วน (%)	ค่าเฉลี่ยต่อช่วงเวลา	ระบบที่ได้รับผลกระทบ	สถานะระบบ
SQL Injection	12,845	31.42	642.25	12	ถูกโจมตี (Attacked) / ถูกบุกรุก (Compromised)
WebShell Upload	9,376	22.93	468.80	9	ถูกโจมตี (Attacked) / ถูกบุกรุก (Compromised)
OS Command Injection	7,214	17.65	360.70	7	ถูกโจมตี (Attacked)
Brute-force Login	5,083	12.43	254.15	6	ถูกโจมตี (Attacked)
Information Disclosure	3,964	9.69	198.20	5	ถูกโจมตี (Attacked)
File Inclusion / Path Traversal	1,452	3.55	72.60	2	ถูกโจมตี (Attacked)

จากตารางที่ 1 แสดงผลการวิเคราะห์แนวโน้มและลักษณะการโจมตีทางไซเบอร์ที่ตรวจพบจากระบบป้องกันแอปพลิเคชันเว็บในช่วงเวลาที่ทำการศึกษา พบว่า ตรวจพบเหตุการณ์การโจมตีทางไซเบอร์รวมทั้งสิ้น 40,934 ครั้ง โดยการโจมตีประเภท SQL Injection มีจำนวนเหตุการณ์สูงที่สุด จำนวน 12,845 ครั้ง คิดเป็นร้อยละ 31.42 ของเหตุการณ์ทั้งหมด และตรวจพบระบบที่ได้รับผลกระทบจำนวน 12 ระบบ ในสถานะถูกโจมตี (Attacked) และถูกบุกรุก (Compromised) สะท้อนให้เห็นว่าการโจมตีที่มุ่งเป้าไปยังชั้นการจัดการข้อมูลและฐานข้อมูลยังคงเป็นภัยคุกคามที่มีความสำคัญต่อระบบแอปพลิเคชันเว็บ

รองลงมาคือการโจมตีประเภท WebShell Upload และ OS Command Injection ซึ่งพบจำนวนเหตุการณ์ 9,376 ครั้ง (ร้อยละ 22.93) และ 7,214 ครั้ง (ร้อยละ 17.65) ตามลำดับ โดยตรวจพบระบบที่ได้รับผลกระทบจำนวน 9 ระบบ และ 7 ระบบตามลำดับ ทั้งสองประเภทเป็นการโจมตีที่เกี่ยวข้องกับการควบคุมสิทธิ์และการสั่งงานระบบผ่านช่องโหว่ของแอปพลิเคชันเว็บ ซึ่งสะท้อนถึงความเสี่ยงเชิงโครงสร้างในระดับแอปพลิเคชัน

สำหรับการโจมตีประเภท Brute-force Login และ Information Disclosure พบจำนวนเหตุการณ์ 5,083 ครั้ง (ร้อยละ 12.43) และ 3,964 ครั้ง (ร้อยละ 9.69) ตามลำดับ โดยเหตุการณ์ส่วนใหญ่อยู่ในสถานะถูกโจมตี (Attacked) แม้ยังไม่ส่งผลให้เกิดการบุกรุกระบบสำเร็จ แต่สะท้อนถึงความพยายามในการเข้าถึงบัญชีผู้ใช้งานและข้อมูลภายในระบบอย่างต่อเนื่อง ขณะที่การโจมตีประเภท File Inclusion / Path Traversal พบในสัดส่วนต่ำที่สุด จำนวน 1,452 ครั้ง (ร้อยละ 3.55) และตรวจพบระบบที่ได้รับผลกระทบเพียง 2 ระบบ

โดยภาพรวม ผลการวิเคราะห์ชี้ให้เห็นว่าเหตุการณ์การโจมตีทางไซเบอร์ส่วนใหญ่เป็นการโจมตีซ้ำต่อระบบแอปพลิเคชันเว็บเดิม และมุ่งเป้าไปยังช่องโหว่ในระดับแอปพลิเคชันเป็นหลัก แม้เหตุการณ์ส่วนใหญ่อยู่ในสถานะถูกโจมตี แต่ยังตรวจพบระบบบางส่วนอยู่ในสถานะถูกบุกรุก (Compromised) ในบางประเภทการโจมตี ซึ่งข้อมูลเชิงประจักษ์ดังกล่าวสามารถนำไปใช้เป็นฐานในการประเมินระดับความเสี่ยงและการจัดลำดับความสำคัญของภัยคุกคามในขั้นตอนการวิเคราะห์ถัดไป

ตารางที่ 2 การวิเคราะห์สถานะการโจมตี ความรุนแรง และระดับความเสี่ยงของภัยคุกคามทางไซเบอร์

สถานะการโจมตี	จำนวนเหตุการณ์	ระบบที่ได้รับผลกระทบ	ระดับความรุนแรง	ระดับความเสี่ยง	แนวทางการจัดการเชิงรุก
ถูกโจมตี (Attacked)	39,862	18	ปานกลาง	ปานกลาง	เพิ่มประสิทธิภาพการเฝ้าระวัง (Enhanced Monitoring)
ถูกบุกรุก (Compromised)	7,945	6	สูง	สูง	การอุดช่องโหว่และเสริมความมั่นคงของระบบ (Patch & Hardening)
ติดมัลแวร์ (Infected)	8,124	82	สูง	สูง	การป้องกันอุปกรณ์ปลายทางและการแบ่งส่วนเครือข่าย (Endpoint Protection & Segmentation)
ถูกควบคุมโดยบอต (Bot-controlled)	2,846	5	สูงมาก	สูงมาก	การบรรเทาการโจมตีจากบอต (Bot Mitigation)

จากตารางที่ 2 พบว่า ระบบป้องกันแอปพลิเคชันเว็บตรวจพบเหตุการณ์การโจมตีทางไซเบอร์ รวมทั้งสิ้น 58,777 ครั้ง โดยเหตุการณ์ส่วนใหญ่อยู่ในสถานะถูกโจมตี (Attacked) จำนวน 39,862 ครั้ง และตรวจพบระบบที่ได้รับผลกระทบจำนวน 18 ระบบ ซึ่งถูกประเมินให้อยู่ในระดับความรุนแรงและระดับความเสี่ยงโดยรวมในระดับปานกลาง สะท้อนให้เห็นว่าเหตุการณ์ส่วนใหญ่เป็นความพยายามโจมตีที่ยังไม่ส่งผลให้เกิดการบุกรุกระบบสำเร็จ อย่างไรก็ตาม การเกิดเหตุการณ์ในลักษณะดังกล่าวอย่างต่อเนื่องบ่งชี้ถึงความจำเป็นในการเสริมการเฝ้าระวังและการตรวจจับภัยคุกคามอย่างสม่ำเสมอ

ในขณะเดียวกัน เหตุการณ์ในสถานะถูกบุกรุก (Compromised) พบจำนวน 7,945 ครั้ง และส่งผลกระทบต่อระบบจำนวน 6 ระบบ โดยถูกจัดอยู่ในระดับความรุนแรงและระดับความเสี่ยงในระดับสูง แสดงให้เห็นว่าการโจมตีบางส่วนสามารถส่งผลต่อความถูกต้องของระบบหรือก่อให้เกิดการเข้าถึงทรัพยากรโดยมิชอบได้จริง สถานะดังกล่าวสะท้อนถึงความเสี่ยงด้านการละเมิดสิทธิ์และความมั่นคงปลอดภัยของข้อมูลในระดับระบบแอปพลิเคชันเว็บ

สำหรับเหตุการณ์ในสถานะติดมัลแวร์ (Infected) พบจำนวน 8,124 ครั้ง และกระทบต่อระบบปลายทางจำนวนมากถึง 82 ระบบ ซึ่งถูกประเมินให้อยู่ในระดับความรุนแรงและระดับความเสี่ยงในระดับสูง ผลการวิเคราะห์สะท้อนถึงความเสี่ยงในการแพร่กระจายของมัลแวร์ภายในเครือข่ายองค์กร และความเป็นไปได้ในการขยายขอบเขตของผลกระทบจากระบบหนึ่งไปยังระบบอื่น

นอกจากนี้ เหตุการณ์ในสถานะถูกควบคุมโดยบอต (Bot-controlled) แม้จะมีจำนวนเหตุการณ์เพียง 2,846 ครั้ง และกระทบต่อระบบจำนวน 5 ระบบ แต่ถูกจัดอยู่ในระดับความรุนแรงและระดับความเสี่ยงในระดับสูงมาก เนื่องจากระบบในสถานะดังกล่าวมีศักยภาพในการถูกควบคุมจากภายนอก และอาจถูกนำไปใช้เป็นฐานสำหรับการโจมตีต่อเนื่องทั้งภายในและภายนอกองค์กร

โดยสรุป ผลการวิเคราะห์ชี้ให้เห็นว่าเหตุการณ์การโจมตีทางไซเบอร์ที่ตรวจพบมีความแตกต่างกันอย่างชัดเจนทั้งในด้านสถานะการโจมตี ระดับความรุนแรง และระดับความเสี่ยง ข้อมูลเชิงประจักษ์ดังกล่าวสามารถนำไปใช้เป็นฐานในการจัดลำดับความสำคัญของภัยคุกคาม และสนับสนุนการกำหนดแนวทางการป้องกันเชิงรุกที่สอดคล้องกับระดับความเสี่ยงของภัยคุกคามในขั้นตอนการวิจัยถัดไป

2. ผลการประเมินระดับความเสี่ยงและจัดลำดับความสำคัญของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบแอปพลิเคชันเว็บ

เพื่อแสดงภาพรวมของแนวโน้มและลักษณะภัยคุกคามทางไซเบอร์ในเชิงระบบ ผู้วิจัยได้สรุปผลการวิเคราะห์โดยพิจารณาจากสถานะการโจมตี จำนวนและสัดส่วนของเหตุการณ์ จำนวนระบบที่ได้รับผลกระทบ และระดับความรุนแรงของผลกระทบที่ตรวจพบ ดังแสดงในตารางที่ 3

ตารางที่ 3 การสรุปการประเมินระดับความเสี่ยงและการจัดลำดับความสำคัญของภัยคุกคามทางไซเบอร์

สถานะภัยคุกคาม	จำนวนเหตุการณ์	สัดส่วน (%)	ระบบที่ได้รับผลกระทบ	ระดับความรุนแรง	ลักษณะผลกระทบเชิงระบบ
ถูกควบคุมโดยบอต (Bot-controlled)	2,846	4.84	5	สูงมาก	การควบคุมระบบจากภายนอกและใช้เป็นฐานในการโจมตี
ติดมัลแวร์ (Infected)	8,124	13.82	82	สูง	การแพร่กระจายของมัลแวร์ภายในเครือข่าย
ถูกบุกรุก (Compromised)	7,945	13.51	6	สูง	การบุกรุกหรือการเข้าถึงทรัพยากรโดยมิชอบ
ถูกโจมตี (Attacked)	39,862	67.83	18	ปานกลาง	ความพยายามโจมตีที่ยังไม่ประสบผลสำเร็จ

จากตารางที่ 3 ผลการวิเคราะห์พบว่า เหตุการณ์ในสถานะถูกควบคุมโดยบอต (Bot-Controlled) มีจำนวน 2,846 ครั้ง และส่งผลกระทบต่อระบบจำนวน 5 ระบบ โดยถูกจัดอยู่ในระดับความรุนแรงสูงมาก สะท้อนถึงศักยภาพในการควบคุมระบบจากภายนอกและการถูกใช้เป็นฐานในการโจมตีต่อเนื่อง แม้จำนวนเหตุการณ์และระบบที่ได้รับผลกระทบจะไม่สูงเมื่อเทียบกับสถานะอื่น แต่ลักษณะผลกระทบในเชิงระบบมีความรุนแรงอย่างชัดเจน

ในขณะเดียวกัน เหตุการณ์ในสถานะติดมัลแวร์ (Infected) พบจำนวน 8,124 ครั้ง และส่งผลกระทบต่อระบบปลายทางจำนวนมากถึง 82 ระบบ โดยถูกจัดอยู่ในระดับความรุนแรงสูง ผลการวิเคราะห์สะท้อนถึงความเสี่ยงในการแพร่กระจายของมัลแวร์ภายในเครือข่ายองค์กร และความเป็นไปได้ในการขยายขอบเขตของผลกระทบในระดับโครงสร้างระบบ

สำหรับเหตุการณ์ในสถานะถูกบุกรุก (Compromised) พบจำนวน 7,945 ครั้ง และส่งผลกระทบต่อระบบจำนวน 6 ระบบ ซึ่งแม้จำนวนระบบที่ได้รับผลกระทบจะน้อยกว่าเหตุการณ์ในสถานะติดมัลแวร์ แต่สะท้อนถึงการบุกรุกระบบหรือการเข้าถึงทรัพยากรโดยมิชอบที่มีนัยสำคัญต่อความมั่นคงปลอดภัยของระบบแอปพลิเคชันเว็บ

ขณะที่เหตุการณ์ในสถานะถูกโจมตี (Attacked) พบจำนวนเหตุการณ์สูงที่สุด คือ 39,862 ครั้ง และส่งผลกระทบต่อระบบจำนวน 18 ระบบ โดยถูกจัดอยู่ในระดับความรุนแรงปานกลาง เนื่องจากเหตุการณ์ส่วนใหญ่เป็นความพยายามโจมตีที่ยังไม่ส่งผลให้เกิดการบุกรุกระบบสำเร็จ อย่างไรก็ตาม ความถี่ของเหตุการณ์ที่ตรวจพบสะท้อนถึงรูปแบบการโจมตีที่เกิดขึ้นอย่างต่อเนื่องในช่วงเวลาที่ศึกษา

โดยสรุป ผลการวิเคราะห์ชี้ให้เห็นว่าภัยคุกคามทางไซเบอร์ที่ตรวจพบมีความแตกต่างกันอย่างชัดเจนทั้งในด้านจำนวนเหตุการณ์ จำนวนระบบที่ได้รับผลกระทบ และระดับความรุนแรงของผลกระทบ ข้อมูลเชิงประจักษ์ดังกล่าวสามารถนำไปใช้เป็นฐานในการจัดลำดับความสำคัญของภัยคุกคาม และรองรับการสังเคราะห์แนวทางการป้องกันเชิงรุกในขั้นตอนถัดไปของการวิจัย

3. แนวทางการป้องกันเชิงรุกที่สอดคล้องกับระดับความเสี่ยงของภัยคุกคามจากข้อมูลระบบป้องกันแอปพลิเคชันเว็บ

เพื่อเชื่อมโยงผลการวิเคราะห์สถานะการโจมตีและระดับผลกระทบของภัยคุกคามทางไซเบอร์ไปสู่การกำหนดแนวทางการป้องกันเชิงรุก ผู้วิจัยได้สังเคราะห์ข้อมูลเชิงประจักษ์จากระบบป้องกันแอปพลิเคชันเว็บ

โดยพิจารณาจากลักษณะเหตุการณ์ ระดับผลกระทบเชิงระบบ และประเด็นความเสี่ยงที่ตรวจพบ เพื่อนำเสนอแนวทางการป้องกันที่เหมาะสมและสอดคล้องกับระดับความเสี่ยงของภัยคุกคามในแต่ละสถานะ ดังแสดงในตารางที่ 4

ตารางที่ 4 การสังเคราะห์แนวทางการป้องกันเชิงรุกตามสถานะภัยคุกคามและระดับความเสี่ยง

สถานะภัยคุกคาม	ข้อมูลเชิงประจักษ์จากระบบป้องกันแอปพลิเคชันเว็บ	ลักษณะความเสี่ยงเชิงระบบ	ระดับการตอบสนองเชิงรุก	แนวทางการป้องกันเชิงรุกที่เสนอ
ถูกโจมตี (Attacked)	ตรวจพบเหตุการณ์จำนวนมาก (39,862 ครั้ง) ส่วนใหญ่ยังไม่บุกรุกสำเร็จ	ความเสี่ยงจากการโจมตีซ้ำและความถี่สูง	การเฝ้าระวังเชิงรุก	ปรับกฎตรวจจับและวิเคราะห์ทราฟฟิกอย่างต่อเนื่อง
ถูกบุกรุก (Compromised)	ตรวจพบการเข้าถึงโดยมิชอบ 7,945 เหตุการณ์ กระทบระบบจำกัด	ความเสี่ยงจากการละเมิดสิทธิ์และข้อมูล	การควบคุมและจำกัดผลกระทบ	เสริมการควบคุมสิทธิ์และการยืนยันตัวตน
ติดมัลแวร์ (Infected)	ตรวจพบ 8,124 เหตุการณ์ กระทบระบบปลายทางจำนวนมาก	ความเสี่ยงจากการแพร่กระจายภายในเครือข่าย	การป้องกันและจำกัดการแพร่กระจาย	เสริมการป้องกันปลายทางและแบ่งส่วนเครือข่าย
ถูกควบคุมโดยบอต (Bot-controlled)	ตรวจพบ 2,846 เหตุการณ์ มีศักยภาพควบคุมจากภายนอก	ความเสี่ยงเชิงระบบระดับสูงมาก	การตอบสนองอย่างเร่งด่วน	บล็อกทราฟฟิกและเสริมการป้องกันบอต

ตารางที่ 4 แสดงผลการสังเคราะห์แนวทางการป้องกันเชิงรุก โดยเชื่อมโยงข้อมูลเชิงประจักษ์จากระบบป้องกันแอปพลิเคชันเว็บเข้ากับสถานะภัยคุกคามและระดับความเสี่ยงเชิงระบบ ผลการวิเคราะห์ชี้ให้เห็นว่าสถานะภัยคุกคามแต่ละประเภทมีลักษณะความเสี่ยงและระดับการตอบสนองที่เหมาะสมแตกต่างกันอย่างชัดเจน สะท้อนถึงความจำเป็นในการกำหนดแนวทางการป้องกันที่สอดคล้องกับระดับความเสี่ยงที่ตรวจพบจริง

สถานะถูกโจมตี (Attacked) ตรวจพบเหตุการณ์ในสัดส่วนสูงสุด โดยส่วนใหญ่ยังไม่ส่งผลให้เกิดการบุกรุกระบบสำเร็จ อย่างไรก็ตาม ความถี่และการเกิดซ้ำของเหตุการณ์ก่อให้เกิดความเสี่ยงเชิงสะสมในระยะยาว แนวทางการตอบสนองที่เหมาะสมจึงควรมุ่งเน้นการเฝ้าระวังเชิงรุก ผ่านการปรับปรุงกฎการตรวจจับ การเพิ่มประสิทธิภาพของกลไกการตรวจจับ และการวิเคราะห์ทราฟฟิกอย่างต่อเนื่อง เพื่อป้องกันการยกระดับของเหตุการณ์ไปสู่ระดับที่มีความรุนแรงมากขึ้น

ในกรณีของสถานะถูกบุกรุก (Compromised) ซึ่งสะท้อนถึงการเข้าถึงทรัพยากรโดยมิชอบ แม้จะส่งผลกระทบต่อระบบในวงจำกัด แต่มีความเสี่ยงสูงต่อความถูกต้องและความลับของข้อมูล แนวทางการตอบสนองที่เหมาะสมจึงควรอยู่ในรูปแบบของการควบคุมและจำกัดผลกระทบ โดยเน้นการเสริมมาตรการควบคุมสิทธิ์การเข้าถึง การปรับปรุงกระบวนการยืนยันตัวตน และการตรวจสอบกิจกรรมของผู้ใช้งานอย่างเป็นระบบ

สำหรับสถานะติดมัลแวร์ (Infected) พบว่ามีผลกระทบต่อระบบปลายทางในวงกว้าง สะท้อนถึงความเสี่ยงในการแพร่กระจายของมัลแวร์ภายในเครือข่ายและการขยายขอบเขตของผลกระทบเชิงระบบ แนวทางการตอบสนองที่เหมาะสมจึงควรมุ่งเน้นการป้องกันและจำกัดการแพร่กระจาย ผ่านการเสริมมาตรการป้องกันในระดับอุปกรณ์ปลายทาง การแบ่งส่วนเครือข่าย และการเฝ้าระวังพฤติกรรมที่ผิดปกติแบบเรียลไทม์

ขณะที่สถานะถูกควบคุมโดยบอต (Bot-Controlled) แม้จะมีจำนวนเหตุการณ์ไม่สูง แต่มีความเสี่ยงเชิงระบบในระดับสูงมาก เนื่องจากมีศักยภาพในการควบคุมระบบจากภายนอกและการถูกใช้เป็นฐานในการโจมตีต่อเนื่อง แนวทางการตอบสนองจึงจำเป็นต้องเป็นการตอบสนองอย่างเร่งด่วน โดยใช้มาตรการบล็อกทราฟฟิกผิดปกติ การเสริมกลไกการป้องกันบอต และการดำเนินการตอบสนองต่อเหตุการณ์โดยทันที

โดยสรุป ผลการสังเคราะห์แสดงให้เห็นว่าการกำหนดแนวทางการป้องกันภัยทางไซเบอร์เชิงรุกควรพิจารณาร่วมกันระหว่างสถานะภัยคุกคาม ระดับความเสี่ยง และลักษณะผลกระทบเชิงระบบ มากกว่าการพิจารณา

จากจำนวนเหตุการณ์เพียงอย่างเดียว ทั้งนี้ ข้อมูลจากระบบป้องกันแอปพลิเคชันเว็บสามารถนำมาใช้เป็นฐานข้อมูลเชิงประจักษ์เพื่อสนับสนุนการกำหนดแนวทางการป้องกันเชิงรุกที่สอดคล้องกับบริบทการใช้งานจริงขององค์กรอย่างเป็นระบบ

อภิปรายผลการวิจัย

ผลการวิจัยจากการวิเคราะห์ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่บันทึกโดยระบบป้องกันแอปพลิเคชันเว็บของมหาวิทยาลัยฯ ในช่วงเวลาที่ศึกษา สะท้อนให้เห็นภาพรวมของสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริงภายใต้บริบทการใช้งานขององค์กร โดยพบว่าการโจมตีมีความหลากหลายในด้านประเภท จำนวนเหตุการณ์ สถานะการโจมตี และระดับผลกระทบต่อระบบแอปพลิเคชันเว็บ ผลการวิเคราะห์ดังกล่าวชี้ให้เห็นถึงความซับซ้อนและความต่อเนื่องของภัยคุกคามที่ระบบต้องเผชิญ และสามารถนำมาอภิปรายเชื่อมโยงกับงานวิจัยที่เกี่ยวข้อง รวมถึงแนวคิดและกรอบทฤษฎีด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ในหลายประเด็นสำคัญ

ประเด็นแรก สถานะการโจมตีในระดับความพยายาม (Attacked) ผลการวิจัยแสดงให้เห็นว่าเหตุการณ์การโจมตีส่วนใหญ่อยู่ในสถานะถูกโจมตี (Attacked) โดยพบจำนวนเหตุการณ์สูงถึง 39,862 ครั้ง คิดเป็นร้อยละ 67.83 ของเหตุการณ์ทั้งหมด สะท้อนถึงความถี่ของความพยายามโจมตีที่เกิดขึ้นอย่างต่อเนื่องต่อระบบแอปพลิเคชันเว็บ แม้เหตุการณ์ส่วนใหญ่ยังไม่ส่งผลให้เกิดการบุกรุกระบบสำเร็จ แต่ลักษณะของการโจมตีที่เกิดซ้ำและมีความถี่สูงบ่งชี้ว่าระบบยังคงอยู่ภายใต้แรงกดดันจากภัยคุกคามภายนอกอย่างสม่ำเสมอ ผลการวิจัยในประเด็นนี้สอดคล้องกับการศึกษาของ Kumar et al. [12] ซึ่งระบุว่าระบบแอปพลิเคชันเว็บมักเผชิญกับการโจมตีในลักษณะความพยายามโจมตี (Attempted attacks) เป็นจำนวนมาก โดยแม้จะไม่ประสบผลสำเร็จในทันที แต่ข้อมูลดังกล่าวสามารถนำมาใช้เป็นฐานในการวิเคราะห์แนวโน้มและพฤติกรรมของผู้โจมตีได้อย่างมีประสิทธิภาพ นอกจากนี้ ผลการวิจัยยังสนับสนุนแนวคิดด้านการบริหารความมั่นคงปลอดภัยเชิงป้องกัน (Preventive security) ซึ่งให้ความสำคัญกับการเฝ้าระวังเชิงรุกและการวิเคราะห์เหตุการณ์ที่ตรวจพบอย่างต่อเนื่อง มากกว่าการพิจารณาเฉพาะเหตุการณ์ที่การโจมตีประสบผลสำเร็จเพียงอย่างเดียว

ประเด็นที่สอง สถานะการโจมตีที่ก่อให้เกิดผลกระทบเชิงคุณภาพต่อระบบ เมื่อพิจารณาสถานะการโจมตีที่ส่งผลกระทบต่อระบบในเชิงคุณภาพ พบว่าเหตุการณ์ในสถานะติดมัลแวร์ (Infected) และถูกบุกรุก (Compromised) แม้จะมีจำนวนเหตุการณ์น้อยกว่าสถานะถูกโจมตี (Attacked) แต่กลับก่อให้เกิดผลกระทบต่อระบบในระดับที่สูงกว่า โดยเฉพาะเหตุการณ์ในสถานะติดมัลแวร์ ซึ่งตรวจพบจำนวน 8,124 ครั้ง และส่งผลกระทบต่อระบบปลายทางมากถึง 82 ระบบ สะท้อนถึงความเสี่ยงด้านการแพร่กระจายของมัลแวร์ภายในเครือข่ายองค์กร และการขยายขอบเขตของผลกระทบเชิงระบบ ผลการวิจัยนี้สอดคล้องกับการศึกษาของ Rawther และ Sathyalakshmi [13] ซึ่งชี้ให้เห็นว่าการติดมัลแวร์ในระบบเว็บแอปพลิเคชันสามารถนำไปสู่การเกิดผลกระทบเชิงลูกโซ่ภายในเครือข่าย หากองค์กรขาดมาตรการควบคุมที่เหมาะสม เช่น การแยกส่วนเครือข่ายและการป้องกันในระดับอุปกรณ์ปลายทาง ทั้งนี้ ผลการวิจัยยังตอกย้ำถึงความสำคัญของการประเมินภัยคุกคามโดยคำนึงถึงระดับผลกระทบเชิงระบบควบคู่กับจำนวนเหตุการณ์ที่ตรวจพบ

ในขณะเดียวกัน เหตุการณ์ในสถานะถูกบุกรุก (Compromised) ซึ่งตรวจพบจำนวน 7,945 ครั้ง แม้จะส่งผลกระทบต่อระบบในวงจำกัดเมื่อเปรียบเทียบกับสถานะติดมัลแวร์ แต่สะท้อนถึงความเสี่ยงด้านการเข้าถึงทรัพยากรโดยมิชอบและการละเมิดสิทธิ์ในระดับที่มีนัยสำคัญ ผลการวิจัยในประเด็นนี้สอดคล้องกับงานวิจัยของ Malik et al. [14] ซึ่งระบุว่าการโจมตีที่นำไปสู่การเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต แม้จะเกิดขึ้นในขอบเขตจำกัด แต่สามารถส่งผลกระทบโดยตรงต่อความมั่นคงปลอดภัยของข้อมูล ความถูกต้องของระบบ และความน่าเชื่อถือของระบบแอปพลิเคชันเว็บโดยรวม

นอกจากนี้ เหตุการณ์ในสถานะถูกควบคุมโดยบอต (Bot-controlled) แม้จะตรวจพบจำนวนเหตุการณ์เพียง 2,846 ครั้ง และส่งผลกระทบต่อระบบจำนวน 5 ระบบ แต่ถูกจัดอยู่ในระดับผลกระทบเชิงระบบที่สูงมาก เนื่องจากระบบในสถานะดังกล่าวมีศักยภาพในการถูกควบคุมจากภายนอกและอาจถูกนำไปใช้เป็นฐานสำหรับการ

โจมตีต่อเนื่องทั้งภายในและภายนอกองค์กร ผลการวิจัยในประเด็นนี้สอดคล้องกับงานวิจัยด้านบอตเน็ตและการโจมตีแบบอัตโนมัติ ซึ่งชี้ให้เห็นว่าเหตุการณ์ที่เกี่ยวข้องกับการควบคุมระบบจากระยะไกล แม้จะเกิดขึ้นในความถี่ที่ต่ำกว่าการโจมตีรูปแบบอื่น แต่มีความเสี่ยงเชิงระบบและผลกระทบในระดับสูงอย่างมีนัยสำคัญ

ประเด็นที่สาม การใช้ข้อมูลเชิงประจักษ์เพื่อกำหนดแนวทางการป้องกันเชิงรุก เมื่อพิจารณาผลการวิจัยในภาพรวม พบว่าการนำข้อมูลเหตุการณ์จริงที่บันทึกจากระบบป้องกันแอปพลิเคชันเว็บมาใช้เป็นฐานข้อมูลเชิงประจักษ์ สามารถสนับสนุนการกำหนดแนวทางการป้องกันภัยทางไซเบอร์เชิงรุกที่สอดคล้องกับระดับความเสี่ยงของภัยคุกคามได้อย่างเป็นระบบ แตกต่างจากงานวิจัยบางส่วนที่มุ่งวิเคราะห์เฉพาะประเภทของการโจมตีเพียงมิติเดียว งานวิจัยนี้ได้บูรณาการข้อมูลด้านสถานะการโจมตี จำนวนเหตุการณ์ และระดับผลกระทบเชิงระบบร่วมกัน เพื่อนำไปสู่การกำหนดแนวทางการตอบสนองที่เหมาะสมกับลักษณะของภัยคุกคามในแต่ละระดับ ซึ่งช่วยลดการตัดสินใจเชิงคาดเดา และเพิ่มความสอดคล้องกับบริบทการใช้งานจริงขององค์กรอย่างมีนัยสำคัญ

โดยสรุป ผลการวิจัยนี้สนับสนุนให้เห็นว่าข้อมูลจากระบบป้องกันแอปพลิเคชันเว็บไม่ได้มีบทบาทจำกัดเพียงการตรวจจับหรือบล็อกการโจมตีเท่านั้น หากแต่ยังสามารถนำมาใช้เป็นฐานข้อมูลเชิงประจักษ์ในการวิเคราะห์แนวโน้มการโจมตี การประเมินระดับความเสี่ยง และการสังเคราะห์แนวทางการป้องกันภัยทางไซเบอร์เชิงรุกที่สอดคล้องกับระดับผลกระทบของภัยคุกคามในสภาพแวดล้อมการใช้งานจริงขององค์กรได้อย่างมีประสิทธิภาพ ทั้งในเชิงวิชาการและเชิงปฏิบัติ

ข้อเสนอแนะ

จากผลการวิจัยที่ได้วิเคราะห์ข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ซึ่งบันทึกโดยระบบป้องกันแอปพลิเคชันเว็บ ผู้วิจัยสามารถสังเคราะห์ข้อเสนอแนะทั้งในเชิงการนำไปใช้และเชิงการวิจัยในอนาคต เพื่อสนับสนุนการพัฒนามาตรการป้องกันภัยทางไซเบอร์ให้มีความเป็นระบบและสอดคล้องกับบริบทการใช้งานจริงขององค์กร ดังต่อไปนี้

1. ข้อเสนอแนะเชิงการนำไปใช้

มหาวิทยาลัยฯ ควรนำข้อมูลเหตุการณ์การโจมตีทางไซเบอร์ที่บันทึกจากระบบป้องกันแอปพลิเคชันเว็บมาใช้เป็นฐานข้อมูลเชิงประจักษ์ในการกำหนดมาตรการป้องกันภัยทางไซเบอร์เชิงรุก โดยพิจารณาสถานะการโจมตี ความถี่ของเหตุการณ์ และระดับผลกระทบเชิงระบบร่วมกัน เพื่อจัดลำดับความสำคัญของภัยคุกคาม และเสริมประสิทธิภาพของกลไกการเฝ้าระวังและการตอบสนองต่อเหตุการณ์ให้เหมาะสมกับบริบทการใช้งานจริงขององค์กร

2. ข้อเสนอแนะสำหรับการวิจัยในอนาคต

การวิจัยในอนาคตควรพิจารณาขยายช่วงเวลาการเก็บรวบรวมข้อมูล หรือบูรณาการข้อมูลจากระบบความมั่นคงปลอดภัยอื่นร่วมกับข้อมูลจากระบบป้องกันแอปพลิเคชันเว็บ เพื่อเพิ่มความครบถ้วนและความแม่นยำในการวิเคราะห์แนวโน้มของภัยคุกคามทางไซเบอร์ รวมถึงสนับสนุนการพัฒนากลยุทธ์การป้องกันภัยทางไซเบอร์ให้มีประสิทธิภาพและสอดคล้องกับบริบทการใช้งานจริงมากยิ่งขึ้น

เอกสารอ้างอิง

[1] Immadisetti, K. M., Datta, D. V., & Raveendran, L. S. (2025). Website Vulnerability Scanning System. *Indian Scientific Journal Of Research In Engineering And Management*, 9(03), 1–9. https://doi.org/10.55041/ijsrem43079

[2] Yaddala, M. N. K., & Sunkara, Y. R. (2024). Comprehensive Survey of Web Security Threats in 2024. *Indian Scientific Journal Of Research In Engineering And Management*, 8(11), 1–7. https://doi.org/10.55041/ijsrem38614

[3] Rathod, J. A., Gowda, D. S., M, K., Talekar, P., Daddi, N., Bhairanallikar, A., & G, G. (2024). The Cross-Site Scripting (XSS) Attack: A Comprehensive Review. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-19230

[4] Babaey, V., & Ravindran, A. (2025). GenXSS: an AI-Driven Framework for Automated Detection of XSS Attacks in WAFs. *Preprints*. https://doi.org/10.20944/preprints202503.0313.v1

[5] Yelkoti, N. K. K. R. (2025). Beyond Traditional WAFs: Behavioral Analytics for Advanced API Threat Detection and Response. *European Journal of Computer Science and Information Technology*, 13(46), 10–19. https://doi.org/10.37745/ejcsit.2013/vol13n461019

[6] Leka, E., Lamani, L., Aliti, A., & Hoxha, E. (2024). Web Application Firewall for Detecting and Mitigation of Based DDoS Attacks Using Machine Learning and Blockchain. *TEM Journal*, 13(4), 2802–2811. https://doi.org/10.18421/tem134-17

[7] Annas, M., Adek, R. T., & Afrillia, Y. (2024). Web Application Firewall (WAF) Design to Detect and Anticipate Hacking in Web-Based Applications. *Deleted Journal*, 1(3), 52. https://doi.org/10.29103/jacka.v1i3.16315

[8] Yaddala, M. N. K., & Sunkara, Y. R. (2024). Comprehensive Survey of Web Security Threats in 2024. *Indian Scientific Journal Of Research In Engineering And Management*, 8(11), 1–7. https://doi.org/10.55041/ijsrem38614

[9] Zaki, A., & Mohammed, S. (2024). Artificial Intelligence for Web Application Firewall (WAF): A Comprehensive Review. *International Research Journal of Innovations in Engineering and Technology,* 8(11), 219–224. https://doi.org/10.47001/irjiet/2024.811027

[10] ศูนย์เทคโนโลยีสารสนเทศ. (2025). *รายงานเหตุการณ์การโจมตีระบบสารสนเทศ.* https://itcenter.kru.ac.th/report_attacked

[11] Incesu, E., & Orhan, F. (2018). An analysis of security reporting system data in a public hospital: A retrospective research. Journal of Academic Research in Health Sciences, 5(2), 79. https://doi.org/10.5455/SAD.13-1525867323

[12] Kumar, Y., Satyanarayana, A. S., Kumar, A., & Sharma, V. (2021). Risks and Threats to Web Applications and Their Preventions: A Theoretical Study on Vital Risks and Threats. *International Journal of Computer Science and Engineering Technology,* 7(2), 432–438. https://doi.org/10.32628/CSEIT217281

[13] Rawther, S., & Sathyalakshmi, S. (2023). The Spread of Malicious Activity in a Computer Network. In *Proceedings of the International Conference on Computing, Communication and Networking Technologies* (pp. 1–6). IEEE. https://doi.org/10.1109/icccnt56998.2023.10307246

[14] Malik, A. K., Gehlot, S., & Aggarwal, A. (2023). Attacks on Web Applications. In *Cybersecurity threats and solutions* (pp. 31–62). IGI Global. https://doi.org/10.4018/978-1-6684-8218-6.ch002