โลกไลน์ที่ปลอดภัย: การพัฒนาระบบตรวจสอบมัลแวร์สำหรับการสื่อสารผ่านแอปไลน์ด้วยไวรัสโททัล

SecureLine World: Developing a Malware Detection System for LINE Communication with VirusTotal

ณัฐนันท์ ภู่พิชิต[1*] และ สุรศักดิ์ มังสิงห์[2]
Nattanun Phupichit[1*] and Surasak Mungsing [2]
*Corresponding author, e-mail: nattanunp.new@gmail.com

Received: April 24th ,2024; **Revised**:, August 19th 2024.; **Accepted**:, April 28th 2025.

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนาระบบตรวจจับและแจ้งเตือนมัลแวร์ในไฟล์หรือลิงก์ที่อาจเป็นอันตราย ซึ่งส่งผ่านแอปพลิเคชันไลน์ โดยใช้เทคโนโลยี ไวรัสโททัล ในการวิเคราะห์ความเสี่ยงผ่านการสแกนด้วยหลายระบบรักษาความปลอดภัย ระบบถูกพัฒนาออกแบบในนาม ไลน์ที่ปลอดภัย เพื่อตรวจสอบและแจ้งเตือนผู้ใช้เกี่ยวกับความเสี่ยงได้อย่างรวดเร็วและแม่นยำ โดยใช้ข้อมูลจำนวน 1,000 ตัวอย่าง ซึ่งประกอบด้วยลิงก์ 840 ตัวอย่าง และไฟล์ 160 ตัวอย่าง เพื่อเสริมสร้างความปลอดภัยทางไซเบอร์

ผลการทดสอบการประเมินประสิทธิภาพของระบบโดยใช้ข้อมูลจำนวน 1000 ตัวอย่างเพื่อตรวจสอบไฟล์หรือลิงก์ที่สื่อสารผ่านแอปไลน์พบว่าให้ผลลัพธ์ความปลอดภัยของไฟล์และลิงก์ได้ร้อยละ 95.00 ซึ่งหมายความว่าระบบสามารถตรวจจับความเสี่ยงของไฟล์และลิงก์ที่อาจเป็นอันตรายได้อย่างมีประสิทธิภาพ โดยเฉพาะเมื่อพิจารณาผลการวิเคราะห์ระบบจากตัวอย่างทั้งหมดโดยการตรวจสอบจำนวนลิงก์จำนวน 840 ตัวอย่างพบว่าผลลัพธ์ความปลอดภัยที่ร้อยละ 95.24 ซึ่งสูงกว่าค่าเฉลี่ยทั่วไป และการตรวจสอบจำนวนไฟล์จำนวน 160 ตัวอย่างให้ผลลัพธ์ความปลอดภัยที่ร้อยละ 93.75 ซึ่งยังคงมีประสิทธิภาพในการตรวจสอบความปลอดภัยของไฟล์อย่างมีนัยสำคัญและเห็นได้ชัดเจน นอกจากนี้ผลการศึกษายังช่วยให้เข้าใจถึงการดำเนินงานและประสิทธิภาพของระบบในสถานการณ์จริงและมีข้อมูลสำคัญสำหรับการพัฒนาและปรับปรุงระบบในอนาคต

คำสำคัญ: ไลน์ที่ปลอดภัย การตรวจจับมัลแวร์ ไวรัสโททัล ความปลอดภัยทางไซเบอร์ แอปพลิเคชันไลน์

[1] นักศึกษาหลักสูตรวิทยาศาสตร์มหาบัณฑิต คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
Master of Science program students, Faculty of Information Technology, Sripatum University
[2] อาจารย์ประจำหลักสูตรวิทยาศาสตร์มหาบัณฑิต คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
Lecturer for the Master of Science program, Faculty of Information Technology, Sripatum University

Abstract

The objective of this research aims to develop a malware detection and alert system in potentially dangerous files or links sent via the LINE application, using VirusTotal technology to analyze risks through scanning with multiple security systems. The system is designed under the name of SecureLine to quickly and accurately check and alert users about risks using 1,000 samples of data, consisting of 840 links and 160 files, to enhance cybersecurity.

The results of the system performance evaluation test using 1,000 samples of data to check files or links communicated via the LINE application showed that the file and link safety results were 95.00 percent, meaning that the system can effectively detect risks of potentially dangerous files and links. In particular, when considering the results of the system analysis from all samples, checking the number of 840 links, the safety results were 95.24 percent, which is higher than the general average. And checking the number of 160 files gave a safety result of 93.75 percent, which is still significantly and clearly effective in checking file safety. In addition, the results of the study also help understand the operation and efficiency of the system in real situations and provide important information for future system development and improvement.

Keywords: SecureLine, Malware Detection, VirusTotal, Cybersecurity, LINE

บทนำ

ในปัจจุบัน บทบาทของเทคโนโลยีสารสนเทศและการสื่อสารในการสนับสนุนและเป็นส่วนสำคัญของชีวิตประจำวันของมนุษย์ไม่ได้มีเพียงแค่การใช้งานเทคโนโลยีในรูปแบบของเสียง ภาพ และตัวอักษรอย่างเดียว แต่ยังรวมถึงการใช้งานเทคโนโลยีอิเล็กทรอนิกส์ที่มีรูปแบบหลากหลาย เช่น เทคโนโลยีคอมพิวเตอร์ เทคโนโลยีโทรคมนาคม และระบบสื่อมวลชนตามนโยบายที่กำหนดไว้ นโยบายด้านอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศมีบทบาทสำคัญในการพัฒนาประเทศโดยเฉพาะ เนื่องจากเป็นเครื่องมือสำคัญในการจัดการข้อมูลตั้งแต่ขั้นตอนการผลิต การจัดเก็บ การประมวลผล การเรียกใช้ และการแลกเปลี่ยน ระบบนี้ช่วยในการจัดการอัตโนมัติและสื่อสารที่มีประสิทธิภาพระหว่างกัน ทำให้ข้อมูลมีความสำคัญมากในสังคมปัจจุบัน

แม้ว่าเทคโนโลยีด้านความมั่นคงปลอดภัยในระบบไอทีจะเจริญไปอย่างก้าวหน้า แต่ภัยคุกคามจากกลุ่มอาชญากรในโลกไซเบอร์ก็ยังคงนำเทคโนโลยีที่ทันสมัยและเทคนิคการหลบหลีกรูปแบบใหม่ๆ มาใช้อย่างต่อเนื่อง งานวิจัยนี้ได้สังเกตการเพิ่มขึ้นที่สุดอย่างต่อเนื่องถึง 1,160% ในจำนวนไฟล์ PDF ที่เป็นอันตรายตั้งแต่ปี 2019-2020 ไฟล์ PDF ที่เป็นอันตรายมักจะใช้เทคนิคการนำทางการจราจร (traffic redirection) ที่มีประโยชน์ในการหลอกลวงและการหลีกเลี่ยงการตรวจจับ และสามารถเปลี่ยนวัตถุประสงค์สุดท้ายของการหลอกลวงได้ตามต้องการ (Ashkan, H. and Ashutosh, C., 2021)

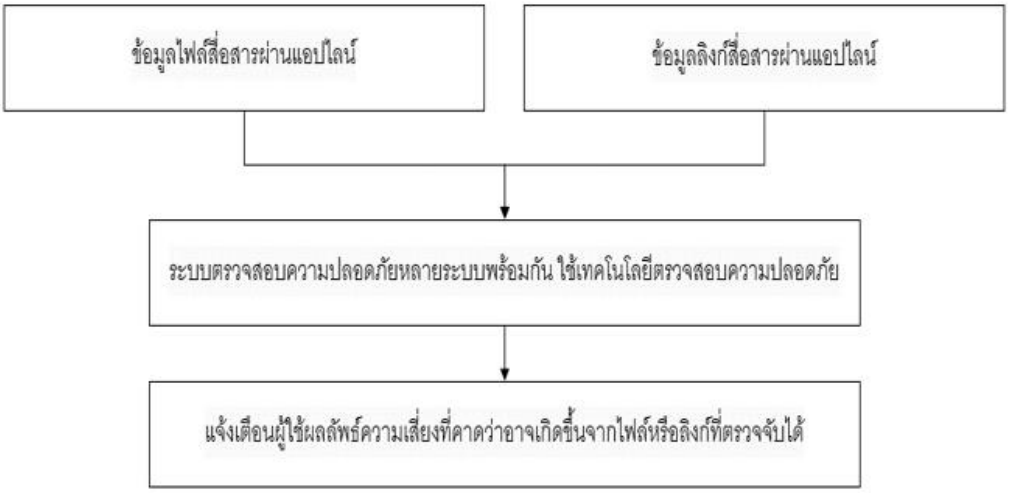
งานวิจัยนี้ได้เริ่มต้นด้วยการประเมินอย่างละเอียดเกี่ยวกับเทคนิคการจำแนกประเภทมัลแวร์ (Virustotal, 2023d) โดยใช้เทคนิคการรวบรวมข้อมูลและการวิเคราะห์อย่างรวดเร็วและอัตโนมัติ การวิเคราะห์มัลแวร์คือกระบวนการที่เกี่ยวข้องกับการตรวจสอบโครงสร้างของโค้ด ไวยากรณ์ และลักษณะอื่นๆ เพื่อระบุปัญหาหรือช่องโหว่ที่เป็นไปได้ในรหัส การวิเคราะห์นี้มักจะถูกนำมาใช้ในการตรวจสอบซอฟต์แวร์เพื่อความปลอดภัยหรือการตรวจจับโปรแกรมคอมพิวเตอร์ที่เป็นมัลแวร์ (Chiradeep B. M., 2021) เพื่อตรวจจับไฟล์ที่เป็นมัลแวร์ ซึ่งมีการบ่งชี้ว่าไฟล์นั้นมีลักษณะของมัลแวร์หรือไม่ การวิเคราะห์จะใช้หลายเทคโนโลยีตรวจสอบความปลอดภัย เช่น การสแกน

แอนตี้ไวรัส (antivirus scanning) การตรวจสอบฮาช (hash checking) การวิเคราะห์เซ็นเนอร์ (signature analysis) ที่มักจะใช้การเปรียบเทียบเซ็นเนเจอร์ของไฟล์ที่ตรวจสอบกับเซ็นเนเจอร์ที่รู้จักของมัลแวร์ที่เคยถูกบันทึกไว้และถูกตรวจจับไว้ก่อนหน้านี้ ถ้าพบเซ็นเนเจอร์ที่ตรงกันหรือคล้ายกันในไฟล์ที่ตรวจสอบกับเซ็นเนเจอร์ของมัลแวร์ที่รู้จักมาก่อน อาจสามารถสรุปได้ว่าไฟล์ที่ตรวจสอบนั้นมีความเสี่ยงต่อการเป็นมัลแวร์ และอื่นๆ อีกมาก โดยไวรัสโททัล จะส่งไฟล์หรือลิงก์ไปยังหลายๆ เครื่องมือตรวจสอบความปลอดภัยอย่างพร้อมกัน ไวรัสโททัลไม่ได้ติดป้ายกำกับโดยตรงว่าเป็นอันตรายหรือไม่ แต่จะคืนคะแนนความเสี่ยงวิเคราะห์การตรวจจับของไฟล์และลิงก์ (Aleieldin, S., Sebastian, B. and Alexander, P., 2020 : 2) แล้วรวมผลการวิเคราะห์เข้าด้วยกันเพื่อให้ผู้ใช้ได้ข้อมูลที่ครอบคลุมและเชื่อถือได้เกี่ยวกับความเสี่ยงของไฟล์นั้น ๆ โดยอัตโนมัติและรวดเร็ว การใช้เทคโนโลยีที่หลากหลายนี้ช่วยให้ ไวรัสโททัลมีความสามารถในการตรวจจับมัลแวร์ได้อย่างมีประสิทธิภาพและเชื่อถือได้ วิธีการของงานวิจัยนี้มีวัตุประสงค์เพื่อเสริมความปลอดภัยในการสื่อสารผ่านแอปไลน์ (line application) การใช้ไวรัสโททัลเป็นเครื่องมือในการตรวจสอบไฟล์หรือลิงก์ที่ผ่านการสื่อสาร โดยไวรัสโททัล มีความสามารถในการวิเคราะห์ไฟล์หรือลิงก์โดยใช้หลายๆ เทคโนโลยีตรวจสอบความปลอดภัย เช่น การสแกนแอนตี้ไวรัสและเครื่องมือการตรวจสอบความปลอดภัยอื่นๆ ซึ่งช่วยให้ผู้ใช้สามารถระบุไฟล์หรือลิงก์ที่เสี่ยงต่อความปลอดภัยได้อย่างแม่นยำขึ้น ผลการวิเคราะห์จะถูกประเมินอย่างชัดเจนและรวดเร็ว ดังนั้น การใช้ไวรัสโททัล เพื่อตรวจสอบไฟล์หรือลิงก์ (VirusTotal, V., 2023) ที่ส่งผ่านการสื่อสารผ่านแอปไลน์จะช่วยเพิ่มความมั่นใจและประสิทธิภาพในการใช้งานได้มากยิ่งขึ้น โมเดลของงานวิจัยนี้แสดงให้เห็นถึงความแข็งแกร่งในรวดเร็วและความแม่นยำที่มีอยู่ในปัจจุบัน ซึ่งเป็นการแสดงให้เห็นถึงความมีประสิทธิภาพของระบบในสถานการณ์จริง (Virustotal, 2023b)

วัตถุประสงค์ของงานวิจัย

เพื่อพัฒนาระบบตรวจสอบและแจ้งเตือนมัลแวร์ที่แฝงอยู่ในไฟล์หรือลิงก์ซึ่งถูกส่งผ่านแอปพลิเคชันไลน์ โดยการทำงานร่วมกับเทคโนโลยี ไวรัสโททัล

กรอบแนวคิดในการวิจัย



รูปที่ 1 กรอบแนวคิดการวิจัย

การวิเคราะห์และระบุความเสี่ยงที่เกี่ยวข้องกับไฟล์หรือลิงก์ที่ส่งผ่านแอปไลน์โดยใช้เทคโนโลยีที่ทันสมัย ซึ่งสามารถสแกน (Virustotal, 2023a) และตรวจจับมัลแวร์อย่างแม่นยำและรวดเร็ว วิเคราะห์ความเสี่ยงโดยอัตโนมัติและรวดเร็วโดยการส่งไฟล์หรือลิงก์ไปยังเครื่องมือตรวจสอบความปลอดภัยหลายๆ ระบบพร้อมกัน เช่น VirusTotal มีกระบวนการทำงาน คือการรับไฟล์หรือลิงก์จากผู้ใช้แล้วส่งไปยังระบบตรวจสอบความปลอดภัยหลายระบบพร้อมกันเพื่อวิเคราะห์ความเสี่ยงอย่างรวดเร็วและแม่นยำ โดยแสดงผลในรูปแบบของคะแนนความเสี่ยง จากหลายระบบ เพื่อให้ผู้ใช้สามารถประเมินความเสี่ยงได้อย่างครอบคลุม และระบบแจ้งเตือนผู้ใช้เกี่ยวกับความเสี่ยงที่คาดว่าอาจเกิดขึ้นจากไฟล์หรือลิงก์ที่ตรวจจับได้ และแนะนำมาตรการป้องกันที่เหมาะสมพัฒนาเครื่องมือให้มีประสิทธิภาพในการตรวจจับและป้องกันมัลแวร์อย่างเชื่อถือได้อย่างมีประสิทธิภาพและแม่นยำ โดยใช้ข้อมูลที่ได้รับจากการวิเคราะห์และระบุความเสี่ยงเพื่อปรับปรุงและพัฒนาต่อไป

ระเบียบวิธีวิจัย

ประชากรและกลุ่มตัวอย่าง

ประชากร (population) ที่ใช้ในการวิจัยได้แก่ประชากรผู้ใช้ไลน์ ในประเทศไทย ปัจจุบันมีจำนวน 54 ล้านคน ณ มิถุนายน 2566 (LINE, 2566) ของงานวิจัยนี้

กลุ่มตัวอย่าง (sampling) ที่ใช้ในการวิจัยได้แก่ ประชากรผู้ใช้ไลน์ ในประเทศไทย จึงกำหนดขนาดตัวอย่างโดยใช้สูตร ทาโร่ ยามาเน่ (Yamane, T., 1967) ขนาดของกลุ่มตัวอย่างที่คำนวณได้เท่ากับ 400 ตัวอย่าง เพื่อพิจารณาความเพียงพอและเหมาะสมในการวิเคราะห์โมเดลสมการโครงสร้าง ดังนั้นในงานวิจัยนี้ควรเก็บข้อมูลจำนวนไฟล์และลิงก์ 1,000 ตัวอย่าง เพื่อแทนความเป็นไปได้ของประชากรในกลุ่มตัวอย่างได้อย่างเหมาะสม

เครื่องมือที่ใช้ในการวิจัยและคุณภาพของเครื่องมือ

ผู้วิจัยได้ดำเนินการทบทวนเอกสารวรรณกรรม และงานวิจัยที่เกี่ยวข้อง เพื่อการวิเคราะห์มัลแวร์เป็นภารกิจที่สำคัญและท้าทายในมุมมองของสถานการณ์ภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว การใช้เทคโนโลยีเซ็นเนเจอร์ในการแยกแยะมัลแวร์ไม่สามารถทำงานได้เร็วเท่ากับการเปลี่ยนแปลงของมัลแวร์เวอร์ชัน การพัฒนาเครื่องมือการจำแนกประเภทมัลแวร์ที่มีประสิทธิภาพมากขึ้นเป็นสิ่งจำเป็นเพื่อให้สามารถตอบสนองต่อแนวโน้มใหม่ๆ และแก้ไขปัญหาที่เกิดขึ้น ดังนี้

1. การบูรณาการเทคโนโลยีการผสมผสานเทคโนโลยีต่างๆ เช่น แอนตี้ไวรัส, และเทคโนโลยีการวิเคราะห์เบื้องต้น โดยเครื่องมือที่ใช้ในการวิจัยครั้งนี้คือระบบที่พัฒนาขึ้นเพื่อ ตรวจจับและแจ้งเตือนมัลแวร์ ผ่านแอปพลิเคชัน LINE โดยใช้เทคโนโลยี VirusTotal และ LINE Messaging API ซึ่งเป็นเครื่องมือหลักในการประมวลผลข้อมูล ตรวจสอบความเสี่ยง และแจ้งเตือนผู้ใช้งาน เพื่อสร้างเครื่องมือที่มีประสิทธิภาพในการตรวจจับและป้องกันมัลแวร์ให้มีประสิทธิภาพมากที่สุด

2. การพัฒนาเครื่องมือเฉพาะทางการสร้างเครื่องมือที่เน้นการวิเคราะห์และตรวจสอบมัลแวร์อย่างเฉพาะทาง VirusTotal เป็นเครื่องมือวิเคราะห์ความปลอดภัยที่สามารถส่งไฟล์หรือลิงก์ไปยังหลายระบบตรวจสอบพร้อมกัน จึงช่วยเพิ่มความแม่นยำในการระบุความเสี่ยง เพื่อให้สามารถตอบสนองต่อการเปลี่ยนแปลงของมัลแวร์ได้อย่างมีประสิทธิภาพ

3. การพัฒนาเครื่องมือที่มีความสามารถในการจำแนกประเภท การพัฒนาเครื่องมือที่สามารถจำแนกประเภทและวิเคราะห์มัลแวร์อย่างถูกต้อง เพื่อให้สามารถตรวจจับและป้องกันมัลแวร์ได้อย่างมีประสิทธิภาพ

4. การปรับปรุงและพัฒนาต่อเนื่อง การทำงานกับชุดเครื่องมือให้มีการปรับปรุงและพัฒนาต่อเนื่องเพื่อให้สามารถรับมือกับมัลแวร์ใหม่ๆ และโจมตีที่เปลี่ยนแปลงได้อย่างมีประสิทธิภาพ

5. การแจ้งเตือนแบบเรียลไทม์ การใช้ LINE Messaging API เป็นเครื่องมือที่สามารถใช้ส่งข้อความแจ้งเตือนไปยังผู้ใช้งานแบบเรียลไทม์ จึงเหมาะสมกับวัตถุประสงค์ของการวิจัยที่เน้นการแจ้งเตือนอัตโนมัติและมีประสิทธิภาพเพื่อส่งข้อความแจ้งเตือนแบบเรียลไทม์เมื่อมีการตรวจจับมัลแวร์หรือความเสี่ยงที่เกี่ยวข้อง เพื่อให้ผู้ใช้สามารถตอบสนองต่อสถานการณ์ทันที (LINE, D., 2022)

6. การจัดการกับผู้ใช้ การใช้ Line Messaging API เพื่อจัดการกับผู้ใช้โดยสามารถส่งคำแนะนำหรือข้อมูลเพิ่มเติมให้กับผู้ใช้เกี่ยวกับมัลแวร์และความเสี่ยงที่เกี่ยวข้อง

7. การส่งข้อมูลการวิเคราะห์ การใช้ Line Messaging API เพื่อส่งข้อมูลการวิเคราะห์มัลแวร์และความเสี่ยงที่เกี่ยวข้องผ่านข้อความ ภาพ หรือไฟล์อื่นๆ เพื่อให้ผู้ใช้สามารถรับข้อมูลอย่างครบถ้วน

8. การสนับสนุนแบบอัตโนมัติ การนำ Line Messaging API มาสนับสนุนระบบการตรวจจับและป้องกันมัลแวร์อย่างอัตโนมัติ โดยการออกแบบระบบการเชื่อมต่อระหว่าง LINE Messaging API กับ Google Apps Script สร้างฟังก์ชันแบบอัตโนมัติ รับข้อมูลไฟล์หรือลิงก์ และส่งไปยัง VirusTotal เพื่อทำการวิเคราะห์และรับผลการวิเคราะห์จาก VirusTotal และประมวลผลเพื่อส่งข้อความแจ้งเตือนไปยังผู้ใช้งาน LINE เช่น การส่งข้อความแจ้งเตือนหรือข้อมูลการวิเคราะห์โดยอัตโนมัติและไม่เข้าถึงข้อมูลของผู้ใช้

การเก็บรวบรวมข้อมูลในการวิจัย

1. การกระจายผ่านเฟซบุ๊ก (facebook) เป็นหนึ่งในช่องทางการสื่อสารที่ใช้กันอย่างแพร่หลายในปัจจุบัน ระบบตรวจสอบและป้องกันความปลอดภัยสำหรับการสื่อสารผ่านแอปไลน์ด้วยไวรัสโททัล (virustotal) เพื่อพิจารณาก่อนนำไปใช้ในการเก็บรวบรวมข้อมูล

2. ดำเนินการจัดเก็บรวบรวมข้อมูลผ่านระบบตรวจสอบและป้องกันความปลอดภัยสำหรับการสื่อสารผ่านแอปไลน์ด้วยไวรัสโททัล ไปกับกลุ่มตัวอย่างผ่านระบบออนไลน์ทุกช่องทาง ได้แก่ ไลน์ (line) เฟสบุ๊ค (facebook) ขอความอนุเคราะห์รวบรวมข้อมูลผู้ใช้งานระบบตรวจสอบและป้องกันความปลอดภัย

3. รวบรวมเก็บแบบสอบถาม โดยการดำเนินการผ่านแบบสอบถามออนไลน์ เผยแพร่ผ่านแพลตฟอร์ม Facebook และ ใช้บริการ Google Forms ซึ่งเป็นเครื่องมือที่น่าเชื่อถือและปลอดภัย และประเมินจำนวนแบบสอบถามที่ได้กลับมาว่ามีความสมบูรณ์และมีจำนวนครบตามที่ได้ออกแบบไว้ รวมทั้งสิ้นจำนวน 1000 ตัวอย่าง จึงถือว่ายอมรับได้

4. ดำเนินการรวบรวมข้อมูลจากไฟล์และลิงก์ 1000 ตัวอย่าง โดยไฟล์และลิงก์จำนวน 1,000 ตัวอย่างจากแหล่งข้อมูลออนไลน์ที่ผู้ใช้ส่งมา และตรวจสอบข้อมูลเพื่อให้ได้ข้อมูลที่สมบูรณ์ก่อนนำมาวิเคราะห์ข้อมูลและแปลผล

การวิเคราะห์ข้อมูล

ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลตามแนวทางการวิจัย ช่วยให้ได้ข้อมูลที่เป็นรายละเอียดและเป็นประโยชน์สำหรับนำข้อมูลมาวิเคราะห์และตรวจสอบประสิทธิภาพและความมั่นคงของระบบที่พัฒนาขึ้นและการประเมินความพึงพอใจของผู้ใช้งาน สถิติเชิงพรรณนา (descriptive statistics) โดยการแจกแจงความถี่ (frequency) ค่าร้อยละ (percentage) และค่าเฉลี่ย (mean) สำหรับค่าความเสี่ยงจากการตรวจสอบและตรวจสอบไฟล์หรือลิงก์ที่ส่งข้อมูลผ่านแอปไลน์ ดังต่อไปนี้

ส่วนที่ 1 การแจกแจงความถี่ (frequency distribution) รวบรวมข้อมูลเกี่ยวกับความเสี่ยงที่ตรวจพบและแจ้งเตือนในรูปแบบของตารางหรือกราฟ แบ่งข้อมูลเป็นช่วงหรือระดับความเสี่ยงและนับจำนวนการเกิดขึ้น

ส่วนที่ 2 ค่าร้อยละ (percentage) แปลงจำนวนข้อมูลในแต่ละช่วงหรือระดับความเสี่ยงเป็นร้อยละของข้อมูลทั้งหมด ช่วยในการเข้าใจและประเมินสัดส่วนของความเสี่ยงที่เกี่ยวข้องกับแต่ละช่วง

ส่วนที่ 3 ค่าเฉลี่ย (mean) คำนวณค่าเฉลี่ยของระดับความเสี่ยงทั้งหมด ให้มุมมองรวบรวมเกี่ยวกับค่าเฉลี่ยของความเสี่ยงที่ผู้ใช้ต้องการจะเผชิญหน้า

ผลการวิจัย

ผลการวิจัยนี้สามารถนำไปปรับใช้ที่ต้องการเสริมสร้างความปลอดภัยในการสื่อสารผ่านแอปไลน์ได้อย่างมีประสิทธิภาพและเชื่อถือได้ โดยขั้นตอนการติดตั้งและการใช้งานระบบการทำงาน โดยผู้ใช้งานสามารถเพิ่มเพื่อนโดยสแกน QR Code เมื่อผู้ใช้งานส่งลิงก์หรือไฟล์ ระบบจะตรวจสอบอัตโนมัติและส่งผลการวิเคราะห์กลับมาทันที การวิจัยด้านการสแกนและวิเคราะห์ข้อมูลการใช้งานผ่านแอปไลน์ด้วยระบบตรวจสอบและป้องกันความปลอดภัยของไวรัสโททัล เป็นการทำงานที่มีความสำคัญในการป้องกันการโจมตีทางไซเบอร์ ผลการวิจัยที่ได้จากการสแกนและวิเคราะห์ข้อมูลในหมวดหมู่ LINK และ FILE ได้แสดงให้เห็นถึงระดับความอันตรายของการใช้งานแต่ละประเภท และ แนวคิดเกี่ยวกับ "Hazard" หรือ "ความอันตราย" คือ ร้อยละของข้อมูลที่มีความเสี่ยงจากมัลแวร์หรือภัยคุกคามที่ตรวจพบ จะสามารถใช้เป็นเกณฑ์ในการจัดระดับความอันตราย เพื่อให้ผู้ใช้ตัดสินใจได้อย่างมีข้อมูลรองรับและเป็นระบบมากขึ้น

ตารางที่ 1 ผลการสแกนทั้งหมด แสดงถึงร้อยละของผลลัพธ์การสแกนที่มีความอันตรายต่อทั้งหมดโดยรวม

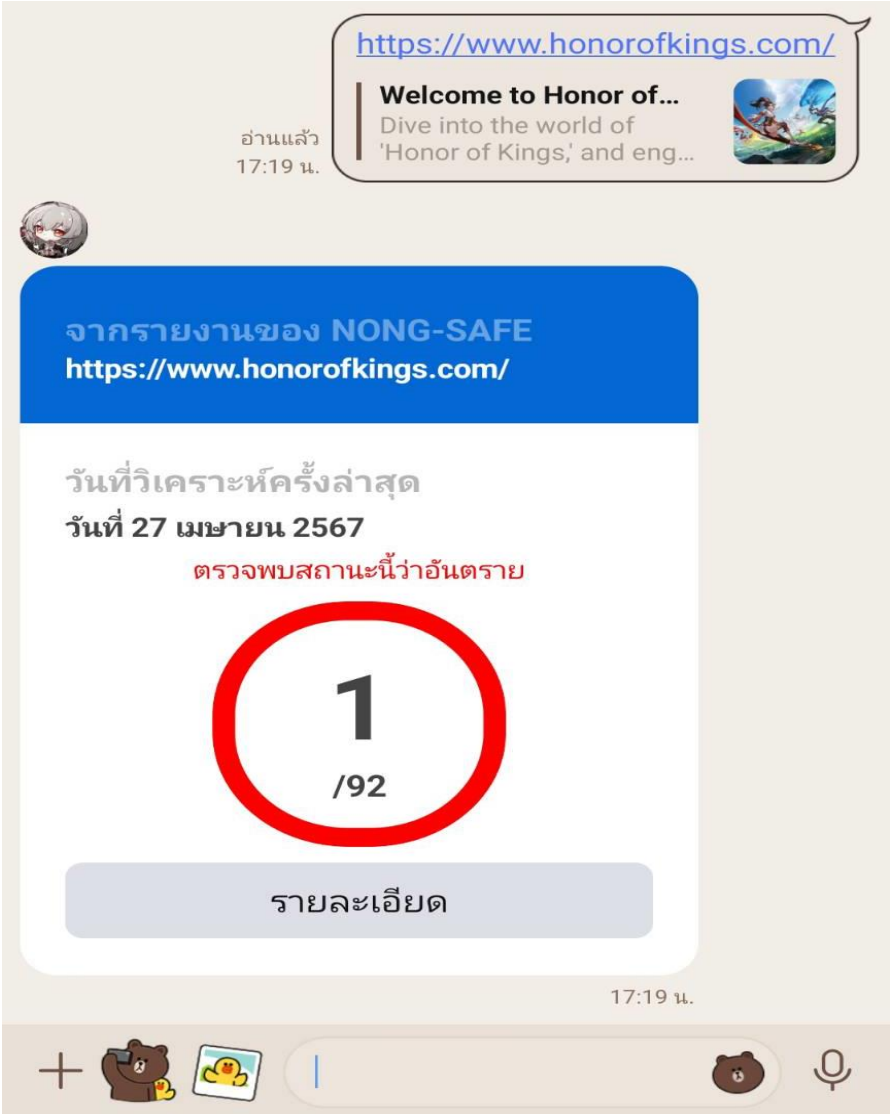
ข้อมูล	R	RS	RF	Hazard
All	1000	950	50	5%
LINK	840	800	40	5%
FILE	160	150	10	6.67%

```
function processInputText(text, event) {
  const ckURL =
    text.match(
      /(?:https?:\/\/[^\s]+)|(www\.[^\s]+)|(https?:\/\/[^\n]+)|(www\.[^\n]+)/g
    ) || [];

  return ckURL.map((url) => {
    try {
      const params = {
        url: url,
      };

      const apiUrl = "https://www.virustotal.com/api/v3/urls";
      const options = {
        method: "post",
        contentType: "application/x-www-form-urlencoded",
        headers: {
          "x-apikey": VIRUSTOTAL_API_KEY,
        },
        payload: buildUrlParams(params),
      };

      const response = UrlFetchApp.fetch(apiUrl, options);
      const jsonresult = JSON.parse(
        response.getContentText()
      ).data.id.toString();
      const result = jsonresult.split("-")[1];
      const output = getVirusTotalDataURL(result, event);
      return output;
    } catch (error) {
      return error.message;
    }
  });
}

function buildUrlParams(params) {
  return Object.keys(params)
    .map((key) => key + "=" + encodeURIComponent(params[key]))
    .join("&");
}

function getVirusTotalDataURL(result) {
  const url = "https://www.virustotal.com/api/v3/urls/" + result;

  const headers = {
    accept: "application/json",
    "x-apikey": VIRUSTOTAL_API_KEY,
  };

  const options = {
    method: "get",
    headers: headers,
  };

  try {
    let response = UrlFetchApp.fetch(url, options);
    let jsonResponse = JSON.parse(response.getContentText());
    return jsonResponse;
  } catch (error) {
    return error.message;
  }
}
```

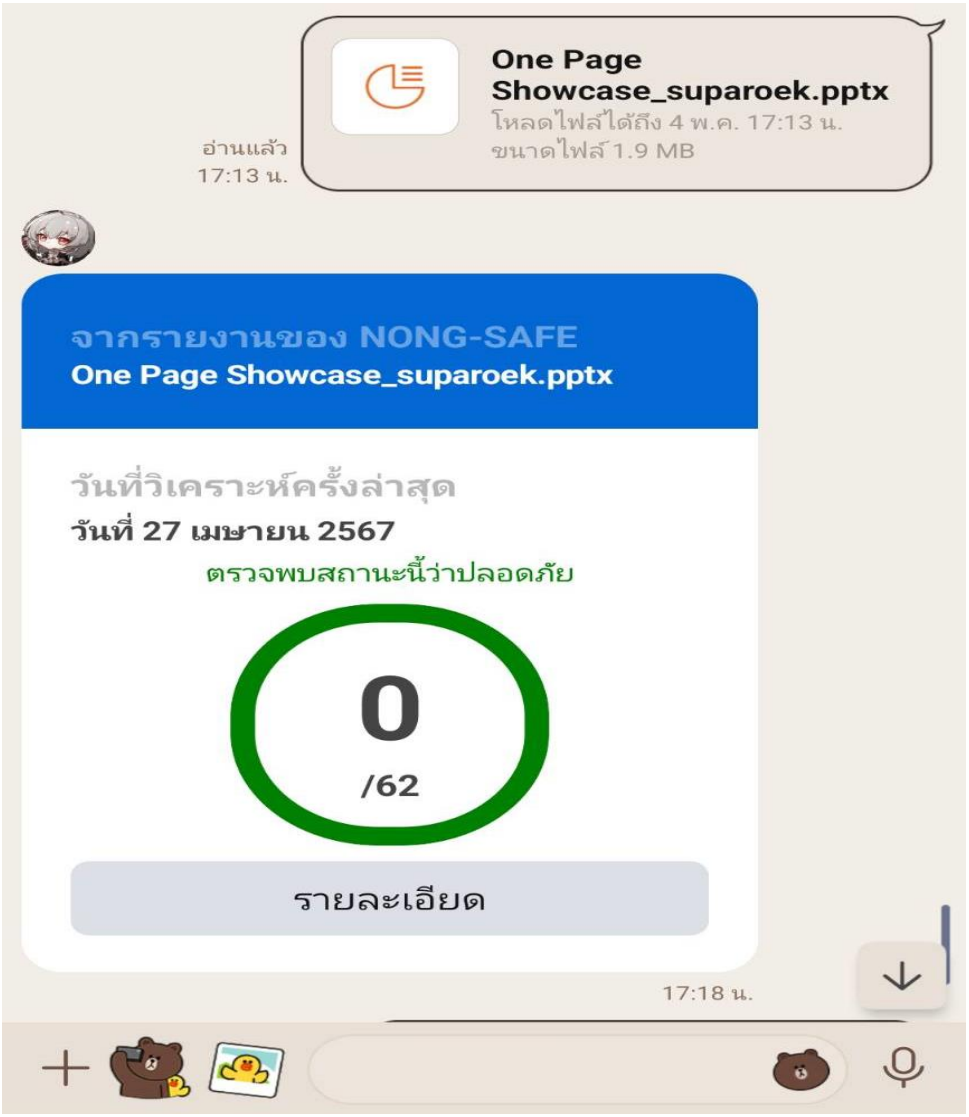
รูปที่ 1 ส่วนหนึ่งของโค้ดของโปรแกรมที่ใช้ในการตรวจสอบความปลอดภัยและความเสี่ยงของลิงก์ โดยใช้ Virustotal API (Virustotal, 2023c) โปรแกรมที่ใช้ในการตรวจสอบความปลอดภัยและความเสี่ยงของลิงก์ โดยใช้ Virustotal โค้ดด้านบนเป็นส่วนหนึ่งของระบบที่ใช้ในการตรวจสอบความปลอดภัยของลิงก์ที่ผู้ใช้ส่งมาผ่าน LINE Messaging API โดยใช้ VirusTotal API เพื่อวิเคราะห์ว่าลิงก์เหล่านั้นมีความเสี่ยงหรือไม่ ระบบนี้เหมาะสมกับงานวิจัยด้านการตรวจจับและแจ้งเตือนภัยคุกคามไซเบอร์แบบอัตโนมัติ ฟังก์ชัน processInputText() ใช้ Regular Expression (RegEx) ในการจับคู่และดึงลิงก์ที่มีรูปแบบ http, https, หรือ www. จากข้อความที่ผู้ใช้ส่งมา แล้วส่งลิงก์เหล่านั้นไปยัง VirusTotal API เพื่อขอการวิเคราะห์ โดยใช้คำขอ HTTP แบบ POST ซึ่งข้อมูลจะถูกแปลงเป็น application/x-www-form-urlencoded ผ่านฟังก์ชัน buildUrlParams() เพื่อส่งข้อมูลอย่างถูกต้อง หลังจากนั้น ฟังก์ชัน getVirusTotalDataURL() จะใช้ Token (id) ที่ได้รับจาก API เพื่อดึงผลการวิเคราะห์ เช่น ความน่าเชื่อถือของลิงก์และจำนวนเครื่องมือที่แจ้งว่าเป็นอันตราย ก่อนที่จะส่งการแจ้งเตือนผู้ใช้ผ่าน LINE เกี่ยวกับความเสี่ยงของลิงก์นั้น การทำงานของระบบนี้ช่วยเพิ่มความปลอดภัยในการสื่อสารผ่าน LINE โดยการแจ้งเตือนผู้ใช้เกี่ยวกับลิงก์ที่อาจเป็นอันตราย ซึ่งเหมาะสำหรับการศึกษาและพัฒนาเครื่องมือในการป้องกันภัยคุกคามไซเบอร์

```
function processFileContent(messageId, name) {
  const lineEndpoint =
    "https://api-data.line.me/v2/bot/message/" + messageId + "/content";
  const lineResponse = UrlFetchApp.fetch(lineEndpoint, {
    headers: {
      Authorization: "Bearer " + CHANNEL_ACCESS_TOKEN,
    },
  });

  try {
    const blob = lineResponse.getBlob();
    const output = getVirusTotalDataFile(
      blob.getBytes(),
      name,
      blob.getContentType()
    );
    return output;
  } catch (error) {
    return error.message;
  }
}

function getVirusTotalDataFile(fileContent, fileName, contentType) {
  const url = "https://www.virustotal.com/api/v3/files";
  const boundary = "boundary_" + Utilities.getUuid();

  const payload = Utilities.newBlob(
    "--" +
      boundary +
      "\r\n" +
      'Content-Disposition: form-data; name="file"; filename="' +
      fileName +
      '"\r\n' +
      "Content-Type: " +
      contentType +
      "\r\n\r\n" +
      fileContent +
      "\r\n" +
      "--" +
      boundary +
      "--"
  );

  const options = {
    method: "POST",
    headers: {
      "x-apikey": VIRUSTOTAL_API_KEY,
      "Content-Type": "multipart/form-data; boundary=" + boundary,
    },
    payload: payload.getBytes(),
  };

  try {
    const virusTotalResponse = UrlFetchApp.fetch(url, options);
    const analysisId = JSON.parse(virusTotalResponse.getContentText()).data.id;
    const analysisResult = getVirusTotalAnalysis(analysisId);
    return analysisResult;
  } catch (error) {
    return error.message;
  }
}

function getVirusTotalAnalysis(analysisId) {
  const url = "https://www.virustotal.com/api/v3/analyses/" + analysisId;
  const headers = {
```

รูปที่ 2 ส่วนหนึ่งของโค้ดของโปรแกรมที่ใช้ในการตรวจสอบความปลอดภัยและความเสี่ยงของไฟล์ โดยใช้ Virustotal API (Virustotal, 2023c) โปรแกรมที่ใช้ในการตรวจสอบความปลอดภัยและความเสี่ยงของไฟล์ โดยใช้ Virustotal โค้ดฟังก์ชัน processFileContent() และ getVirusTotalAnalysis() ในงานวิจัยนี้ มีบทบาทสำคัญในการวิเคราะห์ความเสี่ยงจากไฟล์ที่ผู้ใช้ส่งผ่านแอปพลิเคชัน LINE โดยระบบจะใช้ VirusTotal API ในการอัปโหลดไฟล์ ตรวจสอบมัลแวร์ และดึงผลวิเคราะห์แบบอัตโนมัติ โดยไฟล์ต่าง ๆ เช่น PDF หรือ ZIP จะถูกแปลงเป็นข้อมูลในรูปแบบ multipart/form-data เพื่อให้สามารถส่งผ่าน HTTP ได้ตามมาตรฐาน พร้อมแนบชื่อและชนิดของไฟล์ จากนั้นจะดึง analysisId เพื่อใช้ในการเรียกผลวิเคราะห์จาก VirusTotal API ขั้นตอนทั้งหมดนี้ถูกออกแบบให้เหมาะสมกับการพัฒนาเครื่องมือแจ้งเตือนภัยไซเบอร์ในบริบทการใช้งานจริง โดยเฉพาะบนแพลตฟอร์ม LINE ซึ่งช่วยเพิ่มความมั่นใจและความปลอดภัยให้แก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ



รูปที่ 3 ผลลัพธ์ของการสแกนและการประเมินความเสี่ยงจากระบบตรวจสอบและป้องกันความปลอดภัย ลิงก์ (LINK) ส่วนตัวเลขผลลัพธ์การประเมินความเสี่ยงเป็นอันตราย



รูปที่ 4 ผลลัพธ์ของการสแกนและการประเมินความเสี่ยงจากระบบตรวจสอบและป้องกันความปลอดภัยไฟล์ (FILE) ส่วนตัวเลขผลลัพธ์การประเมินความเสี่ยงเป็นปลอดภัย

จากตารางที่ 1 และรูปที่ 1 - 4 อธิบายถึงส่วนการทำงานและผลลัพธ์ของการป้องกันและอธิบายข้อมูลที่เกี่ยวข้องกับการสแกนและการประเมินความเสี่ยงจากระบบตรวจสอบและป้องกันความปลอดภัย โดยมีรายละเอียดดังนี้ จำนวนผลลัพธ์ของการสแกนทั้งหมด (R) จำนวนผลลัพธ์การสแกนที่ปลอดภัย (RS) จำนวนผลลัพธ์การสแกนที่มีความอันตราย (RF) เปอร์เซ็นต์ของผลลัพธ์การสแกนที่มีความอันตรายต่อผลการสแกนทั้งหมด (Hazard) ในตารางที่กำหนดมีการแบ่งข้อมูลตามชนิดของข้อมูล คือ ไฟล์ (FILE) และ ลิงก์ (LINK) โดยแยกแต่ละชนิดออกจากกันเพื่อให้เห็นภาพรวมของผลการสแกนของแต่ละชนิดได้ชัดเจนขึ้น การวิเคราะห์ผลการสแกนแสดงว่า ในทั้งหมด 1000 รายการที่สแกน มี 950 รายการที่ปลอดภัย (RS) และ 50 รายการที่มีความอันตราย (RF) ซึ่งร้อยละของความอันตรายที่มีต่อทั้งหมด (Hazard) คือ 5% ในการสแกนลิงก์ มีทั้งหมด 840 รายการ โดย 800 รายการปลอดภัยและ

40 รายการมีความอันตราย ซึ่ง Hazard คือ 5% ในการสแกนไฟล์ มีทั้งหมด 160 รายการ โดย 150 รายการปลอดภัยและ 10 รายการมีความอันตราย ซึ่ง Hazard คือ 6.67%

ตารางที่ 2 ตารางคำนวณค่าร้อยละจากผลการสแกนทั้งหมดและแยกตามหมวดหมู่

ข้อมูล	RS	RF
All	95.00%	5.00%
LINK	95.24%	4.76%
FILE	93.75%	6.25%

จากตารางที่ 2 อธิบายให้เห็นภาพรวมเกี่ยวกับการแยกแยะความปลอดภัยและความเสี่ยงในผลการสแกนของไฟล์และลิงก์ทั้งหมดที่ได้รับการวิเคราะห์โดยระบบตรวจสอบและป้องกันความปลอดภัยด้วยไวรัสโททัล โดยในทุกกรณี การสแกนได้รับผลสำเร็จสูงเมื่อเทียบกับความเสี่ยงของผลลัพธ์การสแกนที่พบในไฟล์และลิงก์ที่ตรวจพบว่ามีความอันตราย

ตารางที่ 3 ตารางแสดงค่าเฉลี่ยของความอันตราย (Hazard) ที่คำนวณจากผลการสแกนทั้งหมดและแยกตามหมวดหมู่

หมวดหมู่	Hazard
All	5.22
LINK	4.76
FILE	6.25

จากตารางที่ 3 สามารถสรุปได้ว่าค่าเฉลี่ยของความอันตรายในผลการสแกนทั้งหมดคือ 5.22% โดยมีความแตกต่างของค่าเฉลี่ยของความอันตรายในไฟล์และลิงก์ โดยมีค่าสูงสุดที่ 6.25% ในหมวดหมู่ของไฟล์ และค่าต่ำสุดที่ 4.76% ในหมวดหมู่ของลิงก์

สรุปและอภิปรายผล

จากการทดสอบตามวัตถุประสงค์เพื่อการตรวจจับมัลแวร์ในไฟล์หรือลิงก์ที่อาจเป็นอันตรายโดยใช้เทคโนโลยีที่ทันสมัยและมีประสิทธิภาพและแจ้งเตือนป้องกันความปลอดภัยสำหรับการสื่อสารผ่านแอปไลน์ การวิจัยครั้งนี้มุ่งเน้นการพัฒนาระบบตรวจสอบและแจ้งเตือนมัลแวร์ผ่านแอปพลิเคชัน LINE โดยใช้เทคโนโลยี VirusTotal API ซึ่งเป็นการสร้างระบบใหม่ที่ยังไม่เคยมีผลงานใดพัฒนาในลักษณะเดียวกันมาก่อน ผู้วิจัยได้ออกแบบและพัฒนาเครื่องมือเองทั้งหมด และดำเนินการทดสอบกับ 1,000 ตัวอย่าง ผ่านการกระจายระบบผ่าน Facebook เพื่อศึกษา ประสิทธิภาพ และ ความพึงพอใจของผู้ใช้งาน ผลการวิจัยพบว่า ระบบตรวจสอบและป้องกันความปลอดภัยสำหรับการสื่อสารผ่านแอปไลน์ด้วยไวรัสโททัลได้เสนอผลการสแกนและวิเคราะห์ข้อมูลการใช้งานอย่างละเอียด โดยใช้ข้อมูลจำนวนไฟล์และลิงก์ 1,000 ตัวอย่าง เพื่อตรวจสอบความเสี่ยงที่อาจเกิดขึ้นในการสื่อสารออนไลน์ ผลการวิเคราะห์แสดงให้เห็นถึงค่าความอันตรายที่เกี่ยวข้องกับการใช้งานแอปไลน์ โดยมีค่าเฉลี่ยที่ประมาณ 5.22% ซึ่งการแบ่งหมวดหมู่ตามลักษณะของไฟล์และลิงก์ยังแสดงให้เห็นถึงความแตกต่างในระดับความเสี่ยง โดยมีค่าสูงสุดที่ 6.67% ในหมวดหมู่ไฟล์ และค่าต่ำสุดที่ 4.76% ในหมวดหมู่ลิงก์ โมเดลแสดงให้เห็นถึงความแข็งแกร่งรวดเร็วและความแม่นยำที่มีอยู่ในปัจจุบัน ซึ่งเป็นการแสดงให้เห็นถึงความมีประสิทธิภาพของมันในสถานการณ์จริง ด้านประสิทธิภาพของระบบไวรัสโททัลในการตรวจจับมัลแวร์สอดคล้องกับงานวิจัยของงาน Karthic, A. R. M., and Nurul, A. A. (2023) พบว่า ประเมินประสิทธิภาพของระบบตรวจจับมัลแวร์ในบริบทนี้ ไวรัสโททัล ได้รับคะแนนที่สมบูรณ์แบบ 100% ในเมตริกเหล่านี้ทั้งหมด ซึ่งบ่งชี้ว่ามันจำแนกมัลแวร์ในชุดข้อมูลอย่างถูกต้อง และด้านป้องกันความปลอดภัยสอดคล้องกับงานวิจัยของ Aleieldin, S., Sebastian, B. and Alexander, P. (2020) พบว่าเป็นแพลตฟอร์มออนไลน์ที่ใช้กันอย่างแพร่หลายสำหรับการวิเคราะห์มัลแวร์ ให้ข้อมูลเชิงลึกที่มีค่าแก่ชุมชนวิจัยเกี่ยวกับวิธีใช้ประโยชน์จากไวรัสโททัล สำหรับการสแกนแอปอย่างเหมาะสมตามรายงานการสแกนโดยการจัดการกับความท้าทายและข้อจำกัด เพื่อแนะนำนักวิจัยในการใช้แพลตฟอร์มอย่างมีประสิทธิภาพในการวิเคราะห์และตรวจจับมัลแวร์ แต่มีข้อจำกัดสำหรับบัญชีฟรีจะมีข้อจำกัดจำนวนคำขอ (rate limit) จากที่งานวิจัยนี้ได้ทำการตรวจสอบไฟล์หรือลิงก์และแจ้งเตือนป้องกันความปลอดภัยสำหรับการสื่อสารผ่านแอปไลน์ ช่วยให้ผู้ใช้ไลน์เข้าใจและเพิ่มความมั่นใจในการสื่อสารผ่านแอปไลน์ได้อย่างมีประสิทธิภาพและเชื่อถือได้

ข้อเสนอแนะ

ข้อเสนอแนะในการนำผลการวิจัยไปใช้

ธุรกิจ/ หน่วยงาน/ องค์กร / บุคคลทั่วไปที่เกี่ยวข้องกับการใช้ไลน์หรือประชากรผู้ใช้ไลน์ สามารถนำผลการศึกษาไปใช้ได้ดังนี้

1) การใช้ประโยชน์ในองค์กร นำผลการวิจัยไปใช้ในองค์กรเพื่อปรับปรุงระบบตรวจสอบและป้องกันความปลอดภัย โดยให้ความสำคัญกับการพัฒนาระบบที่สามารถตรวจจับและป้องกันมัลแวร์ได้อย่างมีประสิทธิภาพ

2) การแบ่งปันข้อมูล แบ่งปันผลการวิจัยกับชุมชนวิชาการและองค์กรที่เกี่ยวข้อง เพื่อเสริมสร้างความร่วมมือในการพัฒนาเทคโนโลยีความปลอดภัยของข้อมูล

3) การใช้เพื่อการศึกษา นำผลการวิจัยไปใช้ในการสอนหรือฝึกอบรมเพื่อเพิ่มความเข้าใจและความสามารถในการจัดการความปลอดภัยของบุคคลภายในองค์กร

ข้อเสนอแนะในการวิจัยครั้งต่อไป

จากผลสรุปการศึกษา ผู้วิจัยมีข้อเสนอแนะเพื่อเป็นประโยชน์สำหรับการพัฒนาเครื่องมือและศึกษาความพึงพอใจของผู้ใช้งานวิจัยในครั้งต่อไป ดังนี้

1) การพัฒนาระบบอัตโนมัติ ศึกษาและพัฒนาระบบตรวจสอบและป้องกันความปลอดภัยที่สามารถทำงานอัตโนมัติเพื่อตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว

2) การใช้เทคโนโลยีสมัยใหม่ ใช้เทคโนโลยีเชิงลึกและการเรียนรู้ของเครื่อง (machine learning) เพื่อพัฒนาระบบที่มีความสามารถในการจำแนกประเภทมัลแวร์และการตรวจสอบความปลอดภัยอย่างเชื่อถือได้อย่างมีประสิทธิภาพ

3) การศึกษาแนวโน้มของการโจมตี ศึกษาแนวโน้มและรูปแบบการโจมตีทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็วเพื่อปรับปรุงระบบตรวจจับและป้องกันความปลอดภัยให้เหมาะสมกับสถานการณ์ปัจจุบัน

4) การสร้างฐานข้อมูล สร้างฐานข้อมูลที่มีข้อมูลมัลแวร์และแบบจำลองการโจมตีที่ครอบคลุมทั้งแบบที่เก่าและใหม่ เพื่อใช้ในการศึกษาและพัฒนาระบบตรวจจับและป้องกันความปลอดภัยได้อย่างมีประสิทธิภาพ

เอกสารอ้างอิง

Aleieldin, S., Sebastian, B. and Alexander, P. (2020). Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection. ACM Transactions on Privacy and Security, 1, 2, 34 - 35.

Ashkan, H. and Ashutosh, C. (2021). 2020 Phishing Trends With PDF Files [Online]. Retrieved November 28, 2023, Available : https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/.

Chiradeep, B. M. (2021). What Is Malware Analysis? Definition, Types, Stages, and Best Practices. Spiceworks.

Karthic, A. R. M., and Nurul, A. A. (2023). Cuckoo Sandbox VS Virus Total: Categorical Analysis between Sandboxes. Applied Information Technology And Computer Science, 4, 43.

LINE, D. (2022). Messaging API overview [Online]. Retrieved November 28th, 2023, Available : https://developers.line.biz/en/docs/messaging-api/overview/.

LINE. (2566). 12 years of LINE application with 6 leaders who have elevated the lives of Thai people to the digital world in dimensions [Online]. Retrieved November 28th, 2023, Available : https://linecorp.com/th/pr/news/th/2023/4621.

Yamane, T. (1967). Statistics: An Introductory Analysis. New York : Harper and Row.

VirusTotal, V. (2023). How it works [Online]. Retrieved November 28th, 2023, Available : https://docs.virustotal.com/docs/how-it-works.

Virustotal. (2023a). API Scripts and client libraries [Online]. Retrieved November 28th, 2023, Available : https://docs.virustotal.com/docs/api-scripts-and-client-libraries.

Virustotal. (2023b). Leverage 15 years of malicious sightings and the world-largest live threat feed to make better and faster decisions to improve your security posture in an automated fashion [Online]. Retrieved November 28th, 2023, Available : https://www.virustotal.com/gui/services-overview.

Virustotal. (2023c). VirusTotal API v3 Overview [Online]. Retrieved November 28th, 2023, Available : https://docs.virustotal.com/reference/overview.

Virustotal. (2023d). YARA in a nutshell [Online]. Retrieved November 28th, 2023, Available : https://github.com/VirusTotal/yara.