บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหา

ปัจจุบันปัญหาอาชญากรรมในโลกออนไลน์ จากข้อมูลทางข่าวสารหนังสือพิมพ์ โทรทัศน์ หรือ สื่อทางอิเล็กทรอนิกส์ เว็บไซต์ ต่าง ๆ มีแนวโน้มที่จะรุนแรงขึ้น ทั้งในด้านสถิติตัวเลข การก่ออาชญากรรม การเมือง ธุรกิจ ทรัพย์สิน และวิธีการประกอบอาชญากรรมของการโจมตีเว็บไซต์ ที่เกิดขึ้น เช่น การขโมยข้อมูลสำคัญขององค์กรขนาดใหญ่ไปจนถึงขนาดเล็ก การก่อกวนเว็บไซต์ทางธุรกิจคู่แข่ง เป็นต้น จากการนำเสนอภาคข่าวเกี่ยวกับการกระทำผิดผ่านสื่อต่าง ๆ ทั้งจากโทรทัศน์ วิทยุ หนังสือพิมพ์ และอินเทอร์เน็ต มีจำนวนผู้กระทำความผิด และผู้ที่เป็นเหยื่อของการโจมตีเว็บไซต์ เป็นจำนวนมาก ซึ่งข้อมูลเหล่านี้ได้ถูกจัดเก็บขึ้นมาผ่านหน่วยงาน IEEE Conference on Communications and Network Security, Philadelphia, PA USA. ปัจจุบัน ผ่านเว็บไซต์ ocslab.hksecurity.net ข้อมูลเหล่านี้ถูกจัดเก็บมาตั้งแต่ปี 2019-2021 เพื่อเป็นข้อมูลที่บอกสถิติในการโจมตีเว็บไซต์ ที่เกิดขึ้นในเหตุการณ์ต่าง ๆ ในแต่ละประเทศ เช่น ประเทศสหรัฐอเมริกา ที่ศูนย์กลางของธุรกิจออนไลน์ต่างๆ ไม่ว่าจะเป็น Google , Facebook , Apple เป็น ซึ่งมีบทบาทต่อความสำคัญในการดำเนินการตลาดอย่างมาก เนื่องจากเป็นศูนย์กลางของกิจกรรมต่าง ๆ ทุกด้าน และยังก่อให้เกิดการลงทุนต่าง ๆ มากมาย เป็นแหล่งที่มีผู้คนจับตามองเห็นกันและกันและอาจโดนเพ่งเล็งขึ้นได้จึงอาจทำให้เกิดอาชญากรรมทางไซเบอร์ขึ้นโดยอาจไม่รู้ตัว

การโจมตีเว็บไซต์มีแต่ความสูญเสียและก่อให้เกิดผลเสียทั้งด้านเศรษฐกิจ สังคม ความปลอดภัยในชีวิตและทรัพย์สินของประชาชนตลอดจนความมั่นคงของชาติ ความสูญเสียการโจมตีเว็บไซต์ มีมูลค่าต่อทรัพย์สินและจิตใจ ในปัจจุบัน การโจมตีเว็บไซต์ มีแนวโน้มเพิ่มสูงขึ้นตามการขยายตัวของธุรกิจและการขยายตัวของประเทศ เท่านั้นไม่พอ รูปแบบการโจมตีเว็บไซต์ ยังก้าวหน้าไปตามความเจริญของเทคโนโลยี ส่งผลให้การปราบปรามการอาชญากรรมทางไซเบอร์ เป็นไปด้วยความยากลำบากกว่าแต่ก่อน เช่น อาชญากรทางไซเบอร์มีความรู้ความสามารถและอุปกรณ์ที่ทันสมัยขึ้น แหล่งเรียนรู้ที่เปิดกว้างขึ้น การแอบอ้างหรือซ่อนตัวตนเพื่อใช้ในการโจมตีเว็บไซต์ โดยเว็บไซต์ในประเทศไทยที่นำเสนอข้อมูลเกี่ยวกับการแฮกเว็บไซต์ ยังไม่ค่อยมีการนำเสนอการโจมตีทางเว็บไซต์มากนัก โดยส่วนมากจะเป็นเว็บไซต์ที่มาจากต่างประเทศมีข้อจำกัดเรื่องภาษาที่นำเสนอ ซึ่งมีปัญหาในการเข้าถึงข้อมูลสำหรับคนไทยได้ จากการวิเคราะห์ข้อมูลรายงานการโจมตีเว็บไซต์ เป็นการนำเอาชุดข้อมูลจากเว็บไซต์ ocslab.hksecurity.net มาวิเคราะห์ในเชิงลึก เพื่อให้ทราบสาเหตุการโจมตีเว็บไซต์ ที่เกิด ในอดีตและแนวโน้มที่จะเกิดขึ้นในอนาคต และการโจมตีในรูปแบบไหน โดย เว็บไซต์ ocslab.hksecurity.net เป็น ห้องปฏิบัติการวิจัยการแฮกและตอบโต้ (EST. ในปี 2010) พื้นที่วิจัย

หลักของ Hacking and Countermeasure Research Lab (HCR Lab) คือการรักษาความปลอดภัยที่ขับเคลื่อนด้วยข้อมูล ซึ่งอิงจากการเรียนรู้ของเครื่องและเทคโนโลยีการขุดข้อมูลเพื่อดึงและเรียนรู้ความรู้ที่เป็นประโยชน์จากข้อมูลขนาดใหญ่ โดยเฉพาะอย่างยิ่ง HCR Lab มีชุดข้อมูลที่เป็นเอกลักษณ์และมีค่าซึ่งรวบรวมจากบริการในโลกแห่งความเป็นจริง เช่น ข้อมูลบริการเกมออนไลน์ ข้อมูลการชำระเงินผ่านมือถือและธุรกรรมอีคอมเมิร์ซ ข้อมูลการขับขี่รถยนต์และการโจมตี HCR Lab มีส่วนสนับสนุนในด้านความปลอดภัยที่ขับเคลื่อนด้วยข้อมูลอย่างต่อเนื่องโดยการแบ่งปันชุดข้อมูลนี้ต่อสาธารณะ

จากปัญหาดังกล่าวผู้วิเคราะห์มีความคิดที่จะนำชุดข้อมูลมา การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อใช้สำหรับเผยแพร่ข้อมูลบนเว็บไซต์ มาประมวลผลข้อมูล แยกแยะและพิจารณาข้อมูลผ่านโปรแกรมให้ตรงตามความถูกต้อง โดยผู้วิเคราะห์ข้อมูลได้นำชุดข้อมูลมาทำกระบวนการวิเคราะห์ข้อมูล พิจารณาการแบ่งแยกข้อมูลในการจำแนกข้อมูลด้วยเทคนิค Classification จะแบ่งแยกออกเป็นแต่ละประเภท เช่น ปีที่โจมตี ประเทศที่โดนโจมตี กลุ่มแฮกเกอร์ที่โจมตี ระบบปฏิบัติการที่โดนโจมตี เป็นต้น ทำให้ชุดข้อมูลที่ได้มาในการทำ Decision tree มีความเข้าใจในข้อมูลมากขึ้น

โดยผู้วิเคราะห์มีการสร้างเว็บไซต์เพื่อเผยแพร่ข้อมูล การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 โดยใช้โปรแกรม Visual Studio Code ใช้ในการสร้างเว็บไซต์ ด้วยชุดคำสั่งภาษา PHP , HTML4, HTML5 (Hyper Text Markup Language) ชุดคำสั่ง CSS (Cascading Style Sheets) และมีฐานข้อมูลเป็นชุดคำสั่งภาษา MySQL และนำชุดข้อมูลการโจมตีทางเว็บไซต์ ปี 2019-2021 ที่ได้จากเว็บไซต์ ocslab.hksecurity.net ซึ้งขอใช้ข้อมูลต้องติดต่อขอทางอีเมล ocslab@hksecurity.net เท่านั้น นำข้อมูลที่ได้ มาเติมข้อมูลที่ขาดหายไปให้ครบถ้วน จากนั้นวิเคราะห์ข้อมูลด้วยเทคนิคทางดาต้า ไมน์นิ่ง แบบการจำแนกประเภทข้อมูล (Classification) และใช้เทคนิคการจำแนกประเภท ข้อมูล ด้วยการสร้างโมเดลการตัดสินใจแบบต้นไม้ (Decision Tree) ด้วยโปรแกรม RapidMiner เพื่อให้ข้อมูลมีความสมบูรณ์ทำออกมาแสดง Data Visualization อยู่ในกราฟรูปแบบต่างๆ ใช้โปรแกรม Tableau Public และเผยแพร่ข้อมูลสารสนเทศออกทางเว็บไซต์ เพื่อให้ผู้ใช้งานทั่วที่มีความสนใจได้ทราบถึงการวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 ที่เกิดขึ้น

ซึ่งข้อมูลที่นำมาวิเคราะห์นี้ ผู้ที่สนใจหรือบุคคลทั่วไปสามารถนำข้อมูลที่ผ่านการวิเคราะห์เกี่ยวกับ การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 สามารถนำไปใช้ประโยชน์เกี่ยวกับการอบรม , การทำงานวิจัย , การสอนหรือศึกษาเพื่อเติม , การนำไปเปรียบเทียบข้อมูลภายในองค์กร ต่างๆเป็นต้น

1.2 วัตถุประสงค์

1.2.1 เพื่อการวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021

1.2.2 เพื่อเผยแพร่ข้อมูลการวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 บนเว็บไซต์

1.3 ประโยชน์ที่จะได้รับ

1.3.1 ได้ข้อมูลสารสนเทศของ ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021

1.3.2 ได้เผยแพร่ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021

1.4 ขอบเขต

1.4.1 ขอบเขตผู้วิเคราะห์ข้อมูล

1.4.1.1 ผู้วิเคราะห์ข้อมูลทำการรวบรวมข้อมูล จากนั้นทำการตรวจสอบรายละเอียด ของชุดข้อมูลที่ใช้ข้อมูลทั้งหมด หรือที่จำเป็นต้องเลือกข้อมูลบ้างส่วนมาใช้ในการวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 จากเว็บไซต์ ocslab.hksecurity.net

1.4.1.2 ผู้วิเคราะห์ข้อมูลทำการกลั่นกรองข้อมูล (Data Cleaning) ข้อมูลที่ทำกระบวนการนี้อาจจะต้องมีการทำข้อมูลให้ถูกต้อง เช่น ข้อมูลที่ผิดรูปแบบ เติมข้อมูลที่ขาดหายไปให้ครบถ้วน ให้ข้อมูลมีความสมบูรณ์ ตัดข้อมูลที่ไม่จำเป็นออก เป็นต้น

1.4.1.3 ผู้วิเคราะห์ข้อมูลทำการแปลงข้อมูล (Data Transformation) เตรียมข้อมูลให้อยู่ในรูปแบบที่พร้อมนำไปวิเคราะห์ ใช้เทคนิค (Classification)

1.4.1.4 ผู้วิเคราะห์ข้อมูลวิเคราะห์ข้อมูลด้วยเทคนิคทางดาต้า ไมน์นิ่ง แบบการจำแนกประเภทข้อมูล (Classification) และใช้เทคนิคการจำแนกประเภท ข้อมูล ด้วยการสร้างโมเดลการตัดสินใจแบบต้นไม้ (Decision Tree)

1.4.1.5 ผู้วิเคราะห์ข้อมูลได้ทำการประมวลผลโดยใช้โปรแกรม (Weka 3.8.5) และ (Rapid Miner)

1.4.1.6 ผู้วิเคราะห์ข้อมูลได้นำเสนอข้อมูลแบบ (Visualization) ด้วยการแสดงผลข้อมูลในรูปแบบของภาพ ด้วยโปรแกรม (Tableau Public) และ (API Google charts)

1.4.1.7 นำข้อมูลที่วิเคราะห์มาแสดงผล ข้อมูลบนหน้าเว็บไซต์ แสดงผล (Data Visualization) นำเสนอ และเผยแพร่ข้อมูลผ่าน เว็บไซต์โดยเว็บจะพัฒนาโดยใช้ภาษา

HTML, PHP, JavaScript และชุดคำสั่ง CSS เพื่อนำการวิเคราะห์ข้อมูลด้วยโมเดลที่เลือกใช้ และใช้ Tableau Public, API Google Charts ร่วมกับ การนำเสนอข้อมูลด้วยกราฟ และ Dashboard สำหรับแสดงผลข้อมูลภาพ จากข้อมูลที่ผ่านการวิเคราะห์ แล้วภายในเว็บ

1.4.2 ขอบเขตเว็บไซต์

1.4.2.1 สามารถดูข้อมูลความรู้และบทความเกี่ยวกับ ภัยคุกคามการโจมตีบนเว็บไซต์

1.4.2.2 สามารถดูทฤษฎีและกระบวนการที่วิเคราะห์ข้อมูล CRISP-DM ของเว็บไซต์

1.4.2.3 สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ของประเทศไทย

1.4.2.4 สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์รวมของทุกประเทศ

1.4.2.5 สามารถนำเสนอ กฎที่ได้จากโมเดล Decision tree ให้มีความน่าสนใจ

1.4.2.6 สามารถนำเว็บไซต์ ไปนำเสนอ อบรมให้ความรู้หรือใช้ในการศึกษาทางด้านภัยคุกคามทางด้านเว็บไซต์ได้

1.4.2.7 เว็บไซต์การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 รองรับภาษาทั้งหมด 109 ภาษา

1.4.2.8 เว็บไซต์มีการใช้ google recaptcha เพื่อป้องกันเว็บไซต์จากสแปม

1.4.2.9 มีการป้องการเข้าสู่ระบบที่ไม่สำเร็จจะทำการบล็อก การเข้าสู่ระบบชั่วคราว

1.4.3 ขอบเขตสมาชิกเว็บไซต์

1.4.3.1 สามารถสมัครสมาชิกได้

1.4.3.2 สามารถเข้าสู่ระบบได้ โดย ไอดี และ รหัสผ่าน

1.4.3.3 สามารถแก้ไขข้อมูลส่วนตัวได้

1.4.3.4 สามารถดูข้อมูลความรู้และบทความเกี่ยวกับ ภัยคุกคามการโจมตีบนเว็บไซต์

1.4.3.5 สามารถดูทฤษฎีและกระบวนการที่วิเคราะห์ข้อมูล CRISP-DM ของเว็บไซต์

1.4.3.6 สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ของประเทศไทย

1.4.3.7 สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์รวมของทุกประเทศ

1.4.3.8 สามารถดาวน์โหลดรีพอร์ตข้อมูลแดชบอร์ดภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในรูปแบบของ PDF ได้

1.4.3.9 สามารถกรอกข้อมูลลงบนเว็บไซต์เพื่อเพิ่มข้อมูลได้ (ชุดข้อมูลที่มีจำนวนน้อย)

- สามารถแก้ไขข้อมูลที่กรอกเข้ามาได้
- จำกัดการแก้ไขได้เฉพาะสมาชิกที่เป็นผู้กรอกข้อมูลเท่านั้น
- สามารถดูคำแนะนำการใช้งานการกรอกข้อมูลลงบนเว็บไซต์ได้
- สามารถดูข้อมูลที่กรอกเข้ามาในรูปแบบของตารางได้

1.4.3.10 สามารถอัปโหลดชุดข้อมูล .CSV (ชุดข้อมูลที่มีจำนวนมาก) เพื่อให้ผู้ดูแลเว็บไซต์ได้นำได้ชุดข้อมูลไปผ่านกระบวนการวิเคราะห์ต่าง ๆ และให้ผู้ดูแลเว็บไซต์อัปเดตข้อมูลลงเว็บไซต์นี้

- สามารถดูสถานะของข้อมูลที่ผู้ดูแลเว็บไซต์ดำเนินการอยู่ได้
- สามารถลบการอัปโหลดชุดข้อมูลได้
- จำกัดการลบได้เฉพาะสมาชิกที่เป็นผู้อัปโหลดข้อมูลเท่านั้น
- สามารถดูคำแนะนำการใช้งานการอัปโหลดชุดข้อมูลให้ผู้ดูแลระบบได้
- สามารถดูชุดข้อมูลที่อัปโหลดในรูปแบบของตารางได้

1.4.3.11 สามารถดาวน์โหลดข้อมูลที่ผ่านกระบวนการวิเคราะห์ข้อมูลและจัดการจากผู้ดูแลเว็บไซต์ได้เพื่อนำไปศึกษาต่อ

1.4.3.12 สามารถทำแบบฟอร์มการประเมินทางด้านเว็บไซต์และด้านการวิเคราะห์ข้อมูล ของเว็บไซต์ การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 ได้

1.4.3.13 สามารถติดต่อสอบถามเพิ่มเติมจากผู้ดูแลเว็บไซต์ผ่านทางระบบ Line Notify ได้

1.4.4 ขอบเขตผู้ดูแลเว็บไซต์

1.4.4.1 สามารถเข้าสู่ระบบได้ โดย ไอดี และ รหัสผ่าน

- มีการแจ้งเตือนการเข้าสู่ระบบ ผ่าน Line Notify

1.4.4.2 สามารถแก้ไขข้อมูลส่วนตัวได้

1.4.4.3 สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ของประเทศไทย

1.4.4.4 สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์รวมของทุกประเทศ

1.4.4.5 สามารถดาวน์โหลดรีพอร์ตข้อมูลแดชบอร์ดภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในรูปแบบของ PDF ได้

1.4.4.6 สามารถกรอกข้อมูลลงบนเว็บไซต์เพื่อเพิ่มข้อมูลได้ (ชุดข้อมูลที่มีจำนวนน้อย)

- สามารถแก้ไขข้อมูลที่กรอกเข้ามาได้
- สามารถลบข้อมูลที่กรอกเข้ามาได้
- สามารถดูคำแนะนำการใช้งานการกรอกข้อมูลลงบนเว็บไซต์ได้
- สามารถดูข้อมูลที่กรอกเข้ามาในรูปแบบของตารางได้

1.4.4.7 สามารถอัปโหลดชุดข้อมูล .CSV (ชุดข้อมูลที่มีจำนวนมาก) เพื่ออัปเดตแดชบอร์ดที่แสดงในเว็บไซต์ เป็นข้อมูลที่ผ่านกระบวนการวิเคราะห์ต่าง ๆ และจัดรูปแบบแล้ว

- แสดงจำนวนข้อมูลทั้งหมดที่มีอยู่ในฐานข้อมูลได้

1.4.4.8 สามารถจัดการชุดข้อมูลที่สมาชิกอัปโหลดมาได้

- สามารถแก้ไขสถานะของการดำเนินการได้
- สามารถดาวน์โหลดชุดข้อมูลได้
- สามารถลบชุดข้อมูลได้
- สามารถดูคำแนะนำการใช้งานการจัดการชุดข้อมูลได้

1.4.4.9 สามารถจัดการสมาชิกได้

- สามารถแก้ไขข้อมูลของสมาชิกได้
- สามารถลบสมาชิกได้

1.5 เครื่องมือที่ใช้ในการพัฒนา

1.5.1 Hardware

1.5.1.1 Acer Aspire F 15 intel core i5, 7200U RAM 4GB

1.5.1.2 Hp pavilion AMD Ryzen 5 4600U, RAM 8GB

1.5.2 Software

1.5.2.1 โปรแกรม Tableau Public เพื่อใช้ในการแสดงข้อมูลในรูปแบบของภาพ

1.5.2.2 โปรมแกรม RapidMiner ใช้ในการสร้างโมเดล Decision Tree

1.5.2.3 โปรมแกรม Visual Studio Code ใช้ในการสร้างเว็บไซต์

1.5.2.4 โปรแกรม Adobe XD ใช้ในการออกแบบหน้าเว็บไซต์

1.5.2.5 Microsoft Office Visio 2019 ใช้ในการทำ Data Flow Diagram : DFD

1.5.2.6 Microsoft Office Word 2019 ใช้ในการทำเอกสาร

1.5.2.7 Microsoft Office Excel 2019 ใช้ในการจัดการชุดข้อมูล

1.5.2.8 ระบบปฏิบัติการ Window 10 ใช้ในการเปิดซอฟต์แวร์ต่าง ๆ

1.5.2.9 โปรแกรม Weka 3.8.5 ใช้ในการวิเคราะห์ข้อมูลด้วยเทคนิคเหมืองข้อมูล

1.5.2.10 โปรแกรม XAMPP 7.3.29 ใช้ในการจำลอง Web Server

1.5.2.11 โปรแกรม FileZilla ใช้ติดต่อกับ FTP Server เพื่ออับโหลดไฟล์

1.5.2.12 โปรแกรม phpMyAdmin ทำงานบน Web Server ที่ใช้ควบคุมจัดการฐานข้อมูล

1.5.2.13 ชุดคำสั่งภาษา HTML5, CSS, JAVASCRIPT

1.5.2.14 ชุดคำสั่ง PHP, MySQL

1.5.2.15 ใช้ API Google Charts เพื่อแสดงผลกราฟที่ต้องการนำไปใช้ร่วมกับเว็บไซต์

1.6 สถานที่ใช้ในการดำเนินการศึกษาและรวบรวมข้อมูล

1.6.1 มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา ตั้งที่อยู่ที่ 128 ถนนห้วยแก้ว ตำบลช้างเผือก อำเภอเมืองเชียงใหม่ จังหวัดเชียงใหม่ 50300

1.6.2 สำนักหอสมุด มหาวิทยาลัยเชียงใหม่ 239 ถนน ห้วยแก้ว ตำบลสุเทพ อำเภอเมืองเชียงใหม่ เชียงใหม่ 50200

1.7 ระยะเวลาในการดำเนินการ

ตารางที่ 1.1 ระยะเวลาในการดำเนินงาน

แผนการดำเนินการ	2564					
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1. ค้นหาและศึกษา ข้อมูล	↔					
2. ทำความเข้าใจ ข้อมูล		↔				
3. เตรียมข้อมูล		←	→			
4. สร้างแบบจำลอง			←	→		
5. ประเมินผล				←	→	
6. นำเสนอข้อมูลบน Web Browser				←	→	
7. จัดทำเอกสาร ประกอบโครงงาน	←	→	→	→	→	→

1.8 นิยามศัพท์เฉพาะ

1.8.1 Hacker

Hacker คือ ผู้ที่มีความรู้ความเข้าใจในระบบคอมพิวเตอร์อย่างสูงมาก ไม่ว่าจะเป็นเรื่องเครือข่าย, ระบบปฏิบัติการ จนสามารถเข้าใจว่าระบบมีช่องโหว่ตรงไหน หรือสามารถไปค้นหาช่องโหว่ได้จากตรงไหนบ้าง เมื่อก่อนภาพลักษณ์ของ Hacker จะเป็นพวกชั่วร้าย ชอบขโมยข้อมูล หรือ ทำลายให้เสียหาย เป็นต้น

1.8.2 Malware

Malware หรือ Malicious Software คือโปรแกรมชนิดหนึ่งที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อคอมพิวเตอร์ ซึ่งในปัจจุบัน Malware ถูกแบ่งประเภทออกได้มากมายหลากหลายประเภทตามลักษณะพิเศษของแต่ละชนิดเช่น Computer Virus, Worms, Trojan house, Spyware เป็นต้น ซึ่งโปรแกรมเหล่านี้ก็สามารถแสดงผลต่อคอมพิวเตอร์และผู้ใช้งานได้หลากหลายรูปแบบเช่นกัน ไม่ว่าจะเป็น การขโมยข้อมูล, การเข้ารหัสข้อมูลทำให้ไม่สามารถเข้าถึงข้อมูลได้, การลบข้อมูล, การขโมยหน้า Browser ,การทำลายระบบและอีกมากมายที่แฮคเกอร์สามารถคิดวิธีที่จะหาผลประโยชน์จากองค์กรของท่านได้ซึ่งในบทความนี้เราจะพาท่านมาดูกันว่าประเภทต่างๆ

1.8.3 DDoS

การโจมตีแบบ DDoS (Distribute Denial of Service) คือลักษณะหรือวิธีการหนึ่งของการโจมตีระบบบนอินเทอร์เน็ต เพื่อทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Denial-of-Service) การโจมตีจะเกิดขึ้นพร้อมๆกันและมีเป้าหมายเดียวกัน โดยเครื่องที่ตกเป็นเหยื่อทั้งหมด จะสร้างข้อมูลขยะขึ้นมาแล้วส่งไปที่ระบบเป้าหมายกระแสข้อมูลที่ไหลเข้ามาในปริมาณมหาศาลทำให้ระบบเป้าหมายต้องทำงานหนักขึ้นและช้าลงเรื่อยๆ เมื่อเกินกว่าระดับที่รับได้ก็จะหยุดการทำงานลงในที่สุดอันเป็นเหตุให้ผู้ใช้ไม่สามารถใช้บริการระบบเป้าหมายได้ตามปกติ

1.8.4 Social Engineering

เป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อในที่นี้ก็มักจะเป็นผู้ที่มิสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือ

บัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตาม ซึ่งหลงเชื่อการหลอกลวงนั้น

1.8.5 CSRF (Cross-site Request Forgery)

การโจมตีแบบ CSRF จะใช้ “ตัวตน (Identity)” และ “สิทธิ์ (Privilege)” ของเหยื่อที่มีบนเว็บไซต์ ในการปลอมตัวเป็นเหยื่อและกระทำการหรือธุรกรรมไม่พึงประสงค์ แฮกเกอร์จะพยายามใช้ประโยชน์จากเหยื่อที่มี Login Cookies เก็บไว้ในเว็บเบราเซอร์ ส่งผลให้เว็บไซต์ E-commerce ที่ส่ง Cookie ไปเก็บข้อมูลการพิสูจน์ตัวตนของผู้ใช้มักตกเป็นเป้าหมายของการโจมตีนี้

1.8.6 SQL Injection

SQL Injection เป็นเทคนิคที่ใช้ประโยชน์จากส่งคำสั่ง SQL ผ่านทางเว็บแอพพลิเคชันเพื่อไปโจมตีระบบฐานข้อมูลหลังบ้าน โดยอาศัยช่องโหว่ของการใส่ข้อมูล input ของผู้ใช้ที่สามารถตรวจสอบรูปแบบการโจมตีได้อย่างจำกัด แฮกเกอร์รู้ดีว่านักเขียนโปรแกรมจะนำข้อมูลที่ผู้ใช้ input ลงไป ไปใช้เป็นส่วนหนึ่งของคำสั่ง SQL เพื่อส่งไปยังระบบฐานข้อมูล จึงได้แอบฝังคำสั่ง SQL บางอย่างลงไปใน input เหล่านั้นด้วย ส่งผลให้แฮกเกอร์สามารถดึงข้อมูลหรือเปลี่ยนแปลงแก้ไขข้อมูลในระบบฐานข้อมูลตามคำสั่ง SQL ที่แอบฝังลงไปได้

1.8.7 Cross-site Scripting (XSS)

XSS เกิดจากการที่เว็บแอปพลิเคชันมีช่องโหว่ที่ปล่อยให้ผู้ไม่หวังดีสามารถใส่ JavaScript ให้ ทำงานภายใต้ domain เนื่องจาก JavaScript มีความสามารถในการเข้าถึง HTML DOM (Document Object Model) ทำให้ผู้ไม่หวังดีสามารถแทรก JavaScript เพื่อโจมตีได้

1.8.8 Phishing

Phishing เป็นหนึ่งในการหลอกลวงทางโลกออนไลน์ที่พบได้บ่อยที่สุด Phishing มีหลายรูปแบบ การหลอกลวงประเภทนี้มักจะเกี่ยวข้องกับการใช้กลอุบายหลอกล่อผู้ใช้งานและการแอบอ้างเป็นเว็บไซต์ที่น่าเชื่อถือ เช่น เว็บไซต์ธนาคาร หรือบัญชีโซเชียลมีเดีย ซึ่งมักจะแตกต่างจากของจริง มีการเปลี่ยนชื่อในลิงก์เพียงเล็กน้อยทำให้เราไม่สังเกต บ่อยครั้งที่แฮกเกอร์ส่งอีเมลเพื่อขอให้คุณล็อกอินเข้าสู่ระบบธนาคาร หรือหน้าบัญชีอื่น ๆ เพื่อตรวจสอบหรือยืนยันข้อมูลของคุณ พร้อมกับลิงก์ไปยังเพจปลอม อย่างไรก็ตามโปรดทราบว่าเว็บไซต์ทางการของจริงดังกล่าว ไม่ต้องการให้เราทำเช่นนั้น

1.9 บทสรุป

จากบทนำที่ได้กล่าวมาในข้างต้นทั้งหมดนั้น ผู้วิเคราะห์ข้อมูลได้เล็งเห็นความสำคัญของการนำเทคโนโลยีมาประยุกต์ใช้ในการวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 ด้วยกระบวนการในการในการจัดทำเหมืองข้อมูลเพื่อการวิเคราะห์ชุดข้อมูลแบบ (Classification) ในรูปแบบ (Decision Tree) และเผยแพร่ข้อมูลสารสนเทศบน (Web Site) จากข้อมูลที่ได้มาจาก เว็บไซต์ ocslab.hksecurity.net เนื่องจากเทคโนโลยีในปัจจุบันมีการใช้งานที่ง่ายและมีความสะดวกสบาย อีกทั้งผู้ใช้งานยังเข้าถึงข้อมูลได้ง่าย และมีประสิทธิภาพ