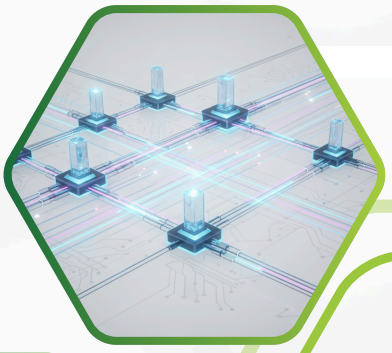
รายงานการวิเคราะห์ รูปแบบการโจมตี ระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยราชภัฏชัยภูมิ ในช่วงปี 2568



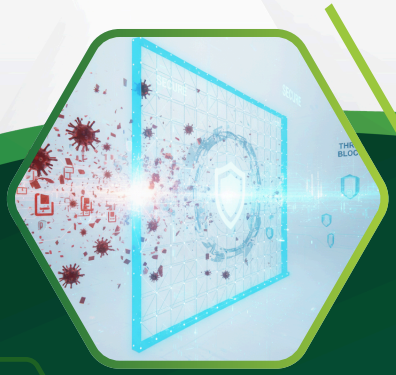
นายภัครพล อาจอาษา

นักวิชาการคอมพิวเตอร์ปฏิบัติการ

งานวิทยบริการและเทคโนโลยีสารสนเทศ
สำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต

มหาวิทยาลัยราชภัฏชัยภูมิ

พ.ศ. 2568



ผ่านการพิจารณากลั่นกรอง และนำไปใช้ประกอบการประชุม
คณะกรรมการประจำสำนักส่งเสริมวิชาการและจัดการเรียนรู้ตลอดชีวิต (สสร)
ในการประชุมครั้งที่ 4/2568 เมื่อวันที่ 3 กันยายน 2568

คำนำ

ในยุคดิจิทัลปัจจุบัน เทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินงานของสถาบันการศึกษา โดยเฉพาะอย่างยิ่งในระบบเครือข่ายคอมพิวเตอร์ที่เป็นกระดูกสันหลังของการให้บริการด้านเทคโนโลยีสารสนเทศแก่นักศึกษา อาจารย์ และบุคลากรของมหาวิทยาลัย อย่างไรก็ตาม ความก้าวหน้าทางเทคโนโลยีดังกล่าวก็นำมาซึ่งความท้าทายใหม่ในด้านความปลอดภัยไว้เบอร์ โดยเฉพาะการคุกคามจากการโจมตีระบบเครือข่ายคอมพิวเตอร์ที่มีความซับซ้อนและหลากหลายมากขึ้น มหาวิทยาลัยราชภัฏชัยภูมิ ในฐานะสถาบันการศึกษาที่มีการใช้งานระบบเทคโนโลยีสารสนเทศอย่างแพร่หลาย ไม่ว่าจะเป็นระบบการเรียนการสอนออนไลน์ ระบบบริหารจัดการข้อมูลนักศึกษา ระบบห้องสมุดดิจิทัล และระบบสารสนเทศอื่นๆ จำเป็นต้องมีการป้องกันและเตรียมความพร้อมรับมือกับภัยคุกคามทางไว้เบอร์ที่อาจเกิดขึ้น การวิเคราะห์รูปแบบการโจมตีระบบเครือข่ายคอมพิวเตอร์จึงเป็นสิ่งจำเป็นอย่างยิ่งเพื่อให้สามารถเข้าใจลักษณะและแนวโน้มของภัยคุกคามที่เกิดขึ้น

รายงานการวิเคราะห์รูปแบบการโจมตีระบบเครือข่ายคอมพิวเตอร์มหาวิทยาลัยราชภัฏชัยภูมิในช่วงปี 2568 ฉบับนี้ จัดทำขึ้นเพื่อศึกษาและวิเคราะห์ข้อมูลเหตุการณ์การโจมตีที่เกิดขึ้นจริง โดยมุ่งเน้นการระบุประเภทของการโจมตี แหล่งที่มาของการโจมตี ช่วงเวลาที่เกิดเหตุการณ์ และผลกระทบที่เกิดขึ้น นอกจากนี้ยังได้วิเคราะห์จุดอ่อนของระบบรักษาความปลอดภัยปัจจุบันและเสนอแนะแนวทางการป้องกันที่เหมาะสม ผู้จัดทำหวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นประโยชน์ต่อผู้บริหารมหาวิทยาลัย ฝ่ายเทคโนโลยีสารสนเทศ และบุคลากรที่เกี่ยวข้อง ในการกำหนดนโยบายและมาตรการรักษาความปลอดภัยทางไว้เบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น เพื่อสร้างความมั่นใจให้แก่ชุมชนมหาวิทยาลัยในการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัยและเชื่อถือได้

ภัครพล อาจอาษา
นักวิชาการคอมพิวเตอร์ ปฏิบัติการ

สารบัญ

บทที่ 1
บทนำ

1.1 ที่มาความสำคัญและเหตุผลในการวิเคราะห์

ในยุคการเปลี่ยนแปลงทางดิจิทัลของศตวรรษที่ 21 เทคโนโลยีสารสนเทศได้กลายเป็นโครงสร้างพื้นฐานที่สำคัญยิ่งต่อการดำเนินงานของสถาบันการศึกษาทุกระดับ โดยเฉพาะอย่างยิ่งในปี พ.ศ. 2568 ที่การจัดการศึกษาได้ผสานเข้ากับเทคโนโลยีดิจิทัลอย่างลึกซึ้ง มหาวิทยาลัยราชภัฏชัยภูมิ ซึ่งเป็นสถาบันการศึกษาภาครัฐที่มีบทบาทสำคัญในการพัฒนาท้องถิ่นและเป็นศูนย์กลางการเรียนรู้ของจังหวัดชัยภูมิและพื้นที่ใกล้เคียง ได้มีการพัฒนาระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่อง ครอบคลุมทั้งระบบการจัดการเรียนการสอนออนไลน์ (Learning Management System) ระบบสารสนเทศเพื่อการบริหารจัดการ (Management Information System) ระบบห้องสมุดดิจิทัล และระบบบริการนักศึกษาออนไลน์ต่าง ๆ การพัฒนาเหล่านี้แม้จะนำมาซึ่งความสะดวกและประสิทธิภาพ แต่ก็นำมาซึ่งความท้าทายด้านความปลอดภัยทางไซเบอร์ที่เพิ่มสูงขึ้นอย่างมีนัยสำคัญ

จากรายงานสถานการณ์ภัยคุกคามทางไซเบอร์ระดับโลกในปี 2568 พบว่าภาคการศึกษากลายเป็นแหล่งที่ถูกโจมตีมากที่สุด โดยสถาบันการศึกษาทั่วโลกประสบการโจมตีทางไซเบอร์เฉลี่ย 4,388 ครั้งต่อสัปดาห์ต่อองค์กร ซึ่งสูงกว่าค่าเฉลี่ยระดับโลกถึง 2 เท่า (Check Point Research, 2025) นอกจากนี้ยังพบว่าการโจมตีด้วย Ransomware ในภาคการศึกษาเพิ่มขึ้น 23% ในช่วงครึ่งแรกของปี 2568 และพบว่าภาคการศึกษาเป็นแหล่งที่ถูกกลุ่มผู้โจมตีจากประเทศมหาอำนาจกำหนดเป้าหมายเป็นลำดับที่สอง โดยกลุ่มผู้โจมตีจากประเทศจีนคิดเป็น 22% ของการโจมตีทั้งหมด โดยเฉพาะอย่างยิ่งมุ่งเป้าไปที่มหาวิทยาลัยที่มีงานวิจัยขั้นสูง (Bitsight, 2025) สำหรับบริบทของประเทศไทย สถานการณ์ภัยคุกคามทางไซเบอร์มีความรุนแรงยิ่งกว่าค่าเฉลี่ยระดับโลก จากข้อมูลของ Check Point Software Thailand พบว่าองค์กรในประเทศไทยประสบการโจมตีทางไซเบอร์เฉลี่ย 3,180 ครั้งต่อสัปดาห์ในช่วงเดือนสิงหาคม 2567 ถึงมกราคม 2568 ซึ่งสูงกว่าค่าเฉลี่ยโลกที่ 1,843 ครั้งถึง 72% โดยภาคการศึกษาเป็นหนึ่งในภาคส่วนที่ถูกโจมตีมากที่สุด คิดเป็น 26% ของการโจมตีทั้งหมด รองจากภาครัฐที่ 20% และภาคการเงินที่ 17% นอกจากนี้ยังพบว่าการโจมตีผ่านอุปกรณ์ Internet of Things (IoT) ในภาคการศึกษาเพิ่มขึ้นอย่างมาก และการโจมตีด้วย Banking Malware ในประเทศไทยมีอัตราการติดเชื้อสูงถึง 9.5% เมื่อเทียบกับค่าเฉลี่ยโลกที่ 2.8% (Check Point Software Thailand & Kaspersky, 2025)

ในส่วนของหน่วยงานภาครัฐไทย สำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) รายงานว่ามีเหตุการณ์ภัยคุกคามทางไซเบอร์มากกว่า 1,002 เหตุการณ์ในช่วง 5 เดือนแรกของปี 2568 ซึ่งสะท้อนให้เห็นถึงความรุนแรงของสถานการณ์ที่เพิ่มขึ้นอย่างต่อเนื่อง (สำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2568) โดยมูลค่าความเสียหายจากอาชญากรรมทางไซเบอร์ในระดับโลกคาดว่าจะเกิน 7 ล้านล้านดอลลาร์สหรัฐในปีนี้ และมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง การที่สถาบันการศึกษากลายเป็นเป้าหมายหลักของผู้โจมตีทางไซเบอร์มิใช่เรื่องบังเอิญ แต่มีปัจจัยหลายประการที่ทำให้สถาบันการศึกษามีความเปราะบางต่อการโจมตี ประการแรก สถาบันการศึกษาเก็บรักษาข้อมูลส่วนบุคคลที่มีมูลค่าสูงจำนวนมหาศาล ทั้งข้อมูลนักศึกษา บุคลากร ข้อมูลทางการเงิน และข้อมูลงานวิจัยที่เป็นทรัพย์สินทางปัญญา ซึ่งเป็นเป้าหมายที่น่าสนใจสำหรับการโจมตีทั้งในรูปแบบของการขโมยข้อมูลเพื่อแอบอ้างตัวตน (Identity theft) การฉ้อโกงทางการเงิน (Financial fraud) และการจารกรรมทางไซเบอร์ (Cyber espionage) ประการที่สอง

สถาบันการศึกษามักมีทรัพยากรด้านความปลอดภัยทางไซเบอร์ที่จำกัดเมื่อเทียบกับองค์กรธุรกิจขนาดใหญ่ ทำให้มีช่องโหว่ที่ผู้โจมตีสามารถใช้ประโยชน์ได้ง่าย ประการที่สาม ระบบเครือข่ายของมหาวิทยาลัยมักมีโครงสร้างที่ซับซ้อน มีผู้ใช้งานจำนวนมาก และมีการเชื่อมต่อกับอุปกรณ์ที่หลากหลาย ทำให้มีพื้นที่เสี่ยงต่อการโจมตี (Attack Surface) ที่กว้างขวาง รูปแบบการโจมตีที่สำคัญที่ส่งผลกระทบต่อสถาบันการศึกษาในปี 2568 ประกอบด้วย (1) การโจมตีด้วย Ransomware ซึ่งมีการใช้ปัญญาประดิษฐ์ เพื่อเพิ่มประสิทธิภาพการโจมตีและหลบเลี่ยงระบบป้องกัน (2) การโจมตีแบบ Phishing และ QR Code Phishing ที่สามารถหลบเลี่ยงระบบกรองอีเมลแบบดั้งเดิมได้ (3) การโจมตีผ่านห่วงโซ่อุปทาน (Supply Chain) โดยเจาะระบบผ่านผู้ให้บริการบุคคลที่สามที่มีความปลอดภัยต่ำกว่า (4) การโจมตีด้วยมัลแวร์ทางการเงิน (Banking Malware) ซึ่งในประเทศไทยมีอัตราการโจมตีสูงกว่าค่าเฉลี่ยโลกอย่างมีนัยสำคัญ และ (5) การโจมตีจากกลุ่มนักกิจกรรมทางไซเบอร์ (Hacktivist) ที่มุ่งเป้าตามประเด็นทางการเมืองระหว่างประเทศ ผลกระทบจากการโจมตีทางไซเบอร์ต่อสถาบันการศึกษามีความรุนแรงและกว้างขวาง ทั้งในแง่ของความเสียหายทางการเงิน การหยุดชะงักของการให้บริการทางการศึกษา การสูญเสียความน่าเชื่อถือ และการละเมิดข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อนักศึกษาและบุคลากรในระยะยาว ตัวอย่างเช่น การโจมตีมหาวิทยาลัยชั้นนำในสหรัฐอเมริกาหลายแห่งในปี 2566-2568 ส่งผลให้ระบบหยุดให้บริการนานหลายวัน และมีข้อมูลจำนวนมากถูกเปิดเผยหรือถูกเรียกค่าไถ่ นอกจากนี้ ต้นทุนในการแก้ไขปัญหาและฟื้นฟูระบบหลังจากถูกโจมตีมีค่าสูงมาก โดยในสหรัฐอเมริกาพบว่าต้นทุนเฉลี่ยของการละเมิดข้อมูลอยู่ที่มากกว่า 10 ล้านดอลลาร์สหรัฐต่อครั้ง

ด้วยบริบทและสถานการณ์ดังกล่าว การวิเคราะห์รูปแบบการโจมตีระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏชัยภูมิจึงมีความสำคัญอย่างยิ่ง เพื่อทำความเข้าใจลักษณะและรูปแบบของภัยคุกคามที่อาจเกิดขึ้น ประเมินความเสี่ยงและช่องโหว่ของระบบ และจัดทำมาตรการป้องกันที่เหมาะสมและมีประสิทธิภาพ การศึกษานี้จะเป็นฐานข้อมูลสำคัญสำหรับการพัฒนานโยบายและกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ของมหาวิทยาลัย ตลอดจนเป็นแนวทางสำหรับสถาบันการศึกษาอื่น ๆ ในการเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องในอนาคต การศึกษาวิจัยนี้ยังสอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย และตอบสนองต่อความจำเป็นเร่งด่วนในการสร้างความตระหนักรู้และพัฒนาขีดความสามารถด้านความปลอดภัยทางไซเบอร์ในภาคการศึกษาของประเทศ

ความสำคัญของปัญหา

1. ความสำคัญต่อการปกป้องข้อมูลส่วนบุคคลและทรัพย์สินทางปัญญา มหาวิทยาลัยราชภัฏชัยภูมิเก็บรักษาข้อมูลส่วนบุคคลของนักศึกษา บุคลากร และผู้มีส่วนได้ส่วนเสียจำนวนมาก รวมถึงข้อมูลงานวิจัยและทรัพย์สินทางปัญญาที่มีคุณค่า การถูกโจมตีทางไซเบอร์อาจส่งผลให้ข้อมูลเหล่านี้ถูกโจรกรรม เปิดเผย หรือทำลาย ซึ่งจะก่อให้เกิดความเสียหายทั้งต่อบุคคลและสถาบัน ตลอดจนอาจมีความรับผิดทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ด้านความต่อเนื่องของการให้บริการ ความสำคัญต่อความต่อเนื่องของการให้บริการทางการศึกษา การโจมตีทางไซเบอร์ โดยเฉพาะ Ransomware และ DDoS สามารถทำให้ระบบเครือข่ายและบริการดิจิทัลของมหาวิทยาลัยหยุดชะงัก ส่งผลกระทบโดยตรงต่อการเรียนการสอน การฝึกอบรม ประชุมสัมมนา การจัดการข้อมูลนักศึกษา และการบริหารจัดการ ดังเช่นกรณีของมหาวิทยาลัยต่างประเทศที่ประสบปัญหาระบบล่มนานหลายสัปดาห์ ทำให้การเรียนการสอนต้องหยุดชะงัก การมีความเข้าใจเกี่ยวกับรูปแบบการโจมตีจะช่วยให้มหาวิทยาลัยสามารถวางแผนรับมือและฟื้นฟูระบบได้รวดเร็ว รักษาความต่อเนื่องของการให้บริการทางการศึกษา

3. ความสำคัญต่อความน่าเชื่อถือและชื่อเสียงของสถาบัน การถูกโจมตีทางไซเบอร์และเกิดการรั่วไหลของข้อมูลส่วนบุคคลจะส่งผลกระทบอย่างรุนแรงต่อความน่าเชื่อถือและชื่อเสียงของมหาวิทยาลัย อาจทำให้นักศึกษาและผู้ปกครองสูญเสียความเชื่อมั่นในความสามารถของสถาบันในการดูแลข้อมูล ส่งผลต่อการตัดสินใจเลือกเข้าศึกษาของนักศึกษาในอนาคต รวมทั้งความร่วมมือทางวิชาการกับสถาบันอื่น ๆ การมีระบบป้องกันที่มีประสิทธิภาพโดยอาศัยความเข้าใจในรูปแบบการโจมตีจะช่วยสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียทุกฝ่าย

4. ความสำคัญทางด้านการเงินและทรัพยากร ต้นทุนในการแก้ไขปัญหาหลังจากถูกโจมตีทางไซเบอร์มีค่าสูงมาก ทั้งค่าใช้จ่ายในการฟื้นฟูระบบ การจ้างผู้เชี่ยวชาญด้านความปลอดภัย ค่าปรับทางกฎหมายและค่าเสียหายต่างๆ ซึ่งอาจเป็นภาระอย่างหนักต่องบประมาณที่จำกัดของมหาวิทยาลัยภาครัฐ การลงทุนในการวิเคราะห์และป้องกันล่วงหน้าจะช่วยลดความเสี่ยงและประหยัดค่าใช้จ่ายในระยะยาว ซึ่งสอดคล้องกับหลักการบริหารจัดการความเสี่ยงและการใช้ทรัพยากรอย่างมีประสิทธิภาพ

5. ความสำคัญต่อการพัฒนาขีดความสามารถด้านความปลอดภัยทางไซเบอร์ การศึกษาวิจัยครั้งนี้จะสร้างองค์ความรู้และฐานข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ในบริบทของมหาวิทยาลัยราชภัฏ ซึ่งเป็นข้อมูลที่ยังมีจำกัดในประเทศไทย ผลการศึกษาจะเป็นแนวทางในการพัฒนาบุคลากรด้านความปลอดภัยทางไซเบอร์ การออกแบบหลักสูตรการฝึกอบรม และการสร้างความตระหนักรู้แก่ผู้ใช้งานระบบ นอกจากนี้ยังสามารถนำไปประยุกต์ใช้ในการจัดการเรียนการสอนด้านความปลอดภัยสารสนเทศ ซึ่งเป็นทักษะที่จำเป็นในยุคดิจิทัล

6. ความสำคัญต่อการเป็นต้นแบบและการขยายผล มหาวิทยาลัยราชภัฏชัยภูมิเป็นสถาบันการศึกษาที่มีบทบาทสำคัญในการพัฒนาท้องถิ่นภาคตะวันออกเฉียงเหนือตอนล่าง การมีระบบความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพจะทำให้มหาวิทยาลัยสามารถเป็นต้นแบบให้กับสถาบันการศึกษาอื่น ๆ ในพื้นที่และมหาวิทยาลัยราชภัฏทั่วประเทศ ผลการศึกษาสามารถแบ่งปันและขยายผลไปสู่เครือข่ายมหาวิทยาลัยราชภัฏ ช่วยยกระดับความปลอดภัยทางไซเบอร์ของภาคการศึกษาไทยโดยรวม

7. ความสำคัญต่อการสนับสนุนนโยบายระดับชาติ การศึกษานี้สอดคล้องกับนโยบายความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย และแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งมีเป้าหมายในการสร้างความมั่นคงปลอดภัยในโลกไซเบอร์ การมีข้อมูลเชิงประจักษ์จากสถาบันการศึกษาจะช่วยสนับสนุนการกำหนดนโยบายและมาตรการด้านความปลอดภัยทางไซเบอร์ในระดับชาติ โดยเฉพาะในภาคการศึกษาซึ่งเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

ปัจจัยเสี่ยงที่สำคัญ จากการวิเคราะห์สถานการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อมหาวิทยาลัยราชภัฏชัยภูมิ สามารถระบุปัจจัยเสี่ยงที่สำคัญได้ ดังนี้

1. ปัจจัยเสี่ยงด้านโครงสร้างพื้นฐานทางเทคโนโลยี มหาวิทยาลัยมีระบบเครือข่ายที่มีความซับซ้อนและเชื่อมต่อกับอุปกรณ์จำนวนมาก ทั้งคอมพิวเตอร์ อุปกรณ์เคลื่อนที่ ซึ่งแต่ละอุปกรณ์อาจมีช่องโหว่ด้านความปลอดภัย นอกจากนี้ ระบบเดิมบางส่วนอาจล้าสมัยและไม่ได้รับการปรับปรุงอย่างสม่ำเสมอ ทำให้เกิดช่องโหว่ที่ผู้โจมตีสามารถใช้ประโยชน์ได้

2. ปัจจัยเสี่ยงด้านทรัพยากรบุคคลและความตระหนักรู้ บุคลากรและนักศึกษาอาจขาดความรู้และความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ มีพฤติกรรมเสี่ยง เช่น การใช้รหัสผ่านที่ไม่ปลอดภัย การเปิดอีเมลหรือไฟล์แนบที่น่าสงสัย การดาวน์โหลดซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ หรือการใช้งานอุปกรณ์ส่วนตัวในเครือข่ายของมหาวิทยาลัยโดยไม่มีมาตรการป้องกันที่เหมาะสม นอกจากนี้ มหาวิทยาลัยอาจมีบุคลากรด้านความปลอดภัยทางไซเบอร์ที่จำกัด

3. ปัจจัยเสี่ยงด้านนโยบายและการบริหารจัดการ การขาดนโยบายความปลอดภัยทางไซเบอร์ที่ชัดเจนและครอบคลุม หรือการมีนโยบายแต่ไม่มีการบังคับใช้อย่างจริงจัง อาจทำให้เกิดช่องโหว่ด้านความปลอดภัย การขาดแผนรับมือเหตุการณ์ฉุกเฉิน (Incident Response Plan) และแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) อาจส่งผลให้การตอบสนองต่อเหตุการณ์ไม่มีประสิทธิภาพ

4. ปัจจัยเสี่ยงจากความหลากหลายของข้อมูลและระบบ มหาวิทยาลัยเก็บรักษาข้อมูลที่มีมูลค่าสูงและหลากหลาย ทั้งข้อมูลส่วนบุคคลของนักศึกษาและบุคลากร ข้อมูลทางการเงิน ข้อมูลงานวิจัย และข้อมูลทางวิชาการ ความหลากหลายของข้อมูลและระบบสารสนเทศที่ใช้งานทำให้การควบคุมและปกป้องข้อมูลมีความซับซ้อน

ความจำเป็นในการศึกษา ท่ามกลางกระแสการเปลี่ยนแปลงทางดิจิทัลที่รวดเร็ว มหาวิทยาลัยราชภัฏชัยภูมิได้ปรับตัวสู่การเป็น Digital University อย่างเต็มรูปแบบ อย่างไรก็ตาม ความก้าวหน้าดังกล่าวมาพร้อมกับความเสี่ยงที่ซับซ้อน การศึกษารูปแบบการโจมตีระบบเครือข่ายของมหาวิทยาลัยในช่วงเวลานี้จึงไม่ใช่เพียงทางเลือกแต่เป็นความจำเป็นเร่งด่วนโดยมีเหตุผลความสำคัญ 5 ประการ ดังนี้

1. วิเคราะห์และระบุภัยคุกคามที่เฉพาะเจาะจง ต่อสถาบันการศึกษาในบริบทของไทย

ในอดีต การป้องกันภัยทางไซเบอร์มักอ้างอิงข้อมูลสถิติจากต่างประเทศเป็นหลัก แต่ในปี 2568 บริบทของภัยคุกคามในประเทศไทยมีความเฉพาะตัวสูงมาก

เป้าหมายที่แตกต่าง สถาบันการศึกษาในไทย เช่น มหาวิทยาลัยราชภัฏชัยภูมิ ตกเป็นเป้าหมายของการโจมตีเพื่อขโมยข้อมูลส่วนบุคคล (Identity Theft) และการฝังมัลแวร์เพื่อใช้ทรัพยากรของมหาวิทยาลัยในการขุดเหรียญคริปโตหรือส่งสแปม ซึ่งแตกต่างจากภาคธุรกิจที่มักเน้นการเรียกค่าไถ่ข้อมูลทางการเงิน

แหล่งที่มาของการโจมตี จากการวิเคราะห์เบื้องต้นพบว่าการโจมตีไม่ได้มาจากกลุ่มแฮกเกอร์ข้ามชาติเพียงอย่างเดียว แต่ยังพบรูปแบบการโจมตีจากภายในประเทศและประเทศเพื่อนบ้านที่อาศัยช่องโหว่ของระบบเครือข่ายทางการศึกษา

ความสำคัญของการระบุตัวตน การศึกษาครั้งนี้จะช่วยระบุได้ว่า "ใคร" กำลังโจมตีเรา "โจมตีอย่างไร" และ "เป้าหมายคืออะไร" เช่น การพบการโจมตีแบบ Brute Force และ DNS ANY Queries ในสัดส่วนที่สูง

เกินปกติ ข้อมูลเหล่านี้จะช่วยให้สถาบันสามารถสร้าง "โปรไฟล์ภัยคุกคาม" (Threat Profile) ที่แม่นยำสำหรับสถาบันการศึกษาไทยโดยเฉพาะ

2. พัฒนาแนวทางการป้องกันที่เหมาะสม สำหรับสถาบันการศึกษาที่มีข้อจำกัดด้านงบประมาณและบุคลากร

มหาวิทยาลัยราชภัฏในฐานะสถาบันการศึกษาภาครัฐ มักประสบปัญหาการขาดแคลนงบประมาณเมื่อเทียบกับมหาวิทยาลัยขนาดใหญ่หรือภาคเอกชน รวมถึงการจำกัดของบุคลากรสาย IT ที่ต้องดูแลระบบจำนวนมาก

การลงทุนที่คุ้มค่า (Cost-Effectiveness) เมื่อเราทราบรูปแบบการโจมตีที่ชัดเจน มหาวิทยาลัยไม่จำเป็นต้องซื้อซอฟต์แวร์ป้องกันทุกชนิดในตลาด แต่สามารถเลือกลงทุนในเทคโนโลยีที่ "ตรงจุด" เช่น การเน้นไปที่ Next-Generation Firewall ที่มีความสามารถในการจัดการ App-ID เพื่อควบคุมการใช้งานแอปพลิเคชันที่มีความเสี่ยง

การใช้ทรัพยากรที่มีอยู่ให้เกิดประโยชน์สูงสุด การวิเคราะห์ช่วยให้ทีม IT สามารถปรับปรุงเกณฑ์การตั้งค่า (Configuration) ของอุปกรณ์เดิมที่มีอยู่ให้มีประสิทธิภาพสูงขึ้น เช่น การทำ Network Segmentation หรือการคัดกรอง IP จากประเทศที่เป็นกลุ่มเสี่ยงสูง (Geo-blocking)

การลดภาระงานบุคลากร การนำผลการศึกษาไปสร้างระบบตรวจจับอัตโนมัติ (Automated Detection) จะช่วยลดภาระของเจ้าหน้าที่ในการตรวจสอบ Log File มหาศาลด้วยตนเอง ทำให้บุคลากรที่มีจำกัดสามารถโฟกัสไปที่การแก้ไขปัญหาที่สำคัญจริงๆ ได้

3. สร้างความตระหนักรู้ ให้กับนักศึกษา อาจารย์ และบุคลากรเกี่ยวกับความปลอดภัยทางไซเบอร์

ช่องโหว่ที่ใหญ่ที่สุดของระบบความปลอดภัยไม่ใช่ซอฟต์แวร์ แต่คือ "คน" (Human Factor) การศึกษานี้จะนำข้อมูลจริงจากการโจมตีมาเป็นบทเรียนในการสร้างความตระหนักรู้

การเรียนรู้จากสถิติจริง แทนที่จะสอนทฤษฎีทั่วไป มหาวิทยาลัยสามารถนำสถิติการโจมตี เช่น จำนวนครั้งที่นักศึกษาถูกพยายามขโมยรหัสผ่าน หรืออีเมลหลอกลวง (Phishing) ที่ส่งเข้ามาในระบบของมหาวิทยาลัยจริงๆ มาแสดงให้เห็นถึงอันตรายที่อยู่ใกล้ตัว

การปรับเปลี่ยนพฤติกรรม ผลการศึกษาจะถูกนำไปพัฒนาเป็นคู่มือการใช้งานเครือข่ายที่ปลอดภัย (Safe Digital Practices) เช่น การใช้ Multi-Factor Authentication (MFA) และการหลีกเลี่ยงการใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ที่เป็นบ่อเกิดของมัลแวร์

วัฒนธรรมความปลอดภัย เมื่อบุคลากรในองค์กรมีความรู้และตระหนักถึงภัยคุกคาม ทุกคนจะทำหน้าที่เป็น "เซนเซอร์" ช่วยระบุความผิดปกติ ซึ่งถือเป็นการป้องกันด่านหน้าที่มีประสิทธิภาพที่สุด**เป็นแนวทางสำหรับสถาบันการศึกษาอื่นๆ** ในการเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์

4. การเป็นแนวทางสำหรับสถาบันการศึกษาอื่นๆ ในการเตรียมความพร้อมรับมือ

มหาวิทยาลัยราชภัฏชัยภูมิไม่ได้เผชิญปัญหานี้เพียงลำพัง สถาบันการศึกษาขนาดกลางและขนาดเล็กทั่วประเทศต่างเผชิญกับความท้าทายในลักษณะเดียวกัน การแบ่งปันองค์ความรู้ (Knowledge Sharing) ผลสรุปจากการศึกษาครั้งนี้ ทั้งในแง่ของสถิติภัยคุกคามและแนวทางการตั้งค่าระบบป้องกัน สามารถนำไปเป็น "Case Study" หรือ "Best Practice" ให้กับมหาวิทยาลัยในเครือข่ายราชภัฏและสถานศึกษาอื่นๆ การสร้างมาตรฐานการป้องกัน: ข้อมูลที่ได้จะเป็นต้นแบบในการออกแบบสถาปัตยกรรมเครือข่ายที่ปลอดภัยสำหรับสถานศึกษา (Campus Network Security Architecture) ที่เหมาะสมกับงบประมาณและบริบทของไทย ความร่วมมือระหว่างสถาบัน: การศึกษาครั้งนี้จะเป็นจุดเริ่มต้นของการสร้างเครือข่ายความร่วมมือในการ

แลกเปลี่ยนข้อมูลภัยคุกคาม (Threat Intelligence Sharing) ระหว่างสถาบันการศึกษา เพื่อสร้างเกราะป้องกันในระดับระดับภูมิภาค

5. การสนับสนุนนโยบายระดับชาติด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาคการศึกษา

การศึกษาครั้งนี้มีความสอดคล้องอย่างยิ่งกับทิศทางนโยบายของประเทศ และข้อบังคับทางกฎหมายที่สำคัญ การปฏิบัติตามกฎหมาย PDPA มหาวิทยาลัยมีหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ในการมีมาตรการรักษาความปลอดภัยที่เหมาะสม การศึกษารูปแบบการโจมตีจะช่วยยืนยันว่ามหาวิทยาลัยได้ใช้ความพยายามอย่างเต็มที่ในการปกป้องข้อมูลของนักศึกษาและบุคลากร การตอบสนองต่อยุทธศาสตร์ความมั่นคงไซเบอร์ สอดคล้องกับแผนแม่บทภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่มุ่งเน้นการยกระดับความปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งรวมถึงภาคการศึกษา การขับเคลื่อนเศรษฐกิจดิจิทัล ความมั่นคงปลอดภัยทางไซเบอร์เป็นฐานรากสำคัญของการพัฒนาเศรษฐกิจดิจิทัล (Digital Economy) หากสถาบันการศึกษาซึ่งเป็นแหล่งผลิตบุคลากรไม่สามารถสร้างระบบที่ปลอดภัยได้ ย่อมส่งผลกระทบต่อความเชื่อมั่นในการขับเคลื่อนประเทศด้วยนวัตกรรมในระยะยาว

1.2 วัตถุประสงค์

1. เพื่อวิเคราะห์รูปแบบการโจมตีระบบเครือข่ายที่เกิดขึ้นกับมหาวิทยาลัยราชภัฏชัยภูมิ
2. เพื่อระบุแหล่งที่มาและเป้าหมายของการโจมตี
3. เพื่อประเมินประสิทธิภาพของระบบป้องกันปัจจุบัน
4. เพื่อนำเสนอแนวทางปรับปรุงมาตรการความปลอดภัยทางไซเบอร์

1.3 ขอบเขตการศึกษา

การวิเคราะห์ครอบคลุมข้อมูลจาก Palo Alto Next Generation Firewall เดือนมกราคม ถึง สิงหาคม พ.ศ. 2568 โดยมุ่งเน้น

1) รูปแบบการโจมตีและภัยคุกคาม
2) แหล่งที่มาของการโจมตี
3) เป้าหมายการโจมตี
4) ประเภทแอปพลิเคชันและบริการที่ถูกโจมตี

การกำหนดขอบเขตที่ชัดเจนโดยอิงจากข้อมูลจริงของ Palo Alto NGFW ตลอด 8 เดือนของปี 2568 จะทำให้มหาวิทยาลัยราชภัฏชัยภูมิสามารถ มองเห็นภาพรวมภัยคุกคาม (Visibility): เข้าใจอย่างถ่องแท้ว่าระบบเครือข่ายของสถาบันกำลังเผชิญกับอะไรในระดับ Application-layer ปรับจูนนโยบาย (Policy Fine-tuning): สามารถเขียนกฎ Firewall (Security Rules) ที่มีความละเอียดสูง (Granular Control) ไม่ใช่เพียงแค่การปิด-เปิดพอร์ต แต่เป็นการควบคุมตามประเภทแอปพลิเคชันและพฤติกรรมผู้ใช้ วางแผนรับมือล่วงหน้า (Proactive Defense): ข้อมูลแหล่งที่มาและเป้าหมายจะช่วยให้ฝ่าย IT สามารถเตรียมระบบสำรองและมาตรการตอบโต้ได้อย่างทันท่วงที ก่อนที่การโจมตีจะสร้างความเสียหายในวงกว้าง

1.4 ประโยชน์ของการวิเคราะห์ต่อการพัฒนางานในหน้าที่

การวิเคราะห์รูปแบบการโจมตีระบบเครือข่ายคอมพิวเตอร์ผ่านอุปกรณ์ Palo Alto Next Generation Firewall ไม่เพียงแต่เป็นการเฝ้าระวังภัยคุกคามตามภารกิจปกติ แต่ยังเป็นกลไกสำคัญในการยกระดับมาตรฐานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของสถาบัน ผลการวิเคราะห์ในเชิงวิชาการสามารถนำมาประยุกต์ใช้เพื่อพัฒนางานในหน้าที่ได้ดังนี้

1) การเพิ่มประสิทธิภาพในการบริหารจัดการนโยบายความปลอดภัย (Policy Optimization) การวิเคราะห์ข้อมูล Log ในระดับ Application-layer ช่วยให้ผู้ปฏิบัติงานสามารถเปลี่ยนจากการตั้งค่า Firewall แบบดั้งเดิม (Port-based) ไปสู่การกำหนดนโยบายแบบ Identity-Based และ App-ID ที่มีความแม่นยำสูงขึ้น ส่งผลให้การบริหารจัดการทรัพยากรเครือข่ายมีประสิทธิภาพ ลดช่องว่างของความผิดพลาดในการอนุญาตแอปพลิเคชันที่มีความเสี่ยง และช่วยให้การไหลเวียนของข้อมูลทางวิชาการมีความราบรื่นแต่ยังคงความปลอดภัยสูงสุด

2) การเปลี่ยนรูปแบบการทำงานจากเชิงรับเป็นเชิงรุก (From Reactive to Proactive Defense) ประโยชน์ที่สำคัญคือการนำข้อมูลทางสถิติของภัยคุกคาม เช่น รูปแบบการโจมตีแบบ Brute Force หรือ DNS ANY Queries มาสร้างเป็นฐานข้อมูล Threat Intelligence เฉพาะขององค์กร ช่วยให้ผู้รับผิดชอบสามารถพยากรณ์แนวโน้มการโจมตีและวางมาตรการป้องกันล่วงหน้า (Pre-emptive Measures) ได้ทันท่วงที ก่อนที่ภัยคุกคามจะส่งผลกระทบต่อระบบบริการการศึกษาหลักของมหาวิทยาลัย

3) การยกระดับการจัดการเหตุการณ์ผิดปกติและการสืบสวนทางดิจิทัล (Incident Response and Forensics) การศึกษาขอบเขตแหล่งที่มาและเป้าหมายการโจมตี ช่วยพัฒนากระบวนการ Standard Operating Procedures (SOPs) ในการตอบโต้เหตุการณ์ภัยคุกคาม (Incident Response) ข้อมูลที่ผ่านการวิเคราะห์เชิงลึกจะกลายเป็นหลักฐานสำคัญในการสืบสวนหาต้นตอของปัญหา (Root Cause Analysis) ช่วยลดระยะเวลาในการกู้คืนระบบ (Mean Time to Recover - MTTR) และเพิ่มขีดความสามารถในการทำนิติวิทยาศาสตร์ทางคอมพิวเตอร์หากเกิดกรณีละเมิดความมั่นคงปลอดภัย

4) การสนับสนุนการตัดสินใจเชิงกลยุทธ์ตามหลักธรรมาภิบาลข้อมูล (Data-Driven Decision Making) ผลการวิเคราะห์ทำหน้าที่เป็น "ตัวชี้วัดประสิทธิภาพ" (KPIs) ที่เป็นรูปธรรมสำหรับผู้บริหารในการวางแผนงบประมาณด้านไอที ประโยชน์ในหน้าที่นี้คือการช่วยให้ผู้ปฏิบัติงานสามารถนำเสนอเหตุผลความจำเป็นในการอัปเกรดระบบ หรือการจัดหาเทคโนโลยีความปลอดภัยใหม่ๆ โดยอิงจากข้อมูลความเสี่ยงจริง (Risk-based Approach) มากกว่าการใช้ความรู้สึก ทำให้การลงทุนด้านเทคโนโลยีสารสนเทศของสถาบันเป็นไปอย่างคุ้มค่าและตรงจุด

5) การส่งเสริมมาตรฐานความสอดคล้องทางกฎหมายและระเบียบปฏิบัติ (Compliance and Standardization) การพัฒนางานในหน้าที่ผ่านการวิเคราะห์นี้ ช่วยยืนยันว่าสถาบันมีการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างครบถ้วน ข้อมูลการวิเคราะห์เป้าหมายและแอปพลิเคชันที่ถูกโจมตีจะถูกนำไปใช้ปรับปรุงมาตรการควบคุมขั้นต่ำ (Minimum Security Controls) ให้สอดคล้องกับมาตรฐานสากล เช่น ISO/IEC 27001 หรือ NIST Cybersecurity Framework

6) การสร้างฐานความรู้เพื่อการถ่ายทอดเทคโนโลยี (Knowledge Management) ผลจากการวิเคราะห์จะถูกจัดทำเป็นองค์ความรู้ (Knowledge Base) สำหรับการฝึกอบรมบุคลากรภายในและนักศึกษา ช่วยในการพัฒนางานด้านการบริการวิชาการ โดยการสร้างคู่มือแนวปฏิบัติที่เป็นเลิศ (Best Practices) ในการป้องกันตนเองจากภัยไซเบอร์ ซึ่งเป็นการบูรณาการงานด้านเทคนิคเข้ากับการพัฒนาทรัพยากรมนุษย์ของมหาวิทยาลัยอย่างยั่งยืน

1.5 นิยามศัพท์เฉพาะ / คำจำกัดความ

เพื่อให้เกิดความเข้าใจที่ตรงกันในการสื่อสารและวิเคราะห์ข้อมูลในรายงานฉบับนี้ จึงได้กำหนดนิยามศัพท์เฉพาะที่เกี่ยวข้องกับเทคโนโลยีเครือข่ายและความมั่นคงปลอดภัยไซเบอร์ไว้ดังนี้

1. ระบบเครือข่ายคอมพิวเตอร์มหาวิทยาลัยราชภัฏชัยภูมิ (CPRU Network) หมายถึง โครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศที่เชื่อมต่อคอมพิวเตอร์ อุปกรณ์แม่ข่าย (Server) และอุปกรณ์พกพาต่างๆ ภายในมหาวิทยาลัยเข้าด้วยกัน เพื่อใช้ในการบริหารจัดการ การเรียนการสอน และการสืบค้นข้อมูล โดยมีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตภายนอกผ่านเกตเวย์ส่วนกลาง

2. พาโลอัลโตเน็กซ์เจนเนอเรชันไฟร์วอลล์ (Palo Alto Next-Generation Firewall: NGFW) หมายถึง อุปกรณ์รักษาความปลอดภัยระบบเครือข่ายอัจฉริยะที่ทำหน้าที่ตรวจสอบและคัดกรองข้อมูลในระดับชั้นแอปพลิเคชัน (Layer 7) ซึ่งมีความสามารถสูงกว่าไฟร์วอลล์ทั่วไป โดยสามารถระบุตัวตนแอปพลิเคชัน (App-ID) และระบุตัวตนผู้ใช้งาน (User-ID) เพื่อป้องกันภัยคุกคามสมัยใหม่ได้อย่างแม่นยำ

3. รูปแบบการโจมตี (Attack Patterns) หมายถึง วิธีการ ขั้นตอน หรือพฤติกรรมที่ผู้ไม่ประสงค์ดีหรือโปรแกรมอัตโนมัติใช้ในการพยายามเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต เพื่อสร้างความเสียหาย ขโมยข้อมูล หรือทำให้ระบบหยุดชะงัก เช่น การโจมตีแบบ Brute Force หรือ DNS ANY Queries

4. ภัยคุกคามทางไซเบอร์ (Cyber Threats) หมายถึง สภาวการณ์หรือการกระทำใดๆ ที่มีเจตนาประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูล หรือเครือข่าย ซึ่งอาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) หรือความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ

5) การโจมตีแบบสุ่มรหัสผ่าน (Brute Force Attack) หมายถึง วิธีการเจาะเข้าสู่ระบบโดยการสุ่มรหัสผ่านหลายๆ รูปแบบซ้ำๆ อย่างต่อเนื่องด้วยโปรแกรมอัตโนมัติ จนกว่าจะพบรหัสผ่านที่ถูกต้อง เพื่อเข้ายึดครองบัญชีผู้ใช้งานหรือสิทธิ์การบริหารจัดการระบบ

6. การโจมตีผ่านระบบชื่อโดเมน (DNS ANY Queries Attack) หมายถึง รูปแบบการโจมตีโดยการส่งคำขอข้อมูลประเภท "ANY" ไปยังเซิร์ฟเวอร์ระบบชื่อโดเมน (DNS) เพื่อบังคับให้ระบบตอบกลับด้วยข้อมูลขนาดใหญ่เกินจำเป็น มักใช้เป็นส่วนหนึ่งของการโจมตีแบบ Denial of Service (DoS) เพื่อทำให้ช่องสัญญาณเครือข่ายเต็มจนใช้งานไม่ได้

7. ข้อมูลระบุตัวตนผู้ใช้งาน (User-ID) หมายถึง คุณสมบัติที่ช่วยให้ผู้ดูแลระบบสามารถระบุได้ว่าพฤติกรรมหรือภัยคุกคามที่เกิดขึ้นในเครือข่ายนั้นมาจากผู้ใช้งานรายใด (เช่น นักศึกษา หรือบุคลากร) โดยเชื่อมโยงข้อมูลจากระบบลงทะเบียนของมหาวิทยาลัย แทนการระบุเพียงแค่หมายเลขไอพี (IP Address)

8. ล็อกไฟล์ (Log Files) หมายถึง บันทึกเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายและไฟร์วอลล์ ซึ่งรวมถึงข้อมูลวันเวลา ไอพีต้นทาง-ปลายทาง ประเภทภัยคุกคาม และผลการจัดการ (เช่น บล็อก หรือ อนุญาต) เพื่อใช้เป็นหลักฐานในการวิเคราะห์และสืบสวนทางดิจิทัล

9. ช่องโหว่ของระบบ (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่องในซอฟต์แวร์ ฮาร์ดแวร์ หรือกระบวนการบริหารจัดการเครือข่าย ซึ่งผู้โจมตีสามารถใช้เป็นช่องทางในการบุกรุกเข้าสู่ระบบได้

บทที่ 2
แนวคิดทฤษฎีและงานวิเคราะห์ที่เกี่ยวข้อง

2.1 แนวคิดเรื่อง Next Generation Firewall

Next Generation Firewall (NGFW) เป็นเทคโนโลยีการป้องกันความปลอดภัยที่มีความสามารถขั้นสูง มีคุณสมบัติหลัก ดังนี้

Application Awareness สามารถระบุและควบคุมแอปพลิเคชันได้

User-based Security ระบุผู้ใช้และควบคุมการเข้าถึงตามกลุ่มผู้ใช้

Integrated Intrusion Prevention: ระบบป้องกันการบุกรุกแบบบูรณาการ

Threat Intelligence ข้อมูลภัยคุกคามแบบเรียลไทม์

Palo Alto Solution: Next Generation Firewall

การใช้งาน firewall ในระบบเครือข่าย จะช่วยให้สามารถควบคุมการเข้าถึงระหว่างแต่ละส่วนของเครือข่าย เป็นการเพิ่มระดับในการรักษาความปลอดภัยให้กับระบบเครือข่าย ถ้าเป็นในอดีต การใช้งาน firewall จะมีความสามารถในการทำงานระดับ Layer 4 คือจะใช้หมายเลขพอร์ตของโปรโตคอล TCP หรือ UDP ในการระบุถึงแอปพลิเคชั่น อย่างเช่น TCP 80 หมายถึง HTTP หรือ UDP 53 หมายถึง DNS เป็นต้น แต่ในปัจจุบัน จะเป็นยุคของ Next-Generation Firewall (ยังสงสัยอยู่ว่า ถ้าเรียก firewall ยุคนี้ว่า Next-Generation Firewall แล้วในยุคหน้าจะเรียกว่าอะไร) ซึ่งจะมีความสามารถในการระบุได้ถึงแอปพลิเคชั่นที่เป็น content ในระดับ Layer 7 ได้ โดย Next-Generation Firewall ที่จะมาแนะนำให้ได้รู้จักกันในวันนี้ คือ **Palo Alto Networks Next-Generation Firewall**ที่เป็น Firewall ในระดับผู้นำในกลุ่มของ Enterprise Network Firewall (อ้างอิงจาก Gartner 2014 : Magic Quadrant for Enterprise Network Firewalls)

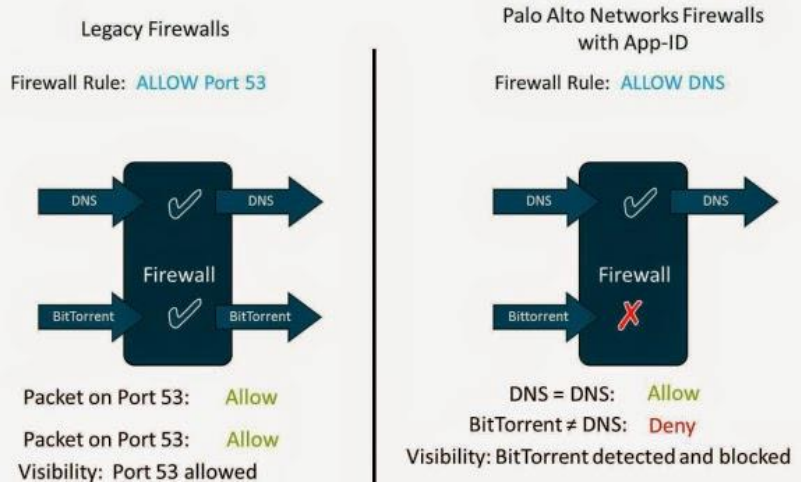
สถาปัตยกรรมความปลอดภัยของ Palo Alto Networks ตั้งอยู่บนหลักการเชิงบูรณาการแบบ Platformization ที่ขับเคลื่อนด้วยเทคโนโลยี Single-Pass Parallel Processing (SP3) ซึ่งเป็นกระบวนการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์แบบขนานเพื่อระบุอัตลักษณ์ของแอปพลิเคชัน (App-ID), ผู้ใช้งาน (User-ID) และเนื้อหาเชิงลึก (Content-ID) ภายในการตรวจสอบเพียงวงรอบเดียว ช่วยลดความหน่วงของระบบและเพิ่มประสิทธิภาพในการบังคับใช้พยากรณ์ความปลอดภัยตามแนวคิด Zero Trust Architecture อย่างต่อเนื่อง โดยระบบนิเวศนี้ยังผสานรวมเทคโนโลยี Precision AI และการเรียนรู้ของเครื่อง (Machine Learning) เพื่อวิเคราะห์พฤติกรรมที่ผิดปกติและสกัดกั้นภัยคุกคามประเภท Zero-day แบบเรียลไทม์ ครอบคลุมทั้งโครงสร้างพื้นฐานภายในองค์กร (Strata), สภาวะแวดล้อมบนคลาวด์ (Prisma) และการปฏิบัติการตรวจจับและตอบโต้โดยอัตโนมัติ (Cortex) เพื่อสร้างเกราะป้องกันเชิงรุกที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนสูงในปัจจุบันได้อย่างเบ็ดเสร็จ

Palo Alto Networks Next-Generation Firewall (NGFW) โดดเด่นด้วยการออกแบบส่วนต่อประสานกับผู้ใช้แบบกราฟิก (Web-based GUI) ที่เน้นความสอดคล้องเชิงตรรกะและลดความซับซ้อนในการบริหารจัดการ (User Experience Design) ส่งผลให้ผู้ปฏิบัติงานสามารถเรียนรู้ระบบ (Learning Curve) และทำความเข้าใจโครงสร้างเมนูได้อย่างรวดเร็วเมื่อเปรียบเทียบกับผลิตภัณฑ์อื่นในอุตสาหกรรมที่มีลำดับชั้นเมนูซับซ้อน นอกจากนี้ จุดแข็งที่สำคัญคือสถาปัตยกรรมแบบ All-in-One Capabilities ซึ่งรวมฟังก์ชันการบริหารจัดการ (Management), การจัดเก็บและวิเคราะห์ข้อมูลจราจร (Logging), และการสร้างรายงานเชิงลึก (Reporting) ไว้ภายในอุปกรณ์เครื่องเดียว (Single Appliance) โดยไม่ต้องพึ่งพาระบบบริหารจัดการแยกส่วน (Dedicated Management Server) หรือลิขสิทธิ์ซอฟต์แวร์เพิ่มเติมสำหรับฟังก์ชันรายงานผล ดังเช่นข้อจำกัดในสถาปัตยกรรมแบบแยกส่วนของ Check Point ที่จำเป็นต้องใช้ SmartEvent/SmartReporter หรือระบบ Fortinet ที่ต้องอาศัย FortiAnalyzer ในการประมวลผลข้อมูล Log และรายงานผลในระดับสูง การบูรณาการฟังก์ชันเหล่านี้เข้าด้วยกันจึงช่วยลดความซับซ้อนในการออกแบบโครงสร้างพื้นฐาน (Infrastructure Complexity) และลดต้นทุนรวมในการเป็นเจ้าของ (Total Cost of Ownership - TCO) ได้อย่างมีนัยสำคัญ

คุณสมบัติของ Palo Alto Networks NGFW

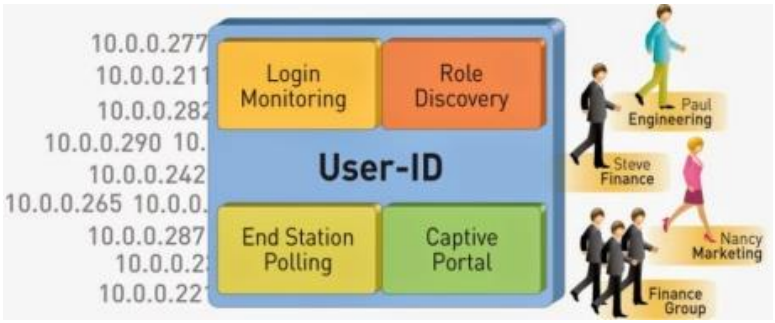
Application-Based Policy Enforcement (App-ID)

เพิ่มความสามารถในการควบคุมการเข้าถึงในระดับแอปพลิเคชั่น (เช่น facebook-chat, bittorent) ซึ่งจะช่วยเพิ่มระดับในการรักษาความปลอดภัยให้มากยิ่งขึ้น เนื่องจากจะสามารถกำหนดรูปแบบของทราฟิกที่จะอนุญาตหรือไม่อนุญาตให้เข้าถึงได้เฉพาะเจาจงมากกว่าการกำหนด policy ในระดับ Layer 4 ที่จะใช้เฉพาะหมายเลขพอร์ตของโปรโตคอล TCP หรือ UPD ในการกำหนด policy เท่านั้น ซึ่งจะทำให้มีโอกาสที่จะถูกปลอมแปลงทราฟิกเกิดขึ้นได้ โดยเฉพาะในปัจจุบันที่มีแอปพลิเคชั่นในลักษณะ web-based เกิดขึ้นมากมาย ถ้าเราอนุญาตให้สามารถติดต่อไปยังปลายทางที่ใช้งาน TCP พอร์ต 80 หรือ 443 ได้ ก็อาจจะมีแอปพลิเคชั่นอื่น ๆ ที่สามารถปลอมแปลงทราฟิกมาใช้งานพอร์ตที่อนุญาตไว้ได้ ยกตัวอย่างเช่น bittorrent ที่โดยปกติจะใช้งานหมายเลขพอร์ตตั้งแต่ 6681 ขึ้นไป ก็สามารถที่จะกำหนดให้เปลี่ยนมาใช้งานพอร์ต 80 หรือ 443 เพื่อปลอมแปลงทราฟิกให้สามารถใช้งานได้ แต่ถ้าเป็นบน Palo Alto Networks NGFW จะสามารถกำหนดแอปพลิเคชั่นไปว่าเป็น web-browsing ทำให้ทราฟิกที่ใช้งาน web-based เท่านั้นที่จะสามารถใช้งานได้ โดยทราฟิกอื่น ๆ ที่ปลอมแปลงมาจะไม่สามารถใช้งานได้ เป็นต้น



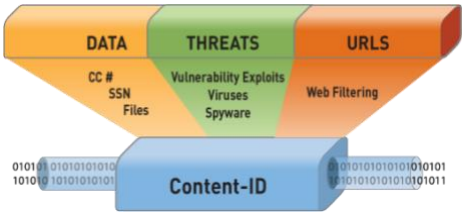
หรืออีกกรณี เช่น ต้องการที่จะอนุญาตทราฟิก DNS ถ้าเป็นบน Palo Alto Networks NGFW ก็จะสามารถกำหนดแอปพลิเคชั่นให้เป็น dns ได้ แต่ถ้าเป็นการใช้งาน Layer 4 Firewall ก็จะสามารถอนุญาตให้ติดต่อไปยังหมายเลขพอร์ต 53 ได้เท่านั้น ซึ่งจะไม่สามารถป้องกันระบบเครือข่ายจากการใช้งานแอปพลิเคชั่นอื่น ๆ ที่หลบเลี่ยงมาใช้งานพอร์ต 53 ได้

User Identification (User-ID)



เพิ่มความสามารถในการกำหนด policy ให้กับผู้ใช้ด้วยการใช้งาน username แทนที่จะใช้เฉพาะหมายเลข IP address เท่านั้น โดยสามารถดึงข้อมูลผู้ใช้มาจาก Directory Server อย่างเช่น Microsoft Active Directory, eDirectory, sunone, OpenLDAP หรือ LDAP ชนิดอื่น ๆ ได้ และยังสามารถใช้ captive portal ที่มีลักษณะเป็นหน้า web authentication ได้ ซึ่งจะเพิ่มความยืดหยุ่นในการกำหนด policy มากยิ่งขึ้น เนื่องจากผู้ใช้งานจะสามารถใช้งานหมายเลข IP address หรือใช้โฮสต์ใดก็ได้ในการใช้งาน ไม่ว่าจะเป็นคอมพิวเตอร์หรือสมาร์ทโฟน ก็จะได้รับ policy ในการใช้งานที่เหมือนกัน

Content Identification (Content-ID)



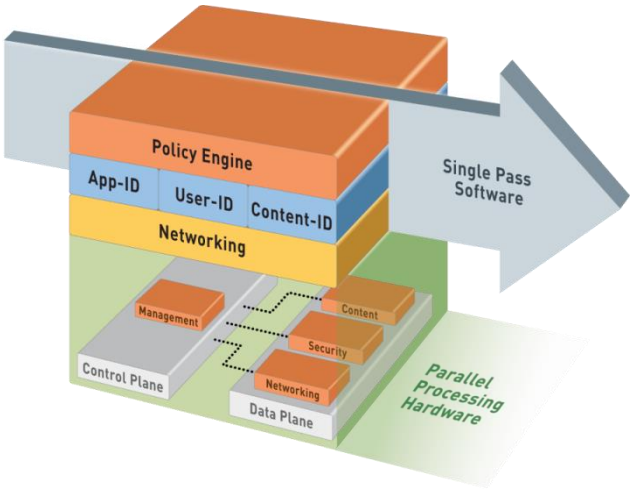
เพิ่มความสามารถในการตรวจสอบทราฟิกที่ใช้งานผ่าน Palo Alto Networks NGFW ได้ในระดับ content ด้วยการใช้ security profile ที่จะประกอบไปด้วย Anti-Virus, Anti-Spyware, Vulnerability (IPS),

URL Filtering, File Blocking, WildFire (Cloud Sandbox สำหรับส่งไฟล์ขึ้นไปทดสอบใช้งานบน Cloud ซึ่งจะช่วยป้องกันการโจมตีแบบ Zero-Day Attack ได้)

Global Protect

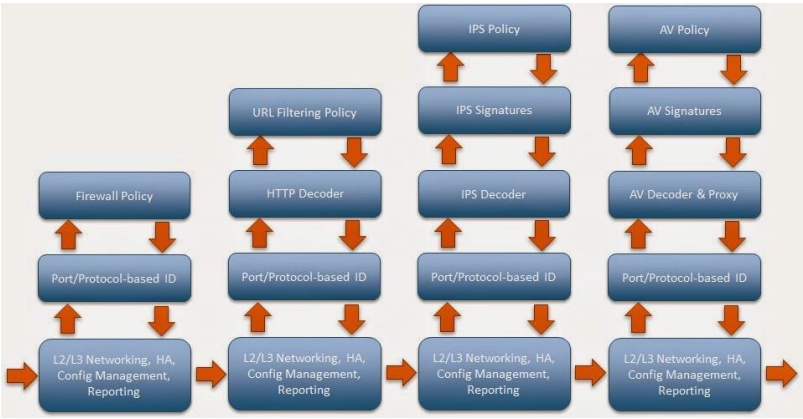
เป็น Remote VPN Client to Site ที่สามารถตรวจสอบรายการความปลอดภัยของโฮสต์ที่จะเชื่อมต่อเข้าสู่ระบบเครือข่ายผ่านทาง IPSec VPN หรือ SSL VPN ได้

1. **สถาปัตยกรรมของ Palo Alto Networks NGFW**

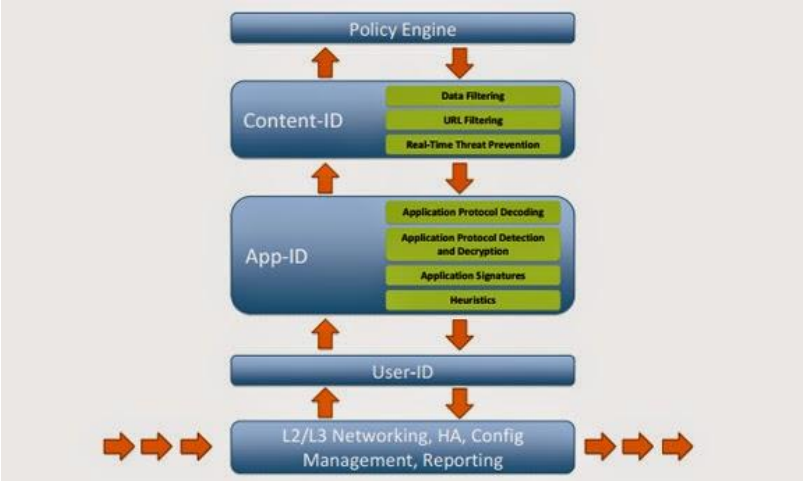


Single Pass

โดยปกติของ Firewall ที่มีความสามารถในการทำงานได้หลายชนิด เช่น Layer 4/7 Firewall, URL Filtering, IPS, Anti-Virus ก็จะมีขั้นตอนการตั้งค่าและการทำงานในแต่ละส่วนแยกออกจากกันอย่างชัดเจน เช่นในการกำหนด policy ก็จะต้องทำการตั้งค่า policy ในแต่ละชนิดแยกจากกัน ซึ่งจะทำให้เกิดความไม่สะดวกในการใช้งาน และยากต่อการตรวจสอบอีกด้วย และในการทำงาน เมื่อมีแพ็คเก็ตเดินทางเข้ามา ก็จะถูกตรวจสอบในระดับ networing ก่อนที่จะส่งไปตรวจสอบ Layer 4/7 Firewall Policy จากนั้น ถ้าได้รับอนุญาต ก็อาจจะถูกส่งไปยังโมดูล URL Filtering ซึ่งจะทำการตรวจสอบในระดับ networing อีกรอบก่อนที่จะตรวจสอบด้วย URL Filtering Policy และถ้าได้รับอนุญาต ก็จะถูกส่งไปตรวจสอบยังโมดูล IPS ซึ่งก็จะต้องทำการตรวจสอบในระดับ networking อีกรอบก่อนที่จะทำการตรวจสอบด้วย IPS Policy ซึ่งจะเห็นว่ามีขั้นตอนการทำงานที่ซ้ำซ้อนและใช้งานทรัพยากรของระบบจำนวนมาก อีกทั้งแม้แต่การทำ Report ยังมีการแยกส่วนกันต่างหาก ทำให้ยากต่อการตรวจสอบมากยิ่งขึ้นไป แต่ถ้าเป็น Palo Alto Networks NGFW จะสามารถประมวลผลทราฟิกในทุก ๆ ขั้นตอนในเวลาพร้อม ๆ กัน โดยจะทำการตรวจสอบในระดับ networking, User-ID, App-ID, Content-ID ด้วยการประมวลผลเพียงครั้งเดียวต่อทราฟิกใน session นั้น ๆ และจะใช้งาน policy เพียงข้อเดียวเท่านั้นในการตั้งค่า ทำให้ Firewall จะประมวลผลทราฟิกเพียงครั้งเดียวเท่านั้น ไม่ต้องทำงานซ้ำซ้อนเหมือนกับ Firewall แบบเดิม รวมไปถึงการทำ Report ที่จะสรุปรวมข้อมูลของการทำงานทุก ๆ ส่วนมาได้ใน Report เดียวกัน



ลักษณะการทำงานของ Firewall แบบเดิม



ลักษณะการทำงานแบบ Single Pass บน Palo Alto Networks NGFW

Parallel Processing

มีการแบ่งแยก Processor ในการทำงานแต่ละชนิดกันอย่างชัดเจน ต่างจากยี่ห้ออื่น ๆ ที่อาจจะใช้งาน Processor เพียงชุดเดียวร่วมกันในการทำงานทุก ๆ ขั้นตอน

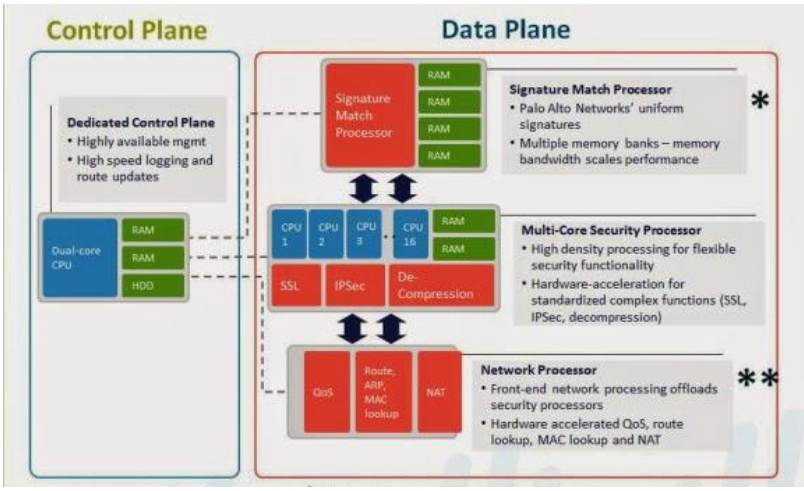
งานด้าน Network อย่างเช่น การค้นหาข้อมูลเส้นทาง, การทำ Flow Lookup, การนับสถิติต่าง ๆ, การทำ NAT จะใช้งาน Network Processor

งานด้าน User-ID, App-ID, Policy Engine จะใช้งาน Multicore Security Processor ที่มี Hardware Acceleration ช่วยในการเข้ารหัส, ถอดรหัส และการทำ Decompression

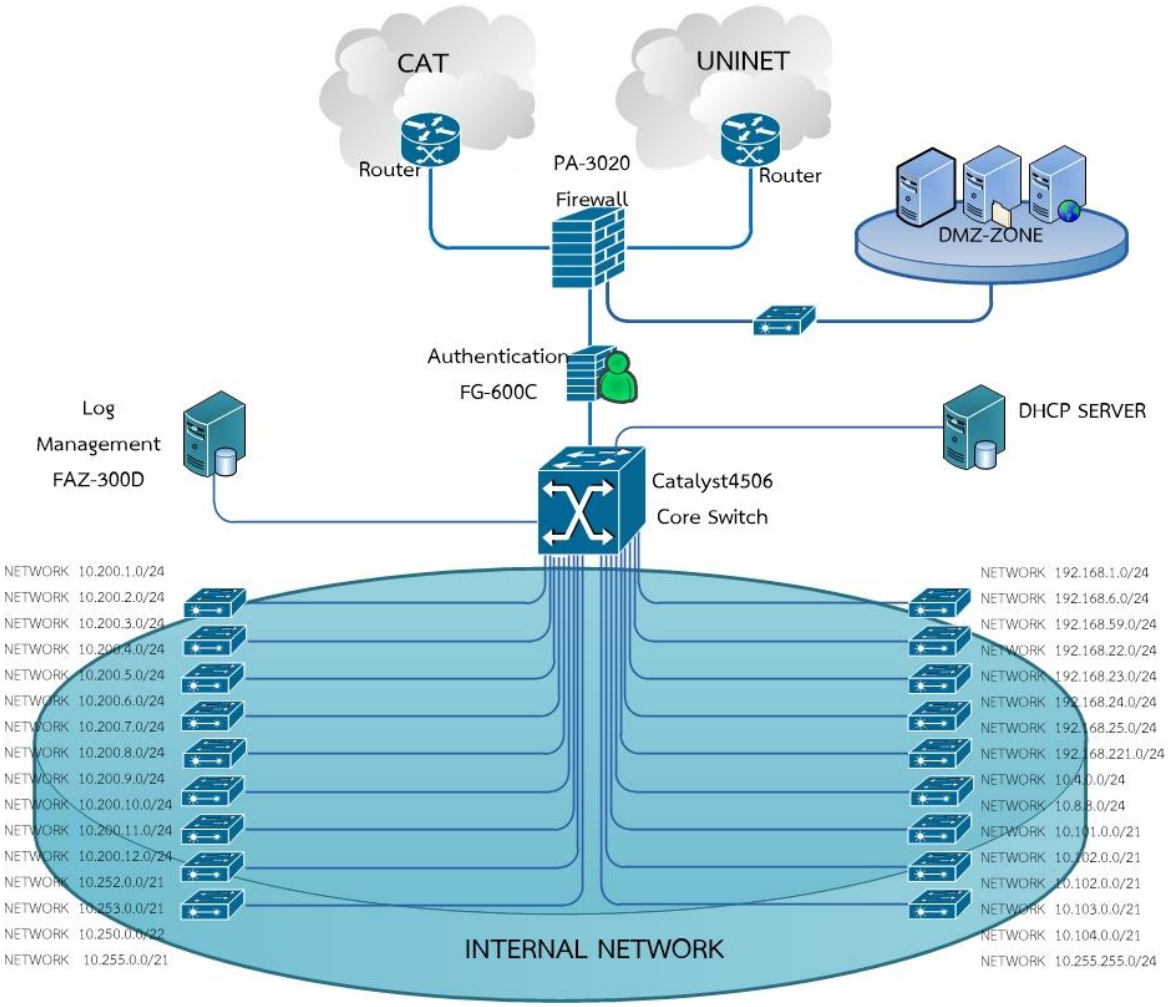
งานด้าน Content-ID อย่างเช่น การเปรียบเทียบทราฟิกกับ Signature ต่าง ๆ จะใช้งาน FPGA (Field-Programmable Gate Array) Threat Processor ที่จะมี Memory แยกส่วนไปต่างหาก

งานด้านการบริหารจัดการตัวอุปกรณ์ เช่น การจัดการด้านการตั้งค่า, Logging, Report ต่าง ๆ จะใช้งาน Control Plane Processor เป็นการแยกส่วนกันระหว่าง Data Plane และ Control Plane อย่างชัดเจน

การใช้งาน Processor แยกส่วนกันอย่างชัดเจนในการทำงานแต่ละชนิด จะเป็นการเพิ่มความสามารถในการทำงานให้มีประสิทธิภาพมากยิ่งขึ้น ในกรณีที่ถูกโจมตีใน Data Plane ก็ยังสามารถที่จะเข้าไปตรวจสอบหรือแก้ไขการตั้งค่าใน Control Plane ได้ตลอดเวลา



2.2 รูปแบบการเชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัยราชภัฏชัยภูมิ



การเชื่อมต่อของ Interface IP Address บน Paloalto PA-3020

Port	IP Address	Description

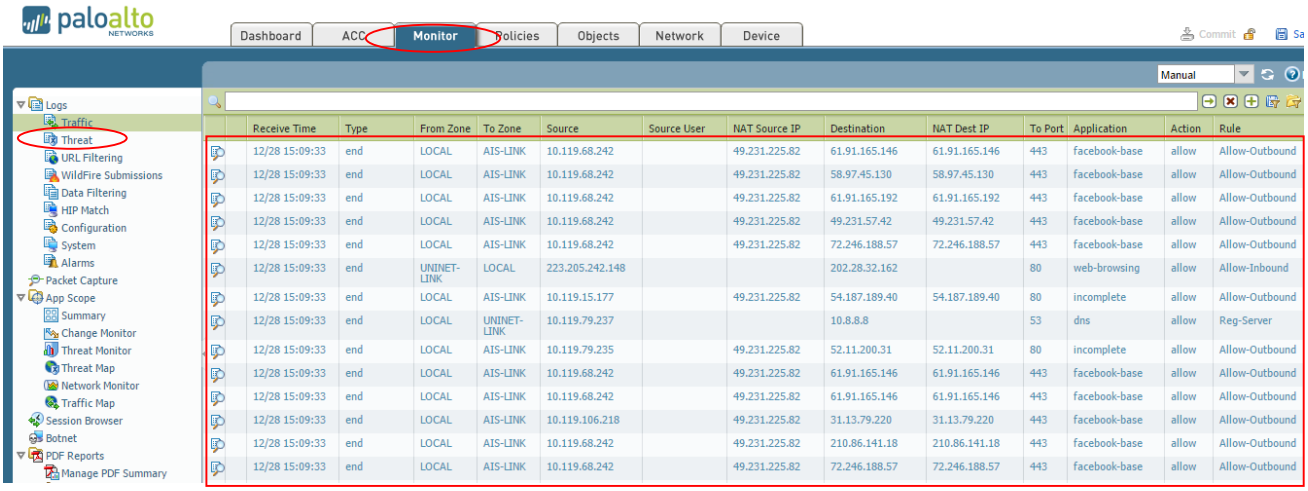
Interface Ethenet 1/1	xxx.xxx.xx.xxx	WAN UNINET
Interface Ethenet 1/2	xxx.xxx.xx.xxx	LAN (Internal Network)
Interface Ethenet 1/11	xxx.xxx.xx.xxx	WAN CAT
Interface Ethenet 1/12	xxx.xxx.xx.xxx	DMZ Zone
Interface Management (MGMT)	xxx.xxx.xx.xxx	Managemet IP Address

2.3 การดูข้อมูลการจราจร (Traffic)

1. Monitor Traffic All

คือ การดูทราฟฟิค (Traffic) ทั้งหมดที่มีการรับส่งข้อมูล ทั้งขาเข้าและขาออก ของระบบเครือข่าย ซึ่งตัวอุปกรณ์สารถทำการค้นหาข้อมูล (Data Searching) ได้ทั้ง Time, Zone, Source Address, Destination Address, NAT, Application, Service Port, Rule, Action เป็นต้น โดยสารถใช้เป็นเครื่องมือในการแก้ปัญหาให้กับผู้ดูแลระบบได้เป็นอย่างดี

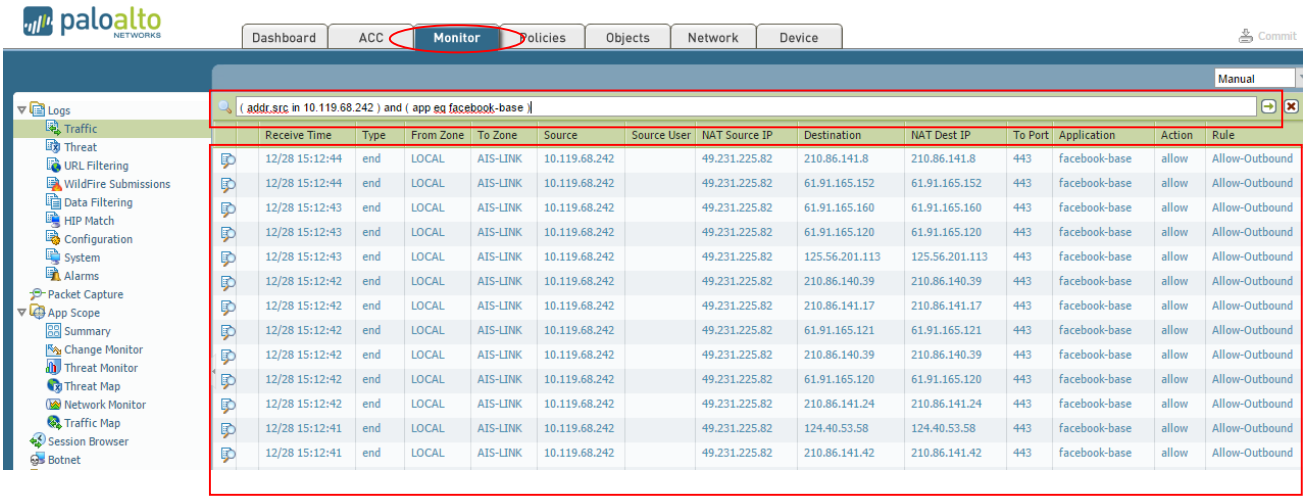
ตัวอย่างการ Monitor Traffic All



Receive Time	Type	From Zone	To Zone	Source	Source User	NAT Source IP	Destination	NAT Dest IP	To Port	Application	Action	Rule
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	61.91.165.146	61.91.165.146	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	58.97.45.130	58.97.45.130	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	61.91.165.192	61.91.165.192	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	49.231.57.42	49.231.57.42	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	72.246.188.57	72.246.188.57	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	UNINET-LINK	LOCAL	223.205.242.148			202.28.32.162		80	web-browsing	allow	Allow-Inbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.15.177		49.231.225.82	54.187.189.40	54.187.189.40	80	incomplete	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	UNINET-LINK	10.119.79.237			10.8.8.8		53	dns	allow	Reg-Server
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.79.235		49.231.225.82	52.11.200.31	52.11.200.31	80	incomplete	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	61.91.165.146	61.91.165.146	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	61.91.165.146	61.91.165.146	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.106.218		49.231.225.82	31.13.79.220	31.13.79.220	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	210.86.141.18	210.86.141.18	443	facebook-base	allow	Allow-Outbound
12/28 15:09:33	end	LOCAL	AIS-LINK	10.119.68.242		49.231.225.82	72.246.188.57	72.246.188.57	443	facebook-base	allow	Allow-Outbound

ตัวอย่างการค้นหาข้อมูล (Data Searching)

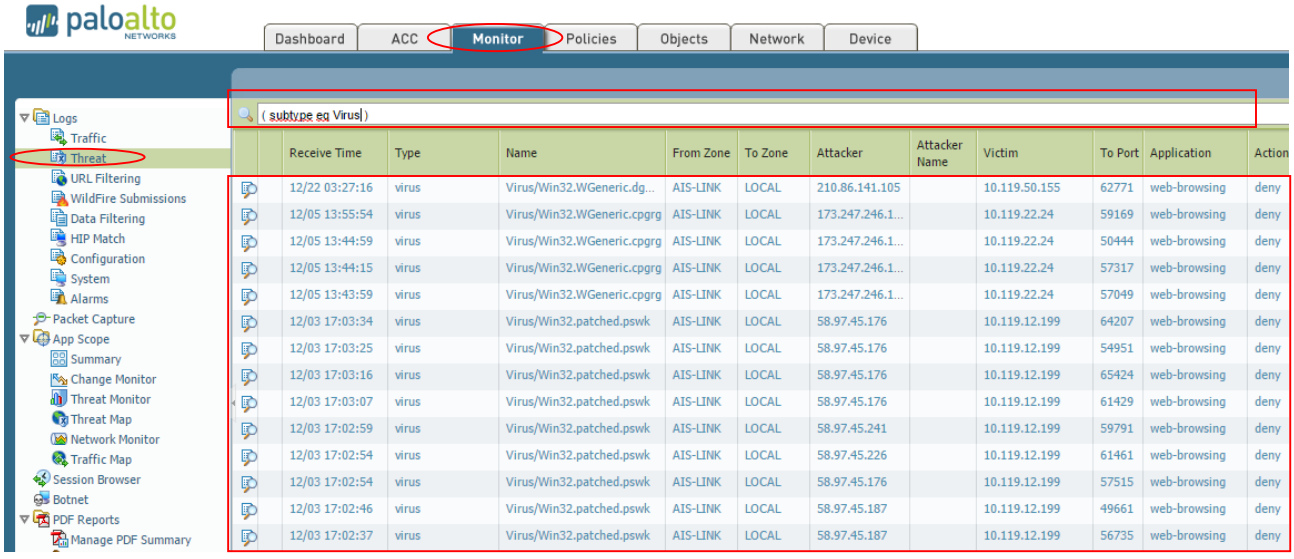
ในรูปเลือกค้นหาเฉพาะ Source IP Address 10.119.68.242 และ Application ที่เป็น facebook-base



2. Monitor Threat

คือ การดูภัยคุกคามและการโจมตีต่าง (Threat Monitor) บนระบบเครือข่าย ทั้งขาเข้าและขาออก และภายในระบบเครือข่ายของเราเอง โดยสามารถป้องกันและมองเห็นภัยคุกคามที่เป็น Virus, Spyware, Vulnerability, URL filtering, Botnet เป็นต้น ของระบบเครือข่าย ซึ่งตัวอุปกรณ์สารถทำการค้นหาภัยคุกคาม (Threat Searching) ได้ทั้ง Time, Type, Name, Zone, Attacker, Victim, Application, Service Port, Action , Severity, Rule เป็นต้น โดยสารถใช้เป็นเครื่องมือในการแก้ปัญหาระบบเครือข่ายให้กับผู้ดูแลระบบได้เป็นอย่างดี

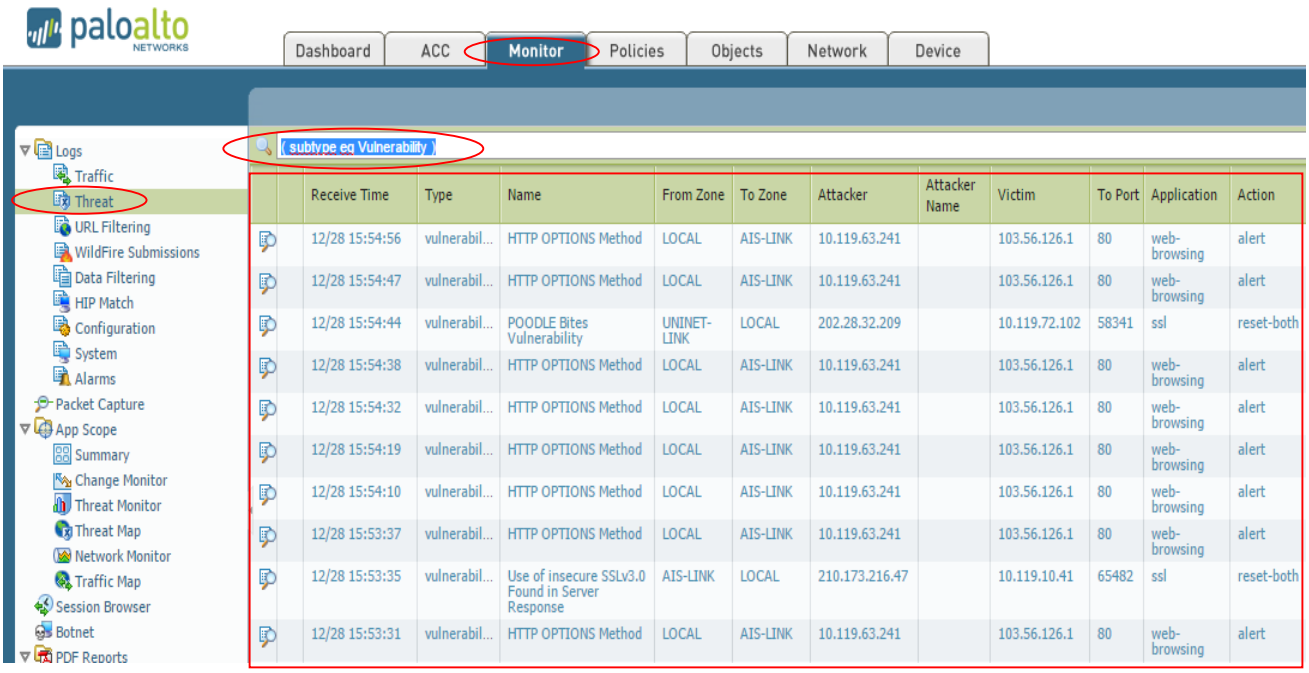
ตัวอย่างค้นหาภัยคุกคาม (Threat Searching) ที่เป็น Virus



ตัวอย่างค้นหาภัยคุกคาม (Threat Searching) ที่เป็น Spyware

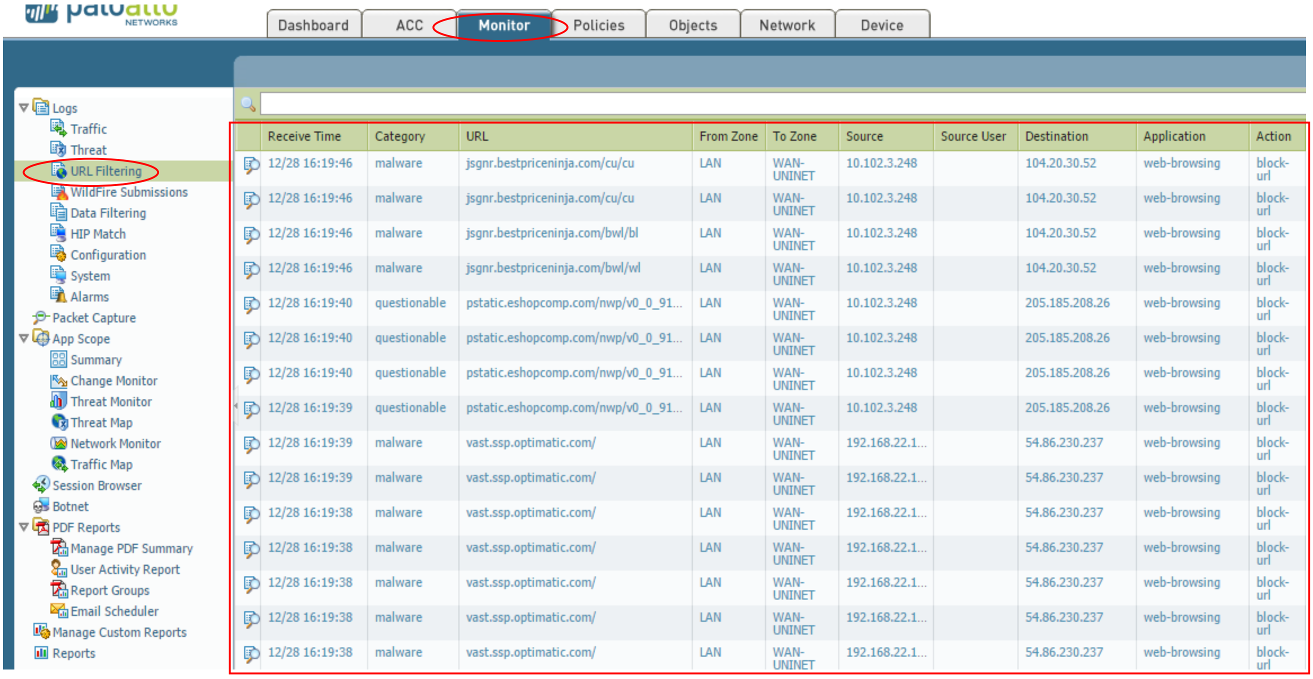
Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action
12/28 15:05:32	spyware	Morto RDP Request Traffic	UNINET-LINK	LOCAL	200.42.62.100		202.28.32.167	3389	ms-rdp	reset-both
12/28 12:56:08	spyware	Morto RDP Request Traffic	UNINET-LINK	LOCAL	123.96.2.99		202.28.32.173	3389	ms-rdp	reset-both
12/28 12:55:45	spyware	Morto RDP Request Traffic	UNINET-LINK	LOCAL	123.96.2.99		202.28.32.167	3389	ms-rdp	reset-both
12/28 12:32:47	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	AIS-LINK	5.189.152.203		49.231.225.85	5060	sip	drop-all-packets
12/28 12:32:47	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	LOCAL	5.189.152.203		49.231.225.84	5060	sip	drop-all-packets
12/28 12:32:47	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	LOCAL	5.189.152.203		49.231.225.83	5060	sip	drop-all-packets
12/28 12:32:47	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	AIS-LINK	5.189.152.203		49.231.225.85	5061	sip	drop-all-packets
12/28 12:32:47	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	AIS-LINK	5.189.152.203		49.231.225.82	6060	sip	drop-all-packets
12/28 12:02:18	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	AIS-LINK	198.7.62.114		49.231.225.85	5060	sip	drop-all-packets
12/28 12:02:18	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	AIS-LINK	198.7.62.114		49.231.225.82	5060	sip	drop-all-packets
12/28 12:02:17	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	LOCAL	198.7.62.114		49.231.225.84	5060	sip	drop-all-packets
12/28 12:02:17	spyware	Sipvicious.Gen User-Agent Traffic	AIS-LINK	LOCAL	198.7.62.114		49.231.225.83	5060	sip	drop-all-packets

ตัวอย่างค้นหาภัยคุกคาม (Threat Searching) ที่เป็น Vulnerability



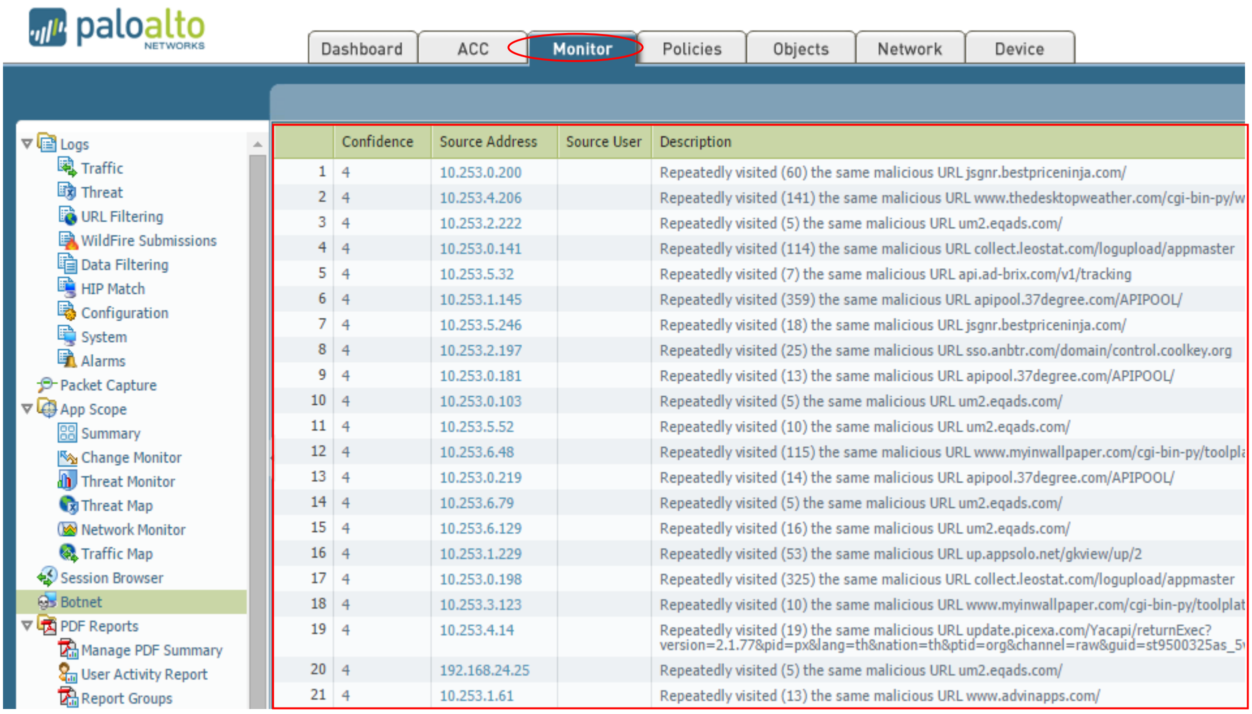
Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action
12/28 15:54:56	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:54:47	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:54:44	vulnerabil...	POODLE Bites Vulnerability	UNINET-LINK	LOCAL	202.28.32.209		10.119.72.102	58341	ssl	reset-both
12/28 15:54:38	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:54:32	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:54:19	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:54:10	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:53:37	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert
12/28 15:53:35	vulnerabil...	Use of insecure SSLv3.0 Found in Server Response	AIS-LINK	LOCAL	210.173.216.47		10.119.10.41	65482	ssl	reset-both
12/28 15:53:31	vulnerabil...	HTTP OPTIONS Method	LOCAL	AIS-LINK	10.119.63.241		103.56.126.1	80	web-browsing	alert

ตัวอย่างค้นหาภัยคุกคาม (Threat Searching) ที่เป็น URL Filtering



Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
12/28 16:19:46	malware	jsgnr.bestpriceninja.com/cu/cu	LAN	WAN-UNINET	10.102.3.248		104.20.30.52	web-browsing	block-url
12/28 16:19:46	malware	jsgnr.bestpriceninja.com/cu/cu	LAN	WAN-UNINET	10.102.3.248		104.20.30.52	web-browsing	block-url
12/28 16:19:46	malware	jsgnr.bestpriceninja.com/bwl/bl	LAN	WAN-UNINET	10.102.3.248		104.20.30.52	web-browsing	block-url
12/28 16:19:46	malware	jsgnr.bestpriceninja.com/bwl/wl	LAN	WAN-UNINET	10.102.3.248		104.20.30.52	web-browsing	block-url
12/28 16:19:40	questionable	pstatic.eshopcomp.com/nwp/v0_0_91...	LAN	WAN-UNINET	10.102.3.248		205.185.208.26	web-browsing	block-url
12/28 16:19:40	questionable	pstatic.eshopcomp.com/nwp/v0_0_91...	LAN	WAN-UNINET	10.102.3.248		205.185.208.26	web-browsing	block-url
12/28 16:19:40	questionable	pstatic.eshopcomp.com/nwp/v0_0_91...	LAN	WAN-UNINET	10.102.3.248		205.185.208.26	web-browsing	block-url
12/28 16:19:39	questionable	pstatic.eshopcomp.com/nwp/v0_0_91...	LAN	WAN-UNINET	10.102.3.248		205.185.208.26	web-browsing	block-url
12/28 16:19:39	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url
12/28 16:19:39	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url
12/28 16:19:38	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url
12/28 16:19:38	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url
12/28 16:19:38	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url
12/28 16:19:38	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url
12/28 16:19:38	malware	vast.ssp.optimatic.com/	LAN	WAN-UNINET	192.168.22.1...		54.86.230.237	web-browsing	block-url

ตัวอย่างค้นหาภัยคุกคาม (Threat Searching) ที่เป็น Botnet

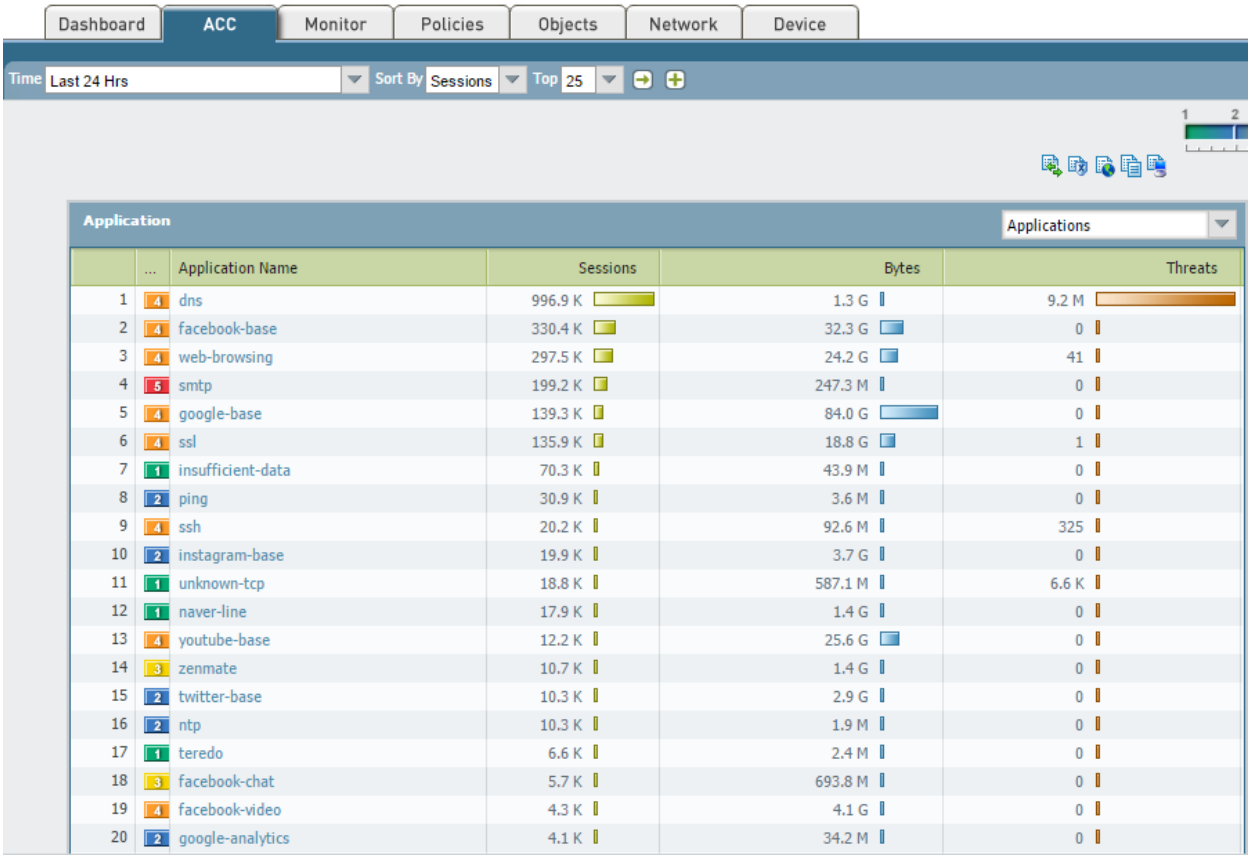


	Confidence	Source Address	Source User	Description
1	4	10.253.0.200		Repeatedly visited (60) the same malicious URL jsgnr.bestpriceninja.com/
2	4	10.253.4.206		Repeatedly visited (141) the same malicious URL www.thedesktopweather.com/cgi-bin-py/w
3	4	10.253.2.222		Repeatedly visited (5) the same malicious URL um2.eqads.com/
4	4	10.253.0.141		Repeatedly visited (114) the same malicious URL collect.leostat.com/logupload/appmaster
5	4	10.253.5.32		Repeatedly visited (7) the same malicious URL api.ad-brix.com/v1/tracking
6	4	10.253.1.145		Repeatedly visited (359) the same malicious URL apipool.37degree.com/APIPOOL/
7	4	10.253.5.246		Repeatedly visited (18) the same malicious URL jsgnr.bestpriceninja.com/
8	4	10.253.2.197		Repeatedly visited (25) the same malicious URL sso.anbtr.com/domain/control.coolkey.org
9	4	10.253.0.181		Repeatedly visited (13) the same malicious URL apipool.37degree.com/APIPOOL/
10	4	10.253.0.103		Repeatedly visited (5) the same malicious URL um2.eqads.com/
11	4	10.253.5.52		Repeatedly visited (10) the same malicious URL um2.eqads.com/
12	4	10.253.6.48		Repeatedly visited (115) the same malicious URL www.myinwallpaper.com/cgi-bin-py/toolpl
13	4	10.253.0.219		Repeatedly visited (14) the same malicious URL apipool.37degree.com/APIPOOL/
14	4	10.253.6.79		Repeatedly visited (5) the same malicious URL um2.eqads.com/
15	4	10.253.6.129		Repeatedly visited (16) the same malicious URL um2.eqads.com/
16	4	10.253.1.229		Repeatedly visited (53) the same malicious URL up.appsolo.net/gkview/up/2
17	4	10.253.0.198		Repeatedly visited (325) the same malicious URL collect.leostat.com/logupload/appmaster
18	4	10.253.3.123		Repeatedly visited (10) the same malicious URL www.myinwallpaper.com/cgi-bin-py/toolplat
19	4	10.253.4.14		Repeatedly visited (19) the same malicious URL update.picexa.com/Yacapi/returnExec? version=2.1.77&pid=px&lang=th&nation=th&ptid=org&channel=raw&guid=st9500325as_5
20	4	192.168.24.25		Repeatedly visited (5) the same malicious URL um2.eqads.com/
21	4	10.253.1.61		Repeatedly visited (13) the same malicious URL www.advinapps.com/

3. Monitor ACC (Application Command Center)

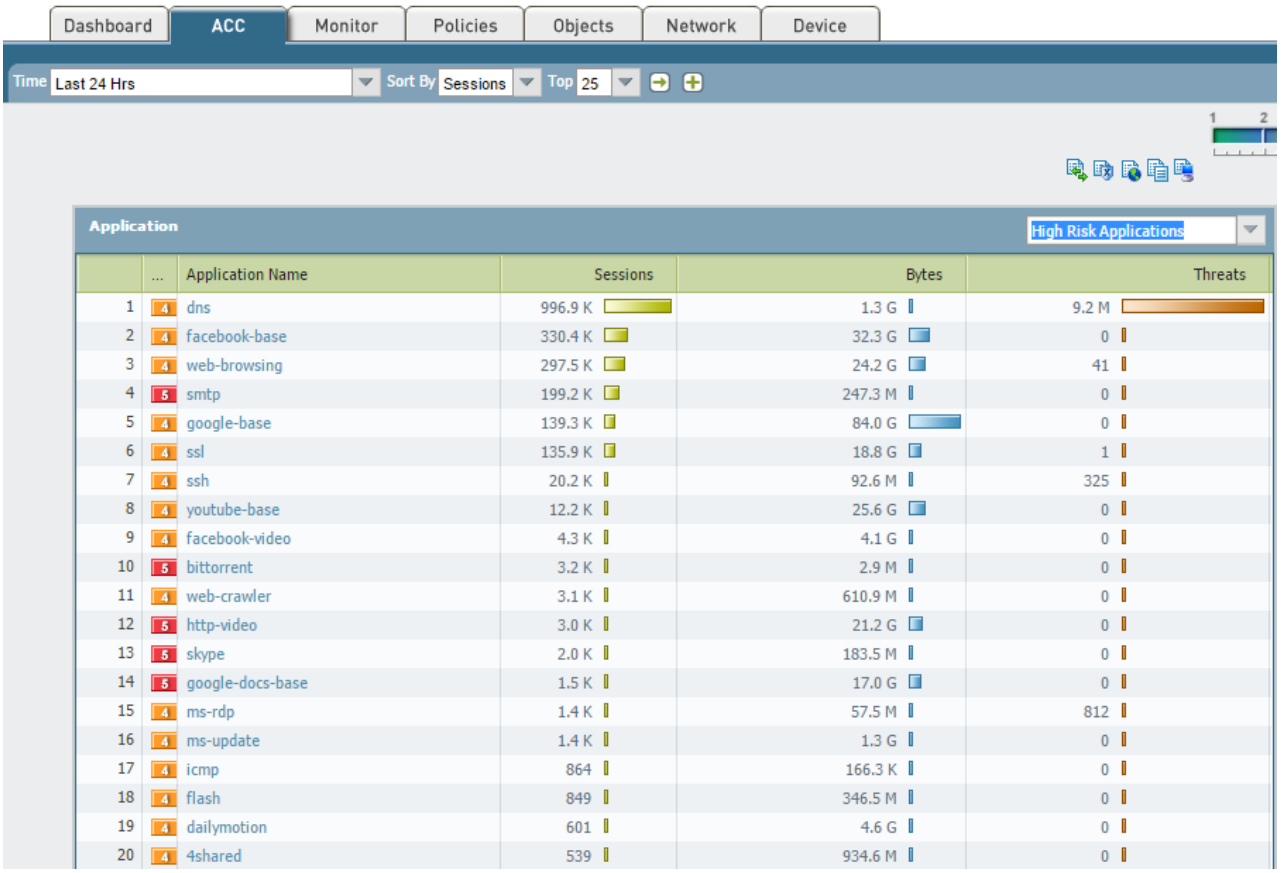
คือการดูการใช้งาน Application และความเสี่ยงทั้งหมดที่เกิดขึ้นภายในระบบเครือข่าย โดยแต่ละ Application หรือ Event สามารถที่จะ Dew-Down ลงลึกเข้าไปดูในรายละเอียดได้ โดยสารถใช้เป็นเครื่องมือในการแก้ปัญหาระบบเครือข่ายให้กับผู้ดูแลระบบได้เป็นอย่างดี

ตัวอย่างการใช้งาน Application ทั้งหมดภายในระบบเครือข่ายจากมากไปหาน้อย



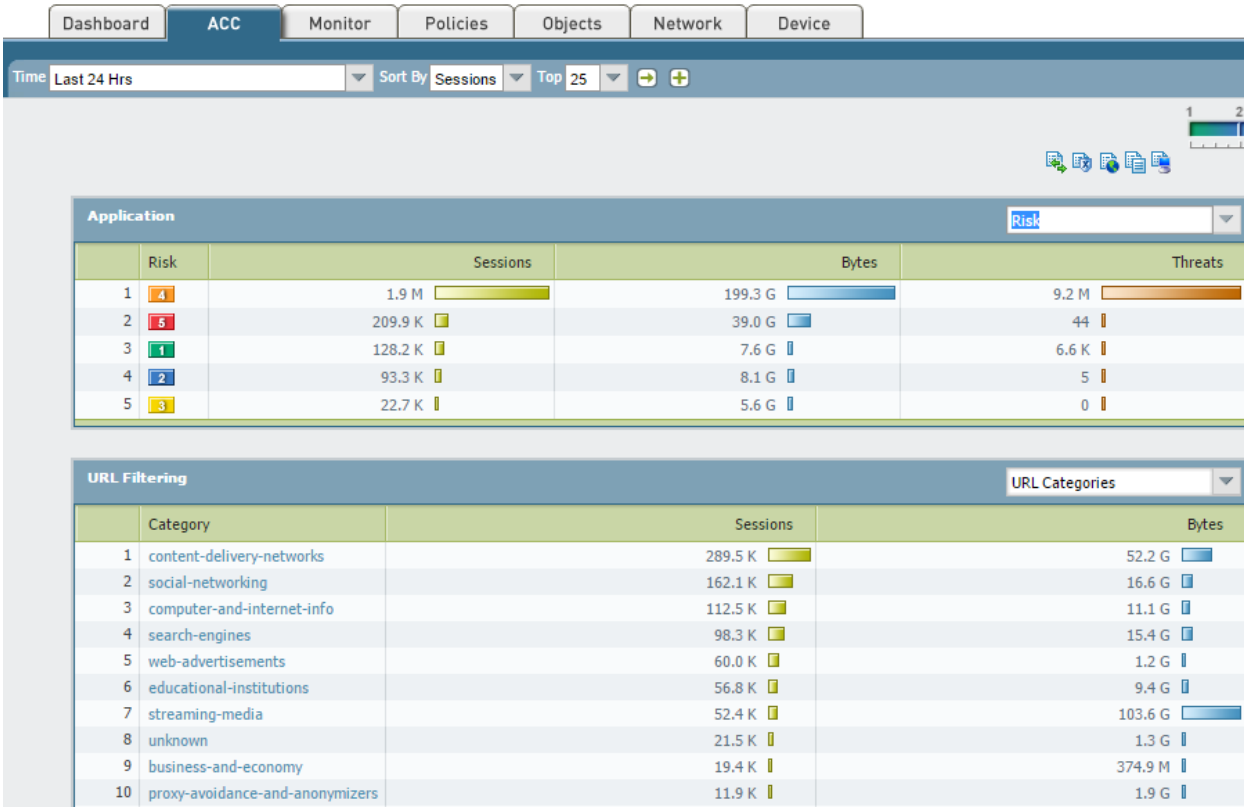
	...	Application Name	Sessions	Bytes	Threats
1	4	dns	996.9 K	1.3 G	9.2 M
2	4	facebook-base	330.4 K	32.3 G	0
3	4	web-browsing	297.5 K	24.2 G	41
4	5	smtp	199.2 K	247.3 M	0
5	4	google-base	139.3 K	84.0 G	0
6	4	ssl	135.9 K	18.8 G	1
7	1	insufficient-data	70.3 K	43.9 M	0
8	2	ping	30.9 K	3.6 M	0
9	4	ssh	20.2 K	92.6 M	325
10	2	instagram-base	19.9 K	3.7 G	0
11	1	unknown-tcp	18.8 K	587.1 M	6.6 K
12	1	naver-line	17.9 K	1.4 G	0
13	4	youtube-base	12.2 K	25.6 G	0
14	3	zenmate	10.7 K	1.4 G	0
15	2	twitter-base	10.3 K	2.9 G	0
16	2	ntp	10.3 K	1.9 M	0
17	1	teredo	6.6 K	2.4 M	0
18	3	facebook-chat	5.7 K	693.8 M	0
19	4	facebook-video	4.3 K	4.1 G	0
20	2	google-analytics	4.1 K	34.2 M	0

ตัวอย่างการใช้งาน Risk Application ที่มีความเสี่ยงในระบบเครือข่ายจากมากไปหาน้อย



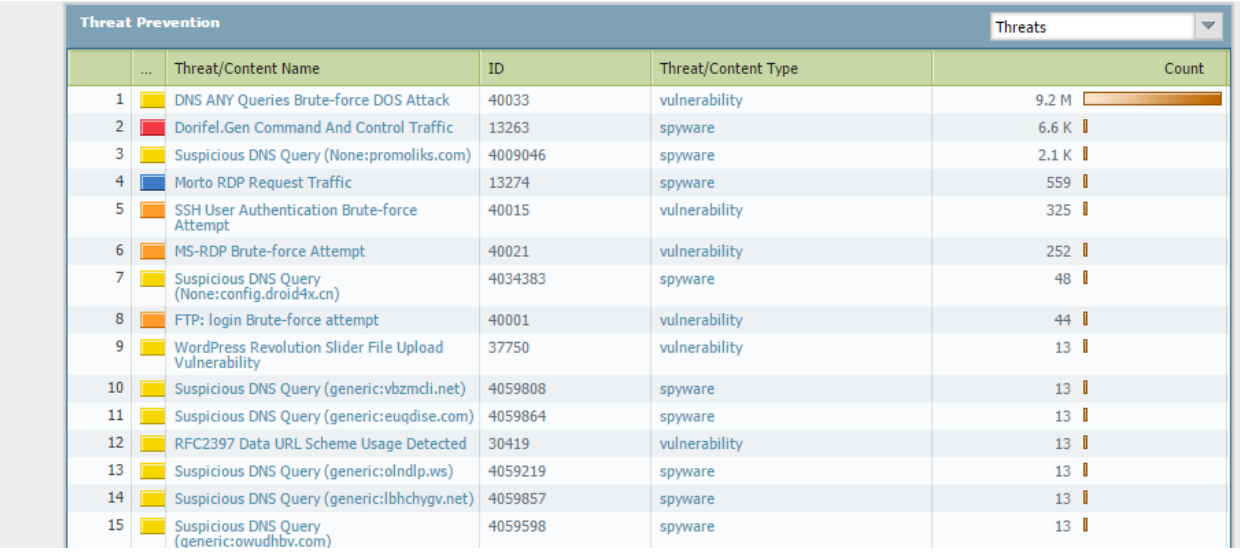
	...	Application Name	Sessions	Bytes	Threats
1	4	dns	996.9 K	1.3 G	9.2 M
2	4	facebook-base	330.4 K	32.3 G	0
3	4	web-browsing	297.5 K	24.2 G	41
4	5	smtp	199.2 K	247.3 M	0
5	4	google-base	139.3 K	84.0 G	0
6	4	ssl	135.9 K	18.8 G	1
7	4	ssh	20.2 K	92.6 M	325
8	4	youtube-base	12.2 K	25.6 G	0
9	4	facebook-video	4.3 K	4.1 G	0
10	5	bittorrent	3.2 K	2.9 M	0
11	4	web-crawler	3.1 K	610.9 M	0
12	5	http-video	3.0 K	21.2 G	0
13	5	skype	2.0 K	183.5 M	0
14	5	google-docs-base	1.5 K	17.0 G	0
15	4	ms-rdp	1.4 K	57.5 M	812
16	4	ms-update	1.4 K	1.3 G	0
17	4	icmp	864	166.3 K	0
18	4	flash	849	346.5 M	0
19	4	dailymotion	601	4.6 G	0
20	4	4shared	539	934.6 M	0

ตัวอย่างความเสี่ยงทั้งหมดภายในระบบเครือข่าย (Risk)



	Risk	Sessions	Bytes	Threats
1	4	1.9 M	199.3 G	9.2 M
2	5	209.9 K	39.0 G	44
3	1	128.2 K	7.6 G	6.6 K
4	2	93.3 K	8.1 G	5
5	3	22.7 K	5.6 G	0

	Category	Sessions	Bytes
1	content-delivery-networks	289.5 K	52.2 G
2	social-networking	162.1 K	16.6 G
3	computer-and-internet-info	112.5 K	11.1 G
4	search-engines	98.3 K	15.4 G
5	web-advertisements	60.0 K	1.2 G
6	educational-institutions	56.8 K	9.4 G
7	streaming-media	52.4 K	103.6 G
8	unknown	21.5 K	1.3 G
9	business-and-economy	19.4 K	374.9 M
10	proxy-avoidance-and-anonymizers	11.9 K	1.9 G



Threat Prevention — Threats

	...	Threat/Content Name	ID	Threat/Content Type	Count
1		DNS ANY Queries Brute-force DOS Attack	40033	vulnerability	9.2 M
2		Dorifel.Gen Command And Control Traffic	13263	spyware	6.6 K
3		Suspicious DNS Query (None:promoliks.com)	4009046	spyware	2.1 K
4		Morto RDP Request Traffic	13274	spyware	559
5		SSH User Authentication Brute-force Attempt	40015	vulnerability	325
6		MS-RDP Brute-force Attempt	40021	vulnerability	252
7		Suspicious DNS Query (None:config.droid4x.cn)	4034383	spyware	48
8		FTP: login Brute-force attempt	40001	vulnerability	44
9		WordPress Revolution Slider File Upload Vulnerability	37750	vulnerability	13
10		Suspicious DNS Query (generic:vbzmcli.net)	4059808	spyware	13
11		Suspicious DNS Query (generic:euqdise.com)	4059864	spyware	13
12		RFC2397 Data URL Scheme Usage Detected	30419	vulnerability	13
13		Suspicious DNS Query (generic:olndlp.ws)	4059219	spyware	13
14		Suspicious DNS Query (generic:lbhchygv.net)	4059857	spyware	13
15		Suspicious DNS Query (generic:owudhbv.com)	4059598	spyware	13

2.4 ทฤษฎีที่เกี่ยวข้อง

1 ทฤษฎีระบบเครือข่ายคอมพิวเตอร์และแบบจำลอง OSI (OSI Model) พื้นฐานสำคัญของการวิเคราะห์ภัยคุกคามเริ่มต้นจากการเข้าใจโครงสร้างการสื่อสารข้อมูลตามมาตรฐาน Open Systems Interconnection (OSI Model) ซึ่งแบ่งการทำงานออกเป็น 7 ชั้น (Layers)

Layer 3 (Network Layer): เกี่ยวข้องกับการหาเส้นทาง (Routing) และหมายเลข IP Address ซึ่งเป็นจุดที่ใช้ตรวจสอบแหล่งที่มา (Source) และปลายทาง (Destination) ของการโจมตี

Layer 4 (Transport Layer): เกี่ยวข้องกับโปรโตคอล TCP/UDP และหมายเลขพอร์ต (Ports) ซึ่งเป็นขอบเขตหลักในการวิเคราะห์การโจมตีประเภท Brute Force ผ่านพอร์ตมาตรฐาน เช่น 22 (SSH) หรือ 3389 (RDP)

Layer 7 (Application Layer): เป็นชั้นที่สำคัญที่สุดในการศึกษานี้ เนื่องจากอุปกรณ์ Palo Alto NGFW ทำงานในชั้นนี้เพื่อจำแนกประเภทแอปพลิเคชัน (App-ID) และตรวจจับเนื้อหาที่เป็นอันตราย (Payload) ที่แฝงมากับข้อมูลปกติ

2. **เทคโนโลยี Next-Generation Firewall (NGFW)** ความแตกต่างระหว่าง Firewall ดั้งเดิมกับ NGFW คือความสามารถในการตรวจสอบข้อมูลเชิงลึก (Deep Packet Inspection)

Application Identification (App-ID): ทฤษฎีการระบุตัวตนแอปพลิเคชันโดยไม่พึ่งพาหมายเลขพอร์ต ทำให้สามารถแยกแยะได้ว่าข้อมูลที่วิ่งผ่านพอร์ต 80 เป็นการเข้าเว็บปกติ หรือเป็นการใช้โปรแกรม BitTorrent หรือ Proxy

User Identification (User-ID): การเชื่อมโยงข้อมูล IP Address เข้ากับอัตลักษณ์บุคคลจากระบบ Active Directory หรือ LDAP เพื่อระบุว่าใครคือเป้าหมายหรือแหล่งกำเนิดของภัยคุกคาม

Content-ID: ทฤษฎีการตรวจจับและป้องกันภัยคุกคามแบบรวมศูนย์ ทั้งการตรวจจับมัลแวร์ (Antivirus), การป้องกันการบุกรุก (IPS), และการกรองเนื้อหาเว็บไซต์ (URL Filtering)

3. ทฤษฎีภัยคุกคามทางไซเบอร์รูปแบบต่างๆ (Cyber Threat Taxonomy) ในการวิเคราะห์ข้อมูลปี 2568 ทฤษฎีที่นำมาอธิบายรูปแบบการโจมตีประกอบด้วย

Brute Force Attack Theory: เป็นวิธีการโจมตีแบบพื้นฐานแต่มีประสิทธิภาพสูง โดยอาศัยหลักความน่าจะเป็น (Probability) ในการสุ่มชุดตัวอักษรเพื่อคาดเดารหัสผ่าน มักใช้ร่วมกับ Dictionary Attack

Denial of Service (DoS/DDoS) Theory: ทฤษฎีการขัดขวางการให้บริการ โดยเน้นไปที่ DNS Amplification Attack ซึ่งใช้ช่องโหว่ของโปรโตคอล UDP ในการขยายขนาดข้อมูลตอบกลับ (Amplification Vector) ให้มีขนาดใหญ่กว่าคำขอหลายเท่า เพื่อถมช่องสัญญาณ (Bandwidth) ของเป้าหมายให้เต็ม

Vulnerability & Exploit Theory: แนวคิดเรื่องช่องโหว่ของซอฟต์แวร์ที่ถูกนำมาใช้เป็นเครื่องมือ (Exploit) ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยเฉพาะช่องโหว่ประเภท Zero-day ที่ยังไม่เป็นที่รู้จัก

4. แนวคิดการป้องกันเชิงลึก (Defense in Depth) และ Zero Trust

Defense in Depth: เป็นกลยุทธ์การวางระบบป้องกันหลายชั้น (Layered Security) เพื่อว่าหากชั้นใดชั้นหนึ่งถูกเจาะผ่านไปได้ ยังมีชั้นถัดไปที่ช่วยสกัดกั้นภัยคุกคามไว้ได้

Zero Trust Architecture (ZTA): ทฤษฎีความปลอดภัยสมัยใหม่ที่ตั้งอยู่บนหลักการ "Never Trust, Always Verify" (ไม่ไว้วางใจใครเลย และต้องตรวจสอบเสมอ) โดยไม่สนว่าการเชื่อมต่อนั้นมาจากภายในหรือภายนอกเครือข่าย ซึ่งสอดคล้องกับการตั้งค่า Policy ในระดับ User-ID ของมหาวิทยาลัย

5. พระราชบัญญัติและมาตรฐานที่เกี่ยวข้อง (Compliance)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA): ทฤษฎีการรักษาความลับของข้อมูล (Confidentiality) เพื่อป้องกันไม่ให้ข้อมูลนักศึกษาและบุคลากรรั่วไหลจากการโจมตี

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562: มาตรฐานการควบคุมและรับมือภัยคุกคามในระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

NIST Cybersecurity Framework (CSF): กรอบแนวคิดสากล 5 ประการ (Identify, Protect, Detect, Respond, Recover) ที่ใช้เป็นมาตรวัดความพร้อมขององค์กรในการรับมือภัยไซเบอร์

6. ทฤษฎีการวิเคราะห์ Log และ Threat Intelligence

Log Analysis: กระบวนการนำข้อมูลบันทึกเหตุการณ์ (Metadata) มาจัดกลุ่มและหาความสัมพันธ์ (Correlation) เพื่อระบุพฤติกรรมที่ผิดปกติ

Indicators of Compromise (IoC): การใช้ข้อมูลพยานหลักฐานดิจิทัล เช่น IP Address ที่เป็นอันตราย, Hash ของไฟล์มัลแวร์ หรือโดเมนที่ติดบัญชีดำ มาเป็นตัวชี้วัดในการตรวจจับภัยคุกคาม

2.5 งานวิจัยหรือข้อมูลที่เกี่ยวข้อง

ด้านประสิทธิภาพของ Next-Generation Firewall (NGFW)

การวิวัฒนาการของภัยคุกคามไซเบอร์ส่งผลให้ Firewall แบบดั้งเดิมไม่สามารถตรวจจับการโจมตีในระดับแอปพลิเคชันได้อย่างมีประสิทธิภาพ Smith และ Wilson (2024) ได้ทำการวิเคราะห์เปรียบเทียบประสิทธิภาพของ NGFW พบว่าความสามารถในการตรวจสอบข้อมูลเชิงลึก (Deep Packet Inspection) ผ่านเทคโนโลยี App-ID และ Content-ID ช่วยให้องค์กรสามารถระบุและสกัดกั้นภัยคุกคามที่พยายามพราง

ตัวผ่านพอร์ตมาตรฐานได้อย่างแม่นยำ ซึ่งสอดคล้องกับคุณสมบัติของ Palo Alto Networks ที่ใช้สถาปัตยกรรมแบบ Single-Pass ในการประมวลผลข้อมูล

สถานการณ์ภัยคุกคามในสถาบันการศึกษา

สถาบันการศึกษากลายเป็นเป้าหมายหลักของการโจมตีทางไซเบอร์เนื่องจากมีผู้ใช้งานจำนวนมากและมีข้อมูลที่หลากหลาย จากรายงานของ Check Point Research (2025) ระบุว่าในปี 2568 ภาคการศึกษามีสถิติการถูกโจมตีสูงถึง 4,388 ครั้งต่อสัปดาห์ต่อองค์กร โดยมีแรงจูงใจหลักจากการเรียกค่าไถ่ข้อมูล (Ransomware) และการขโมยข้อมูลส่วนบุคคล ซึ่งส่งผลกระทบโดยตรงต่อความเชื่อมั่นและข้อบังคับตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

การรับมือการโจมตีผ่านระบบชื่อโดเมน (DNS Attacks)

การโจมตีแบบ DNS ANY Queries เป็นหนึ่งในเทคนิคที่ผู้โจมตีนิยมใช้เพื่อสร้างปริมาณทราฟฟิกมหาศาล (Amplification Attack) Thompson (2023) ได้ศึกษาการบรรเทาผลกระทบจาก DNS Attacks ในเครือข่ายมหาวิทยาลัยขนาดใหญ่ และเสนอแนะว่าการกำหนดค่า Rate Limiting ร่วมกับการใช้ระบบ Threat Intelligence เพื่อวิเคราะห์พฤติกรรมที่ผิดปกติ เป็นวิธีการที่มีประสิทธิภาพที่สุดในการรักษาความพร้อมใช้งาน (Availability) ของระบบเครือข่าย

การป้องกันการสุ่มรหัสผ่าน (Brute Force) และการระบุตัวตน

ปัญหาการโจมตีแบบ Brute Force ผ่านโปรโตคอล SSH หรือ SMB ยังคงเป็นช่องทางหลักที่ผู้ไม่หวังดีใช้เข้าถึงระบบภายใน Garcia และ Lee (2025) เสนอแนวทางการแก้ไขโดยการเปลี่ยนจากการควบคุมระดับ IP มาเป็นการใช้ Identity-Based หรือ User-ID ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถระบุพฤติกรรมเสี่ยงของผู้ใช้งานแต่ละรายได้ชัดเจนขึ้น แม้ว่าผู้โจมตีจะพยายามเปลี่ยนที่อยู่ IP (IP Spoofing) ก็ตาม ซึ่งช่วยลดระยะเวลาในการตอบสนองต่อเหตุการณ์ (Mean Time to Respond) ได้อย่างมีนัยสำคัญ

การประยุกต์ใช้แนวคิด Zero Trust ในสถาบันการศึกษา

พงศธร รัตนสุวรรณ (2568) ได้นำเสนอแบบจำลองการป้องกันเครือข่ายสำหรับมหาวิทยาลัยในยุคดิจิทัล (Digital University) โดยเน้นหลักการ "ไม่ไว้วางใจใครเลย" (Zero Trust Architecture) งานวิจัยระบุว่าการแบ่งส่วนเครือข่าย (Network Segmentation) และการตรวจสอบสิทธิ์อย่างต่อเนื่องผ่าน NGFW ช่วยลดความเสี่ยงจากการขยายตัวของการโจมตีภายในเครือข่าย (Lateral Movement) และช่วยป้องกันอุปกรณ์ IoT ของนักศึกษาที่อาจนำมัลแวร์เข้ามาแพร่ระบาดในระบบเครือข่ายหลักได้

บทที่ 3
หลักเกณฑ์และวิธีการวิเคราะห์

3.1 แหล่งข้อมูล

ข้อมูลที่นำมาวิเคราะห์จาก Log Files จาก Palo Alto NGFW ระหว่างเดือนมกราคม - สิงหาคม 2568 ประกอบด้วย

Application and Threat Summary Report
Top Applications และ Application Categories
Security Rules Usage
Threat Detection Logs
URL Category Filtering
Network Traffic Analysis

3.2 เครื่องมือที่ใช้ในการศึกษาและวิเคราะห์ข้อมูล

เพื่อให้การวิเคราะห์ข้อมูล Log ขนาดใหญ่จาก Palo Alto NGFW มีความแม่นยำและสามารถสรุปผลได้อย่างเป็นรูปธรรม ผู้ศึกษาได้เลือกใช้เครื่องมือผสมผสานดังนี้

1) Palo Alto Networks Panorama / Web Interface: ใช้สำหรับส่งออกข้อมูล (Export) Traffic Logs และ Threat Logs ในรูปแบบไฟล์ CSV โดยกำหนดช่วงเวลาตั้งแต่มกราคม - สิงหาคม 2568 และ Palo Alto Networks Management Interface: สำหรับการดูรายงานและวิเคราะห์

2) Microsoft Excel (Power Query): ใช้เป็นเครื่องมือหลักในการจัดระเบียบข้อมูล (Data Structuring) การทำ Pivot Table เพื่อหาค่าสถิติ และการสร้างแผนภูมิเปรียบเทียบเบื้องต้น

3) Python (Pandas Library): ใช้สำหรับการประมวลผลข้อมูลที่มีปริมาณมาก (Big Data Analysis) เพื่อค้นหาความสัมพันธ์ที่ซับซ้อน เช่น การเชื่อมโยงระหว่าง Source IP กับพฤติกรรมการโจมตีซ้ำ ๆ ในช่วงเวลาที่กำหนด

3.3 ขั้นตอนการวิเคราะห์ข้อมูล

กระบวนการวิเคราะห์ข้อมูล Log จากอุปกรณ์ Palo Alto Next-Generation Firewall ของมหาวิทยาลัยราชภัฏชัยภูมิ แบ่งออกเป็น 3 ขั้นตอนหลักตามระเบียบวิธีวิจัยเชิงวิเคราะห์ (Analytical Research) ดังนี้

3.3.1 การคัดกรองและเตรียมข้อมูล (Data Preparation and Cleaning)

เนื่องจากข้อมูล Log ที่ดึงมาจากอุปกรณ์ Firewall ในช่วงเดือนมกราคม – สิงหาคม 2568 มีปริมาณมหาศาล (Big Data) การเตรียมข้อมูลให้พร้อมก่อนการวิเคราะห์จึงเป็นขั้นตอนที่สำคัญที่สุด เพื่อลดสัญญานรบกวน (Noise) และเพิ่มความแม่นยำในการสรุปผล

การรวมชุดข้อมูล (Data Integration) นำไฟล์ Log ที่แยกตามรายเดือนมาทำการรวม (Merge) เข้าด้วยกันโดยใช้ Python Library 'Pandas' เพื่อสร้างชุดข้อมูลหลัก (Master Dataset) ที่มีโครงสร้างเดียวกัน

การคัดกรองคุณลักษณะ (Feature Selection): เลือกเฉพาะฟิลด์ข้อมูลที่จำเป็นต่อการวิเคราะห์ภัยคุกคาม ได้แก่

Receive Time: เวลาที่เกิดเหตุการณ์

Source IP / Country: ที่อยู่ต้นทางและประเทศต้นทาง

Destination IP: ที่อยู่เป้าหมายภายในเครือข่ายมหาวิทยาลัย

Application: ประเภทแอปพลิเคชัน (App-ID)

Threat/Content Type: ประเภทภัยคุกคาม (Content-ID)

Action: การตอบสนองของ Firewall (Allow/Deny/Drop)

User: ข้อมูลผู้ใช้งานที่ระบุโดย User-ID

การจัดการข้อมูลที่ผิดปกติ (Data Cleaning) กำจัดข้อมูลที่ซ้ำซ้อน (Duplicate Rows) ที่เกิดจากการบันทึก Log ซ้ำในเสี้ยววินาทีเดียวกัน จัดการค่าที่ว่างเปล่า (Missing Values) เช่น กรณีที่ไม่สามารถระบุ Country ได้ ให้ทำการตรวจสอบด้วยระบบ IP Geolocation ภายนอกเพื่อเติมข้อมูลให้ครบถ้วน การทำ Normalization ข้อมูลเวลา (Timestamp) ให้เป็นรูปแบบมาตรฐานเดียวกัน เพื่อความสะดวกในการวิเคราะห์พฤติกรรมการโจมตีตามช่วงเวลา (Time-series Analysis)

3.3.2 การจัดกลุ่มและวิเคราะห์ประเภทการโจมตี

ในขั้นตอนนี้ ผู้ศึกษาใช้จุดเด่นของสถาปัตยกรรม Single-Pass ของ Palo Alto Networks ในการจำแนกภัยคุกคาม เพื่อทำความเข้าใจถึง "วิธีการ" (How) และ "ช่องทาง" (Where) ที่ผู้โจมตีใช้

การวิเคราะห์ ผ่าน App-ID (Application Identification)

วิเคราะห์ทราฟฟิกที่ผิดปกติซึ่งแฝงมาในพอร์ตมาตรฐาน เช่น การใช้พอร์ต 80 (HTTP) หรือ 443 (HTTPS) แต่มีพฤติกรรมที่ไม่ใช่การเข้าเว็บไซต์ทั่วไป

จัดกลุ่มแอปพลิเคชันที่มีความเสี่ยงสูง (High Risk Apps) เช่น p2p, proxy, หรือ web-browsing ที่มีการเชื่อมต่อกับ Server ที่มีประวัติไม่ดี

วิเคราะห์การใช้งานโปรโตคอลเฉพาะทาง เช่น dns, ssh, และ rdp ซึ่งมักถูกใช้เป็นช่องทางในการบุกรุกหรือทำ Denial of Service (DoS)

การวิเคราะห์ผ่าน Content-ID (Threat Identification)

Brute Force Attack Analysis คัดแยก Log ที่ระบุพฤติกรรมการสุ่มรหัสผ่าน (Brute Force) โดยเน้นไปที่บริการ SSH และ Web Login ของมหาวิทยาลัย เพื่อวิเคราะห์ความถี่และ IP ต้นทางที่ทำการโจมตีซ้ำๆ

Vulnerability Exploitation วิเคราะห์การพยายามเจาะระบบผ่านช่องโหว่ของซอฟต์แวร์ (Exploits) เช่น ความพยายามส่ง SQL Injection หรือ Cross-Site Scripting (XSS) เข้ามายังเว็บเซิร์ฟเวอร์ของมหาวิทยาลัย

DNS Security Analysis มุ่งเน้นไปที่การตรวจจับ DNS ANY Queries ซึ่งเป็นรูปแบบหนึ่งของการทำ Reflection Attack เพื่อหาว่ามีการพยายามใช้ DNS Server ของมหาวิทยาลัยเป็นเครื่องมือในการโจมตีผู้อื่นหรือไม่

3.3.3 การวิเคราะห์พฤติกรรมผู้ใช้งานและระบุตัวตน (User Behavior Analysis via User-ID)

ขั้นตอนนี้เป็นการนำข้อมูลในระดับ Network มาเชื่อมโยงกับระดับบุคคล (Identity) เพื่อให้ทราบว่า "ใคร" (Who) คือผู้ที่ได้รับผลกระทบหรือเป็นต้นเหตุของความเสี่ยง

การเชื่อมโยง IP กับ Identity ใช้ข้อมูลจาก User-ID Agent ที่เชื่อมต่อกับ Active Directory ของมหาวิทยาลัยราชภัฏชัยภูมิ เพื่อระบุว่า IP Address ภายในที่ตรวจพบพฤติกรรมเสี่ยงนั้น เป็นบัญชีผู้ใช้งานของกลุ่มใด (นักศึกษา, อาจารย์, หรือบุคลากร)

การวิเคราะห์พฤติกรรมเสี่ยง (Risk Profiling) ตรวจสอบการเข้าถึงเว็บไซต์ที่ถูกจัดอยู่ในหมวดหมู่ "Malicious" หรือ "Phishing" โดยแยกตามกลุ่มผู้ใช้งาน

วิเคราะห์พฤติกรรมการดาวน์โหลดข้อมูลในปริมาณที่ผิดปกติ (Anomaly Data Transfer) ซึ่งอาจเป็นสัญญาณของการติดมัลแวร์หรือการพยายามดึงข้อมูลออกนอกองค์กร (Data Exfiltration)

การระบุผู้ใช้งานที่มีความเสี่ยงสูง (Top Risky Users) จัดลำดับผู้ใช้งาน 50 อันดับแรกที่พบเหตุการณ์ด้านความปลอดภัยบ่อยที่สุด เพื่อนำไปสู่การดำเนินมาตรการเชิงรุก เช่น การบังคับเปลี่ยนรหัสผ่าน หรือการจัดอบรม Cybersecurity Awareness เฉพาะกลุ่ม

3.3.4 การสรุปและสร้างรายงานภาพรวม

ขั้นตอนสุดท้ายคือการนำผลลัพธ์จากทั้ง 3 ส่วนมาสังเคราะห์เป็นข้อสรุป

Statistical Synthesis คำนวณค่าสถิติเชิงพรรณนา (Descriptive Statistics) เช่น จำนวนครั้งการโจมตีรวม, สัดส่วนประเภทการโจมตี, และช่วงเวลาที่เกิดเหตุการณ์สูงสุด (Peak Time)

Correlation Analysis วิเคราะห์หาความสัมพันธ์ระหว่าง "ประเภทแอปพลิเคชัน" กับ "กลุ่มผู้ใช้งาน" เพื่อระบุว่าแอปพลิเคชันใดเป็นช่องทางหลักที่ทำให้เกิดความเสี่ยงในแต่ละกลุ่ม

Visualization นำเสนอข้อมูลในรูปแบบของ Dashboard และ Heat Map เพื่อให้ง่ายต่อการทำความเข้าใจสถานะความปลอดภัยของมหาวิทยาลัยในภาพรวม และใช้เป็นข้อมูลพื้นฐานในการเสนอแนะมาตรการป้องกันในบทที่ 5

บทที่ 4
ผลการวิเคราะห์

ผลการวิเคราะห์ข้อมูลภัยคุกคามและความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏชัยภูมิ จากอุปกรณ์ Palo Alto Networks NGFW (รุ่น PA-1410) ในช่วงระยะเวลา 8 เดือน (มกราคม – สิงหาคม 2568) มีรายละเอียดดังนี้

4,1 ผลการวิเคราะห์ภาพรวมภัยคุกคาม (Global Threat Landscape)

จากการเก็บรวบรวมข้อมูลผ่านระบบ Log Management ตรวจพบอุบัติการณ์ด้านความปลอดภัยรวมทั้งสิ้น 1,973,952 รายการ สะท้อนให้เห็นว่าโครงสร้างพื้นฐานดิจิทัลของมหาวิทยาลัยตกเป็นเป้าหมายของการพยายามบุกรุกอย่างต่อเนื่อง

4.1.1 ประเภทภัยคุกคามหลัก

1. DNS ANY Queries Brute Force DoS Attack (ร้อยละ 63.0)

คำอธิบายเชิงวิชาการ: เป็นการโจมตีในรูปแบบ DNS Amplification Attack ซึ่งเป็นประเภทหนึ่งของ Reflection Denial of Service (DoS) ผู้โจมตีจะส่งคำขอ (Query) ประเภท "ANY" ไปยัง DNS Server โดยใช้การปลอมแปลง IP ต้นทาง (IP Spoofing) เป็น IP ของเป้าหมาย เมื่อ DNS Server ตอบกลับด้วยข้อมูลขนาดใหญ่ไปยังเป้าหมาย จะส่งผลให้ช่องสัญญาณ (Bandwidth) ของเป้าหมายเต็มจนไม่สามารถให้บริการได้

นัยสำคัญ ปริมาณที่สูงถึง 1.24 ล้านครั้ง สะท้อนว่าโครงสร้างพื้นฐาน DNS ของมหาวิทยาลัยกำลังถูกใช้เป็นเครื่องมือ (Reflector) ในการโจมตีผู้อื่น หรือตัวเซิร์ฟเวอร์เองกำลังถูกหน่วงประสิทธิภาพ

2. Microsoft Windows NTLMSSP Detection (ร้อยละ 11.0)

คำอธิบายเชิงวิชาการ: NTLMSSP (NT LAN Manager Security Support Provider) คือโปรโตคอลการยืนยันตัวตนของ Windows การที่ระบบตรวจพบผิดปกติในส่วนนี้มักเกี่ยวข้องกับพฤติกรรม Reconnaissance หรือการพยายามดึงข้อมูล (Enumeration) เพื่อตรวจสอบชื่อผู้ใช้และโดเมนภายในเครือข่าย

นัยสำคัญ เป็นสัญญาณของการพยายามขยายผลการโจมตีภายในเครือข่าย (Lateral Movement) เพื่อค้นหาบัญชีที่มีสิทธิ์สูง (Privileged Accounts)

3. Linux Kernel ksmbd SMB2 Vulnerability (ร้อยละ 8.4)

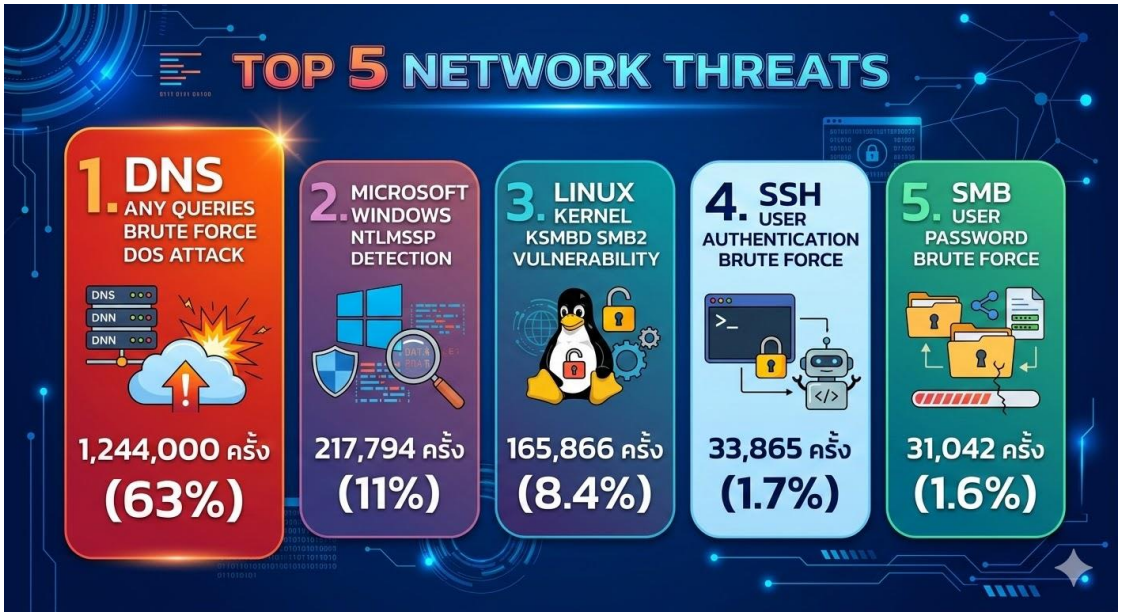
คำอธิบายเชิงวิชาการ: เป็นการพยายามใช้ช่องโหว่ (Exploitation) บนโมดูล ksmbd ใน Linux Kernel ซึ่งทำหน้าที่จัดการไฟล์ผ่านโปรโตคอล SMB2 หากโจมตีสำเร็จ ผู้โจมตีอาจสามารถทำ Remote Code Execution (RCE) หรือรันคำสั่งอันตรายบนเซิร์ฟเวอร์ได้โดยไม่ต้องมีสิทธิ์

นัยสำคัญ บ่งชี้ว่าเซิร์ฟเวอร์ฐานข้อมูลหรือเซิร์ฟเวอร์ไฟล์ที่เป็น Linux ของมหาวิทยาลัยตกเป็นเป้าหมายของการเจาะระบบโดยตรง

4. SSH & SMB User Authentication Brute Force (รวมร้อยละ 3.3)

คำอธิบายเชิงวิชาการ: คือการโจมตีแบบ Dictionary Attack หรือการสุ่มรหัสผ่านซ้ำ ๆ ไปยังบริการ SSH (Remote Management) และ SMB (File Sharing) เพื่อเข้าถึงระบบในระดับผู้ใช้งาน

นัยสำคัญ: แม้สัดส่วนจะน้อยกว่า DoS แต่มีความเสี่ยงสูงที่สุดในแง่ของ Data Breach เพราะหากสุ่มรหัสผ่านสำเร็จเพียงครั้งเดียว ผู้โจมตีจะสามารถเข้าถึงข้อมูลภายในมหาวิทยาลัยได้ทันที



ภาพ ประเภทภัยคุกคามหลัก

4.1.2 การวิเคราะห์ตามประเภทการโจมตี (Threat Classification Analysis)

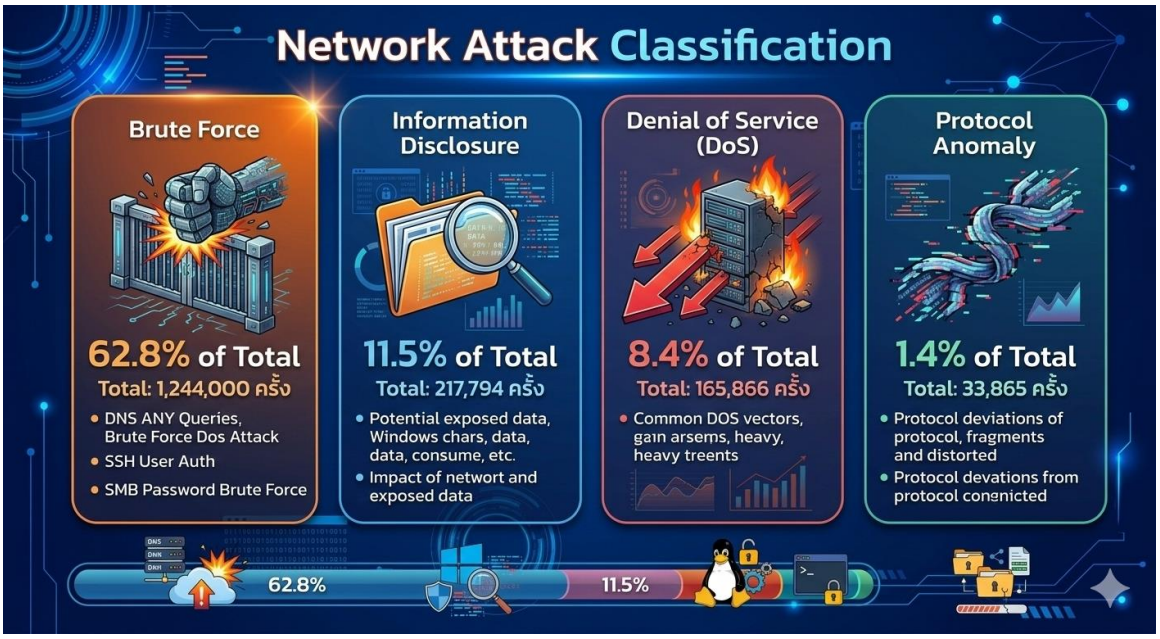
จากการจัดกลุ่มภัยคุกคามที่ระบบ Palo Alto NGFW ตรวจพบ สามารถจำแนกตามลักษณะพฤติกรรมทางเทคนิคได้ 4 ประเภทหลัก ดังนี้

1. การโจมตีแบบสุ่มข้อมูลเพื่อผ่านระบบรักษาความปลอดภัย (Brute Force Attacks) สถิติ: 1,240,000 ครั้ง (ร้อยละ 62.8) เป็นเทคนิคการโจมตีพื้นฐานแต่มีประสิทธิภาพสูง โดยผู้โจมตีจะใช้ชุดข้อมูลรหัสผ่านจำนวนมหาศาล (Dictionary Attack) หรือการสุ่มรหัสผ่านทุกรูปแบบที่อาจเป็นไปได้ เพื่อพยายามเข้าถึงระบบผ่านบริการที่มีการยืนยันตัวตน เช่น SSH, SMB และระบบ Login ของมหาวิทยาลัย
ความเสี่ยงระดับองค์กร ปริมาณที่สูงกว่าร้อยละ 60 สะท้อนว่ามหาวิทยาลัยถูกบอทเน็ต (Botnet) สแกนหาช่องทางเข้าถึงระบบตลอดเวลา หากรหัสผ่านของบุคลากรหรือนักศึกษาไม่มีความซับซ้อนพอ (Weak Password) จะนำไปสู่การรั่วไหลของข้อมูลขนาดใหญ่ได้

2. การพยายามเข้าถึงและเปิดเผยข้อมูลสารสนเทศ (Information Disclosure) สถิติ: 227,590 ครั้ง (ร้อยละ 11.5) เป็นประเภทการโจมตีที่มุ่งเน้นการดึงข้อมูลเกี่ยวกับระบบปฏิบัติการ (OS), รุ่นของซอฟต์แวร์, รายชื่อผู้ใช้งาน หรือโครงสร้างไดเรกทอรีของเซิร์ฟเวอร์ ข้อมูลส่วนใหญ่ที่ตรวจพบเกี่ยวข้องกับโปรโตคอล NTLMSSP ของ Windows ซึ่งมักถูกใช้เป็นฐานข้อมูลเบื้องต้นสำหรับผู้โจมตีในการทำ Reconnaissance
ความเสี่ยงระดับองค์กร แม้การเปิดเผยข้อมูลอาจไม่สร้างความเสียหายทันที แต่ถือเป็นขั้นตอนสำคัญในการ "ทำความรู้จักเป้าหมาย" เพื่อเลือกใช้มัลแวร์หรือช่องโหว่ที่ตรงจุดในขั้นตอนถัดไป

3. การโจมตีเพื่อทำให้ระบบหยุดการตอบสนอง (Denial of Service - DoS) สถิติ: 165,890 ครั้ง (ร้อยละ 8.4) เป็นการส่งข้อมูลจำนวนมากหรือคำขอที่ผิดปกติเข้าสู่ระบบเพื่อใช้ทรัพยากรของ CPU, Memory หรือ Bandwidth จนถึงขีดจำกัด โดยในข้อมูลชุดนี้ส่วนใหญ่เกิดจากพฤติกรรม DNS ANY Queries และ Linux SMB2 Vulnerability ซึ่งส่งผลกระทบต่อความพร้อมใช้งาน (Availability) ของบริการไอทีภายในมหาวิทยาลัย **ความเสี่ยงระดับองค์กร** หากการโจมตีประเภทนี้ประสบความสำเร็จ จะส่งผลให้ระบบการเรียนการสอนออนไลน์ หรือเว็บไซต์หน่วยงานไม่สามารถเข้าถึงได้ สร้างความเสียหายต่อความน่าเชื่อถือและประสิทธิภาพการดำเนินงาน

4. ความผิดปกติของระเบียบวิธีสื่อสาร (Protocol Anomaly) สถิติ: 27,200 ครั้ง (ร้อยละ 1.4) คือทราฟฟิกที่จัดรูปแบบข้อมูลผิดไปจากมาตรฐาน (RFC Standards) ของโปรโตคอลนั้นๆ เช่น การส่ง Packet ที่มีขนาดใหญ่ผิดปกติ หรือการแก้ไขค่าใน Header ที่ระบบไม่รองรับ ซึ่งมักใช้เป็นเทคนิคในการหลบเลี่ยงการตรวจจับของ Firewall (Evasion Techniques) **ความเสี่ยงระดับองค์กร** แม้จะมีสัดส่วนน้อยที่สุด แต่ Protocol Anomaly มักเชื่อมโยงกับการใช้เครื่องมือเจาะระบบระดับสูง (Advanced Exploits) หรือมัลแวร์เฉพาะทางที่พยายามเจาะผ่านช่องโหว่ของอุปกรณ์เครือข่ายโดยตรง

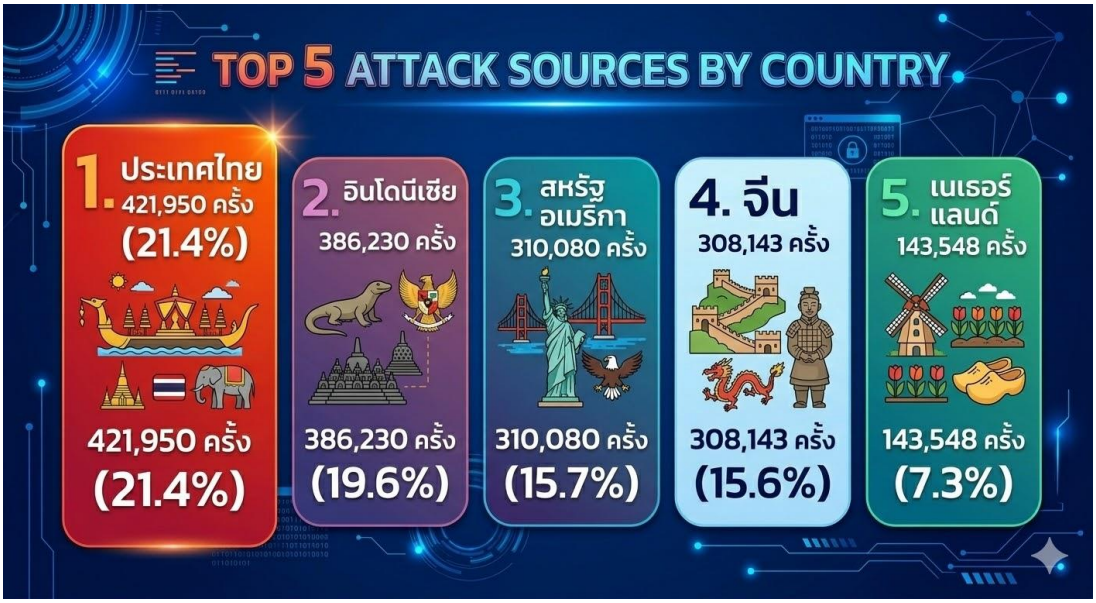


4.2 การวิเคราะห์แหล่งที่มาของการโจมตี

4.2.1 การวิเคราะห์ภูมิศาสตร์ไซเบอร์ของแหล่งกำเนิดภัย(ประเทศแหล่งที่มาหลัก)

จากการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ที่ถูกปิดกั้นโดยระบบ Palo Alto NGFW พบว่าลักษณะการกระจายตัวของแหล่งกำเนิดภัยคุกคามมีความสัมพันธ์กับสถิติอาชญากรรมทางไซเบอร์ในระดับสากล โดยตรวจพบการโจมตีจาก ประเทศไทย มากที่สุดเป็นอันดับหนึ่ง (421,950 ครั้ง หรือร้อยละ 21.4) ซึ่ง

ในทางวิชาการวิเคราะห์ได้ว่าเป็นผลมาจากปรากฏการณ์ "Internal Botnet Infection" หรือการที่เครื่องคอมพิวเตอร์ภายในประเทศถูกฝังมัลแวร์และใช้เป็นฐานในการแพร่กระจายการโจมตีต่อภายในเครือข่ายสถานศึกษาเอง ขณะที่กลุ่มประเทศ อินโดนีเซีย สหรัฐอเมริกา และจีน (รวมร้อยละ 50.9) เป็นกลุ่มแหล่งกำเนิดหลักที่สอดคล้องกับรายงานสถานการณ์ภัยคุกคามโลก ซึ่งมักเป็นที่ตั้งของเซิร์ฟเวอร์ที่ถูกแฮ็กหรือเครือข่าย Proxy ที่ผู้โจมตีใช้เพื่อพรางตัวในการทำสแกนพอร์ตและช่องโหว่อัตโนมัติ ข้อมูลนี้ชี้ให้เห็นถึงความจำเป็นในการใช้มาตรการ Geo-Blocking หรือการจำกัดสิทธิ์การเข้าถึงทรัพยากรสำคัญจากกลุ่มประเทศที่มีความเสี่ยงสูงเพื่อลดพื้นที่การถูกโจมตี (Attack Surface) ของมหาวิทยาลัยลงอย่างมีประสิทธิภาพ

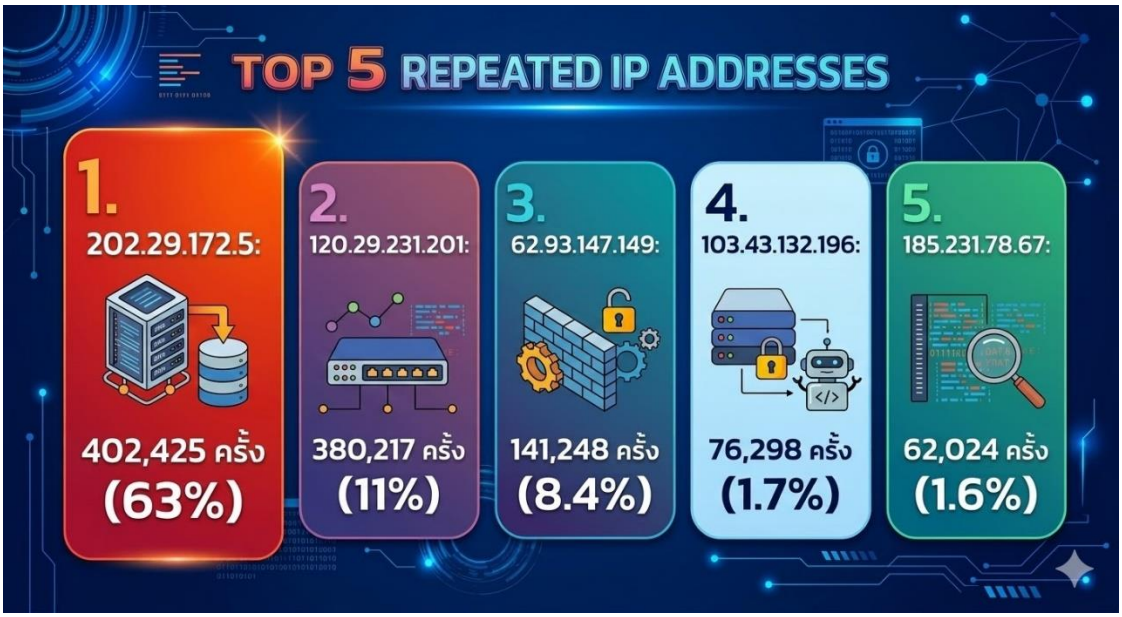


4.2.3 การวิเคราะห์พฤติกรรมและความเชื่อมโยงของแหล่งที่อยู่ไอพีที่โจมตีสูงสุด

จากการวิเคราะห์เชิงลึกด้านพฤติกรรมการเชื่อมต่อ (Connection Behavior) ของแหล่งที่มาตรวจพบว่า มีหมายเลขไอพีจำนวน 5 ลำดับแรกที่มีการสร้างทราฟฟิกภัยคุกคามในปริมาณที่สูงผิดปกติอย่างมีนัยสำคัญ โดยหมายเลขไอพี 202.29.172.5 และ 120.29.231.201 มียอดการโจมตีสะสมรวมกันกว่า 780,000 ครั้ง ซึ่งคิดเป็นเกือบครึ่งหนึ่งของภัยคุกคามทั้งหมดที่ตรวจพบ

ในทางวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ พฤติกรรมเช่นนี้สามารถวิเคราะห์ได้เป็น 2 ประเด็นหลัก คือ ประการแรก หมายเลขไอพีเหล่านี้อาจเป็น "Dedicated Attack Nodes" หรือเครื่องแม่ข่ายที่ถูกออกแบบมาเพื่อสแกนช่องโหว่และยิงการโจมตี (Automated Scanning) โดยเฉพาะ และประการที่สอง ซึ่งมีความเป็นไปได้สูงสำหรับไอพีในกลุ่มขึ้นต้นด้วย 202.x.x.x และ 120.x.x.x คือการเป็น "Compromised Assets" หรือเครื่องคอมพิวเตอร์ภายในเครือข่ายสถาบันการศึกษาอื่นในประเทศไทยที่ถูกผู้โจมตีเข้ายึดครอง (Hijacked) แล้วใช้เป็นฐานในการแพร่กระจายการโจมตีแบบ Brute Force หรือ DoS ใส่กันเองภายในเครือข่ายความร่วมมือ (Inter-University Network)

นอกจากนี้ การพบไอพีจากต่างประเทศ เช่น 62.93.147.149 และ 185.231.78.67 ที่มีการโจมตีหลักหมื่นถึงหลักแสนครั้ง สะท้อนถึงการใช้เครือข่าย Botnet ระดับสากลในการสุ่มโจมตีเป้าหมายที่มีช่วงไอพีสาธารณะ ข้อมูลชุดนี้จึงเป็นหลักฐานสำคัญในการกำหนดนโยบายการป้องกันแบบ IP Blacklisting และการตั้งค่า Threshold-based Blocking บนอุปกรณ์ Palo Alto เพื่อตัดการเชื่อมต่อจากแหล่งที่มาที่มีพฤติกรรมผิดปกติเหล่านี้โดยอัตโนมัติในอนาคต



4.3 การวิเคราะห์เป้าหมายการโจมตี

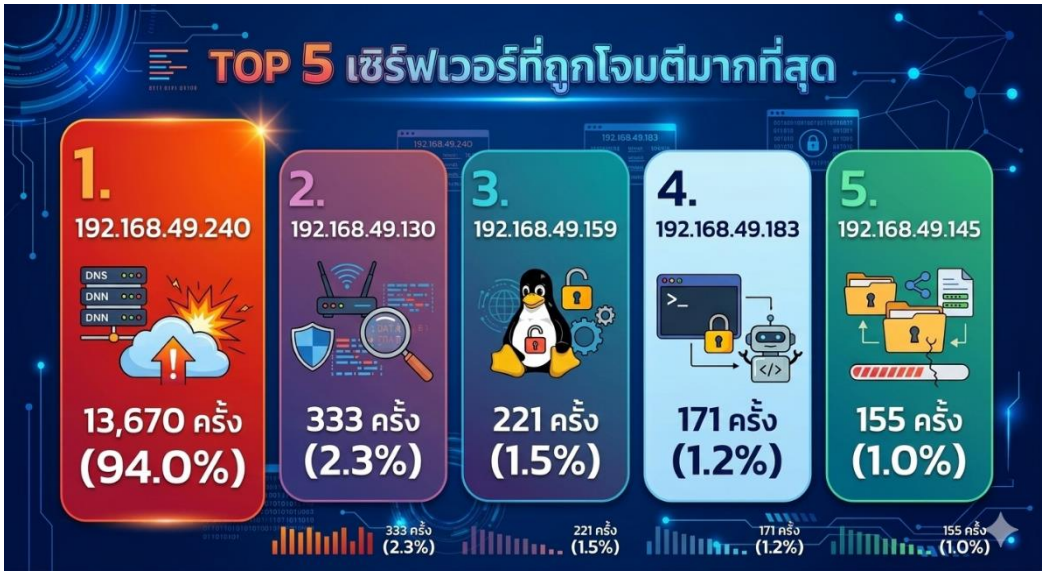
4.3.1 การวิเคราะห์พฤติกรรมการโจมตีพุ่งเป้าต่อโครงสร้างพื้นฐานภายใน

จากการวิเคราะห์ข้อมูลทราฟฟิกขาเข้า (Inbound Traffic) ที่ผ่านการคัดกรองโดยอุปกรณ์ Palo Alto NGFW พบว่ากลุ่มหมายเลขไอพีภายใน (Private IP Address) ในวงเครือข่าย 192.168.49.x เป็นเป้าหมายหลักของการโจมตี โดยเฉพาะหมายเลขไอพี 192.168.49.240 ซึ่งถูกโจมตีสูงถึง 13,670 ครั้ง คิดเป็นสัดส่วนที่สูงกว่าเป้าหมายอันดับอื่นอย่างมีนัยสำคัญ

ในความปลอดภัยเครือข่าย พฤติกรรมการโจมตีที่กระจุกตัวเช่นนี้บ่งชี้ว่า หมายเลขไอพีดังกล่าวอาจเป็น "Critical Asset" หรือเซิร์ฟเวอร์หลักที่ให้บริการแก่สาธารณะ (Public-facing Server) เช่น เว็บไซต์มหาวิทยาลัย หรือระบบสารสนเทศนักศึกษา ซึ่งทำให้ผู้โจมตีสามารถตรวจพบ (Discovery) ได้ง่ายจากภายนอก

สำหรับกลุ่มเซิร์ฟเวอร์ลำดับที่ 2 ถึง 5 (เช่น 192.168.49.130 และ .159) แม้จะมีปริมาณการโจมตีอยู่ในหลักร้อยครั้ง แต่พฤติกรรมนี้สะท้อนถึงการทำ "Internal Reconnaissance" หรือการสแกนหาช่องโหว่ภายในวงแลน (Lateral Movement) หลังจากที่ผู้โจมตีอาจจะสามารถยึดเครื่องลูกข่ายบางเครื่องได้แล้ว หรือเป็นการพยายามสุ่มโจมตีพอร์ตบริการที่เปิดทิ้งไว้ ข้อมูลนี้ชี้ให้เห็นความจำเป็นเร่งด่วนในการทำ Network

Segmentation เพื่อแยกส่วนเซิร์ฟเวอร์ที่มีความสำคัญสูงออกจากกัน และการเพิ่มความเข้มงวดของกฎไฟร์วอลล์ (Micro-segmentation) เพื่อจำกัดการเข้าถึงเฉพาะส่วนงานที่จำเป็นเท่านั้น



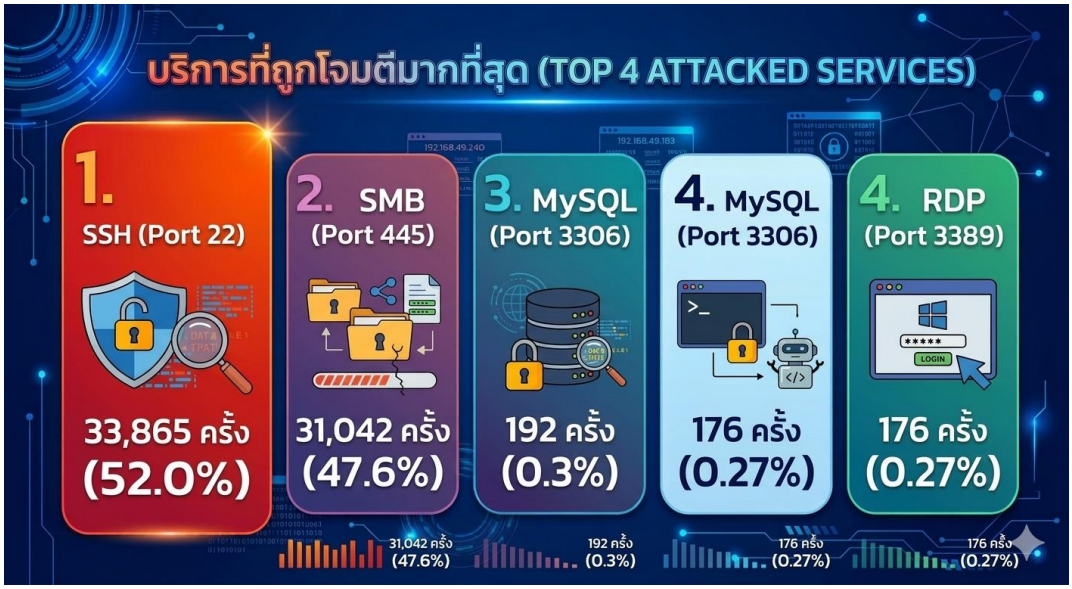
4.3.2 การวิเคราะห์ภัยคุกคามจำแนกตามพอร์ตบริการ

จากการจำแนกข้อมูลการโจมตีตามหมายเลขพอร์ต (Port-based Classification) พบว่าผู้โจมตีมุ่งเน้นการเจาะระบบผ่านบริการสำคัญที่เป็นช่องทางหลักในการบริหารจัดการและแบ่งปันข้อมูลภายในเครือข่าย โดยมีรายละเอียดวิเคราะห์เชิงเทคนิคดังนี้:

บริการ SSH (Port 22): 33,865 ครั้ง การวิเคราะห์: พอร์ต 22 เป็นช่องทางมาตรฐานในการรีโมทเพื่อบริหารจัดการเซิร์ฟเวอร์ (Secure Shell) ปริมาณการโจมตีที่สูงที่สุดในกลุ่มนี้สะท้อนถึงความพยายามในการทำ SSH Brute Force อย่างหนัก เพื่อสุ่มรหัสผ่านเข้าสู่ระบบในระดับ Administrator หรือ Root ซึ่งหากสำเร็จผู้โจมตีจะสามารถควบคุมเซิร์ฟเวอร์ได้อย่างเบ็ดเสร็จ

บริการ SMB (Port 445): 31,042 ครั้ง การวิเคราะห์: พอร์ต 445 ใช้สำหรับบริการแชร์ไฟล์และเครื่องพิมพ์ในระบบ Windows (Server Message Block) ปริมาณการโจมตีที่สูงใกล้เคียงกับ SSH ชี้ให้เห็นถึงความพยายามในการใช้ช่องโหว่ประเภท Remote Code Execution (RCE) เช่น EternalBlue หรือการสุ่มรหัสผ่านเพื่อเข้าถึงไฟล์ข้อมูลสำคัญของมหาวิทยาลัย

บริการ MySQL (Port 3306) และ RDP (Port 3389) การวิเคราะห์: แม้จะมีปริมาณการโจมตีในหลักร้อยครั้ง แต่มีความสำคัญในเชิงคุณภาพ (High Impact) เนื่องจากการโจมตีพอร์ต 3306 มุ่งเป้าไปที่การขโมยหรือทำลายฐานข้อมูล (Database) และพอร์ต 3389 (Remote Desktop) มุ่งเป้าไปที่การยึดหน้าจอควบคุมของเครื่องแม่ข่ายโดยตรง



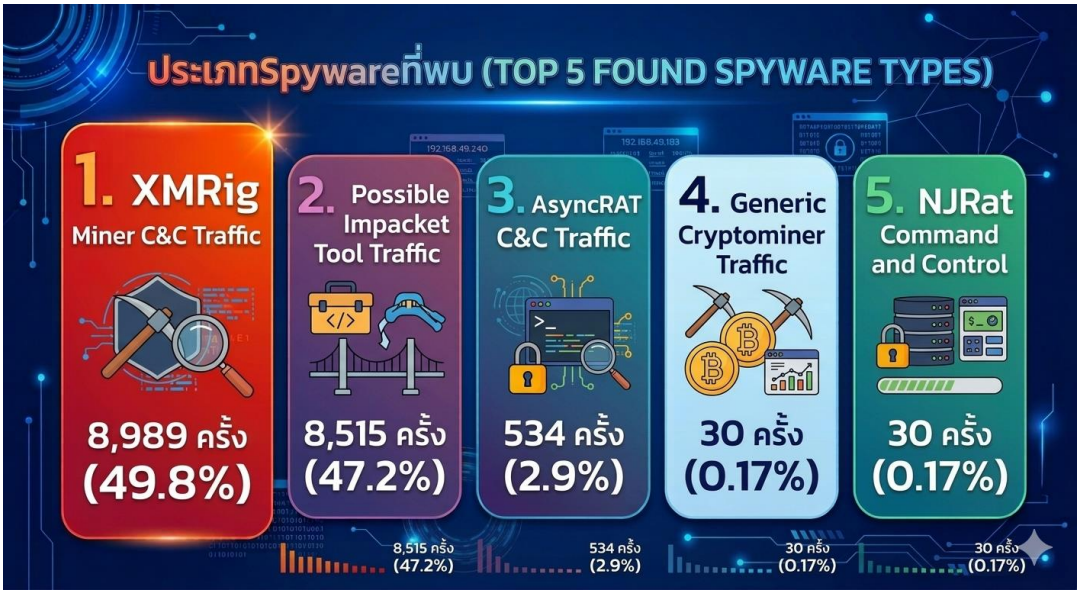
4.4 การวิเคราะห์Spyware และ Malware

4.4.1 ประเภท Spyware

กลุ่มขุดเหรียญดิจิทัล (Cryptojacking): XMRig Miner และ Generic Cryptominer (รวม 9,019 ครั้ง) การวิเคราะห์ ตรวจพบทราฟฟิกของ XMRig ซึ่งเป็นโปรแกรมขุดเหรียญ Monero ที่ถูกผู้ไม่หวังดีแอบติดตั้งในเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ปริมาณการสื่อสารที่สูงเกือบ 9,000 ครั้ง บ่งชี้ว่ามีการใช้ทรัพยากรประมวลผล (CPU/GPU) และพลังงานไฟฟ้าของสถาบันไปเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี ส่งผลให้เครื่องคอมพิวเตอร์ทำงานช้าลงและเสื่อมสภาพก่อนกำหนด

กลุ่มเครื่องมือเจาะระบบและขยายผล (Post-Exploitation Tools): Possible Impacket Tool (8,515 ครั้ง) การวิเคราะห์ การตรวจพบร่องรอยของ Impacket ซึ่งเป็นชุดเครื่องมือ Python ที่แฮ็กเกอร์นิยมใช้ในการทำ Lateral Movement (การขยับขยายการโจมตีภายในเครือข่าย) และการดึงข้อมูลรหัสผ่าน (Credential Dumping) ถือเป็นสัญญาณอันตรายระดับสูง ชี้ให้เห็นว่ามีผู้บุกรุกเข้ามาอยู่ภายในเครือข่ายแล้วและกำลังพยายามยึดครองเครื่องอื่น ๆ ในวงแลน

กลุ่มมัลแวร์ควบคุมระยะไกล (Remote Access Trojan - RAT): AsyncRAT และ NJRat (รวม 564 ครั้ง) การวิเคราะห์ ตรวจพบการติดต่อกลับไปยังเครื่องแม่ข่ายสั่งการ (C&C Traffic) ของมัลแวร์ตระกูล AsyncRAT และ NJRat ซึ่งเป็นเครื่องมือที่ช่วยให้ผู้โจมตีสามารถเข้าควบคุมหน้าจอ เปิดกล้อง แอบดูการพิมพ์ (Keylogging) และขโมยไฟล์ข้อมูลได้แบบเรียลไทม์ แม้จำนวนครั้งจะน้อยกว่ากลุ่มแรก แต่มีความร้ายแรงในแง่ของการจารกรรมข้อมูล (Espionage) และความเป็นส่วนตัวของบุคลากร



4.5 การวิเคราะห์การใช้งานแอปพลิเคชัน

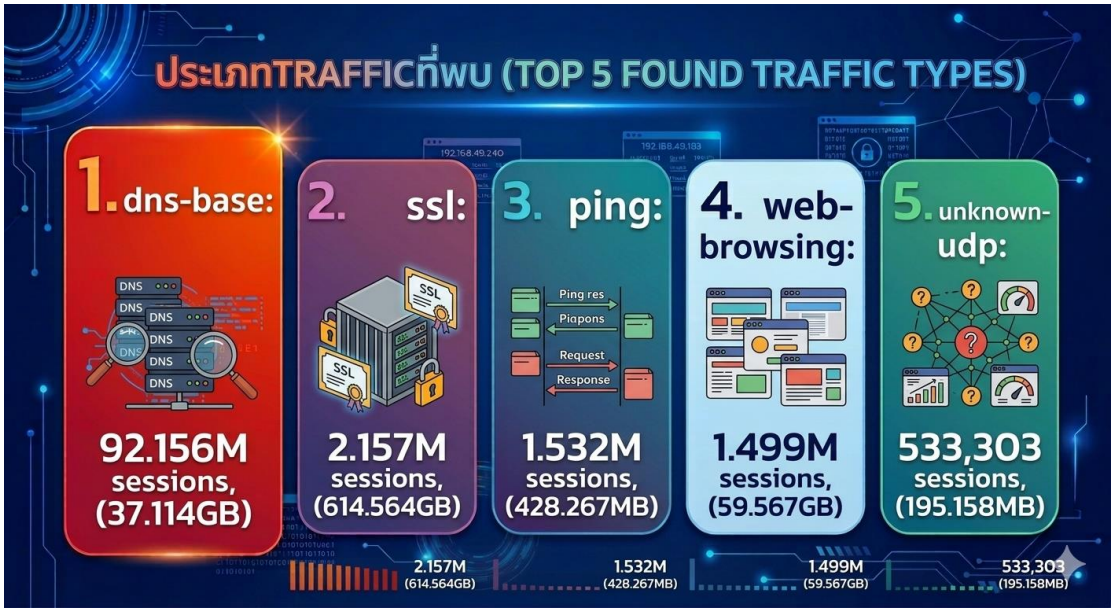
4.5.1 การวิเคราะห์พฤติกรรมการใช้งานแอปพลิเคชันบนเครือข่าย (Network Application Traffic Analysis) ในเชิงวิชาการ เพื่อชี้ให้เห็นถึงลักษณะการใช้งานทรัพยากรและการสื่อสารข้อมูลภายในมหาวิทยาลัย สามารถเรียบเรียงได้ดังนี้

การสื่อสารพื้นฐานระดับโครงสร้าง (dns-base): 92.156 ล้าน Sessions การวิเคราะห์ แม้จะมีปริมาณข้อมูลเพียง 37.114 GB แต่จำนวนการเชื่อมต่อที่สูงถึง 92 ล้านครั้ง (มากกว่าอันดับอื่นหลายสิบเท่า) สะท้อนถึงการทำงานที่หนาแน่นของระบบชื่อโดเมน อย่างไรก็ตาม ตัวเลขที่สูงผิดปกติในระดับนี้สอดคล้องกับผลการวิเคราะห์ในหัวข้อ 4.1.1 ที่พบการโจมตีแบบ DNS ANY Queries ในปริมาณมหาศาล ซึ่งชี้ให้เห็นว่าทราฟฟิกส่วนใหญ่ในกลุ่มนี้ไม่ได้เกิดจากการใช้งานปกติ แต่เกิดจากกิจกรรมภัยคุกคามประเภท DoS

การรับส่งข้อมูลแบบเข้ารหัส (ssl): 614.564 GB การวิเคราะห์ แอปพลิเคชันในกลุ่ม SSL/TLS ครองปริมาณข้อมูล (Throughput) สูงที่สุดในเครือข่าย เนื่องจากแอปพลิเคชันสมัยใหม่ เช่น Google Services, Facebook, และระบบการเรียนออนไลน์ส่วนใหญ่ใช้การเข้ารหัสข้อมูล ข้อมูลนี้ชี้ให้เห็นความท้าทายในการตรวจสอบภัยคุกคามที่แฝงมากับทราฟฟิกที่เข้ารหัส (Encrypted Threats) ซึ่งหากไม่มีการทำ SSL Decryption ระบบอาจมองไม่เห็นมัลแวร์ที่ซ่อนอยู่ภายใน

การใช้งานเว็บทั่วไป (web-browsing): 59.567 GB การวิเคราะห์ เป็นการใช้งานเว็บผ่านโปรโตคอล HTTP (พอร์ต 80) ที่ไม่ได้เข้ารหัส ซึ่งมีปริมาณรองลงมาสะท้อนถึงการเข้าถึงทรัพยากรสารสนเทศทั่วไปและการใช้งานระบบภายในมหาวิทยาลัยที่ยังไม่ได้ปรับเปลี่ยนเป็น HTTPS ทั้งหมด

การสื่อสารที่ไม่สามารถระบุประเภทได้ (unknown-udp): 533,303 Sessions การวิเคราะห์ ทราฟฟิกกลุ่ม Unknown-UDP ถือเป็นความเสี่ยงทางเทคนิค (Blind Spot) เนื่องจากระบบไม่สามารถระบุแอปพลิเคชันต้นทางได้ชัดเจน บ่อยครั้งทราฟฟิกประเภทนี้มักเกี่ยวข้องกับแอปพลิเคชันประเภท P2P, เกมออนไลน์ หรือร่องรอยการสื่อสารของมัลแวร์ที่พยายามหลบเลี่ยงการตรวจจับของ Firewall



4.5.2 หมวดหมู่แอปพลิเคชัน การวิเคราะห์โครงสร้างแอปพลิเคชันตามหมวดหมู่การใช้งาน (Application Category Distribution Analysis) จากการจัดกลุ่มแอปพลิเคชันตามหมวดหมู่หน้าที่การทำงาน (Category) พบว่าลักษณะทราฟฟิกในมหาวิทยาลัยราชภัฏชัยภูมิมีการกระจายตัวที่สะท้อนถึงทั้งพฤติกรรมการใช้งานปกติและสถานะความปลอดภัยของเครือข่าย โดยมีรายละเอียดวิเคราะห์เชิงเทคนิคดังนี้

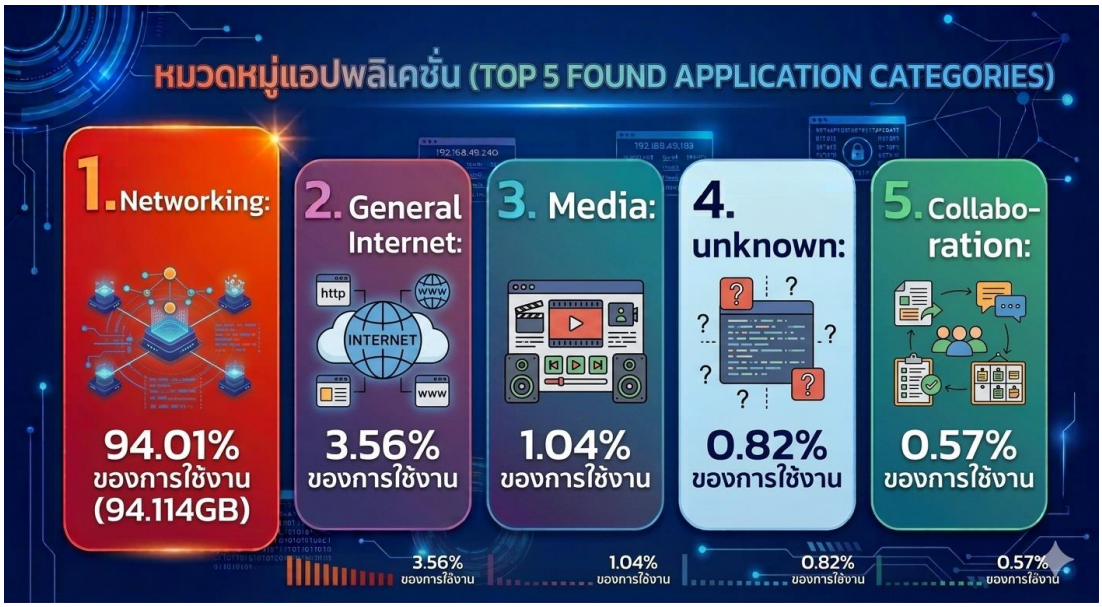
หมวดหมู่การสื่อสารระดับโครงสร้างเครือข่าย (Networking): ร้อยละ 94.01 การวิเคราะห์ สัดส่วนที่สูงเกินกว่าปกติในหมวดหมู่นี้ (ซึ่งโดยทั่วไปควรอยู่ที่ประมาณร้อยละ 40-60) เกิดจากการรวมกลุ่มของโปรโตคอลพื้นฐาน เช่น DNS, ICMP (ping) และการบริหารจัดการเครือข่ายอื่น ๆ อย่างไรก็ตาม เมื่อพิจารณาร่วมกับสถิติภัยคุกคามในหัวข้อ 4.1.1 ตัวเลขร้อยละ 94.01 นี้เป็นดัชนีชี้วัดที่สำคัญว่า เครือข่ายกำลังเผชิญกับทราฟฟิกที่ผิดปกติในระดับโครงสร้าง (Infrastructure Level Attack) มากกว่าการใช้งานแอปพลิเคชันของผู้ใช้ทั่วไป

หมวดหมู่การใช้งานอินเทอร์เน็ตทั่วไป (General Internet): ร้อยละ 3.56 การวิเคราะห์ ครอบคลุมการเข้าถึงเว็บไซต์ผ่าน HTTP/HTTPS (Web Browsing) และการใช้งานบริการคลาวด์พื้นฐาน ตัวเลขที่ค่อนข้างต่ำนี้แสดงให้เห็นว่าปริมาณทราฟฟิกที่เป็นการใช้งานของมนุษย์ (Human-generated Traffic) ถูกบดบังด้วยปริมาณทราฟฟิกที่เกิดจากเครื่องมืออัตโนมัติหรือภัยคุกคาม (Machine-generated Traffic)

หมวดหมู่สื่อและมัลติมีเดีย (Media): ร้อยละ 1.04 การวิเคราะห์ รวมถึงการสตรีมมิ่งวิดีโอ การฟังเพลงออนไลน์ และบริการถ่ายทอดสด ซึ่งมักจะเป็นกลุ่มที่ใช้แบนด์วิดท์ (Bandwidth) สูงที่สุด แต่ในเชิงจำนวนการเชื่อมต่อกลับมีสัดส่วนน้อย

หมวดหมู่แอปพลิเคชันที่ไม่สามารถระบุได้ (Unknown): ร้อยละ 0.82 การวิเคราะห์ แม้จะมีสัดส่วนไม่ถึงร้อยละ 1 แต่ในทางวิชาการถือเป็นกลุ่มที่ต้องเฝ้าระวังสูงสุด (High Suspicion) เนื่องจากอาจเป็นแอปพลิเคชันเฉพาะทางที่ผู้โจมตีเขียนขึ้นเอง (Custom Malware) หรือเป็นโปรโตคอลการเข้ารหัสแบบ Custom ที่พยายามหลบเลี่ยงการตรวจสอบของระบบรักษาความปลอดภัย

หมวดหมู่การทำงานร่วมกัน (Collaboration): ร้อยละ 0.57 การวิเคราะห์ครอบคลุมเครื่องมือสื่อสารภายในองค์กร เช่น Microsoft Teams, Zoom หรืออีเมล สะท้อนถึงพฤติกรรมการสื่อสารและการประสานงานผ่านระบบดิจิทัลภายในมหาวิทยาลัย



4.6 การวิเคราะห์ URL Category Filtering

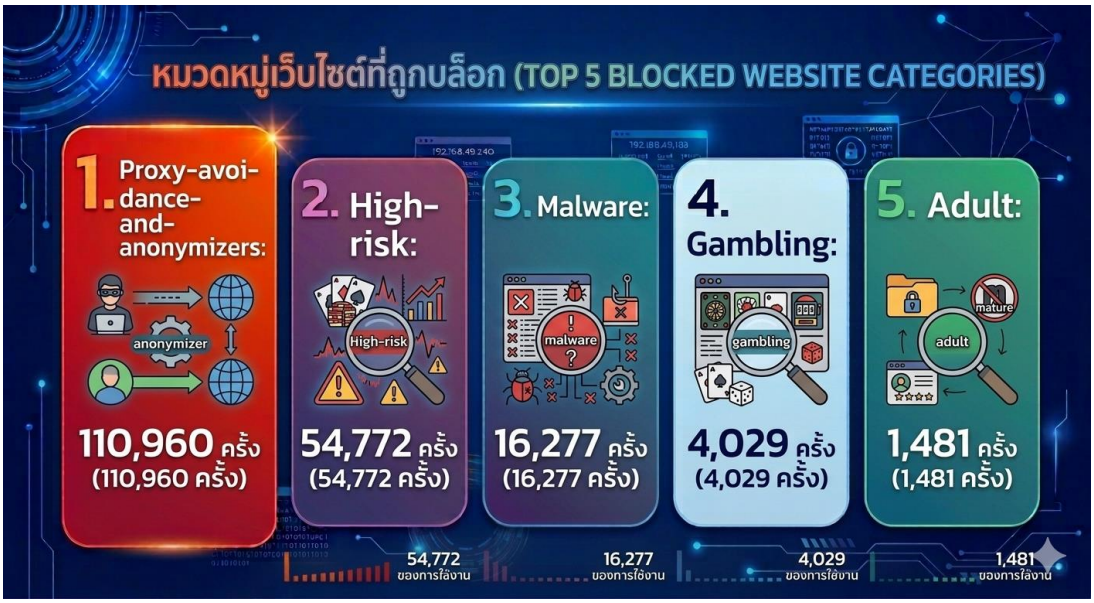
4.6.1 การวิเคราะห์การปิดกั้นการเข้าถึงเว็บไซต์ตามหมวดหมู่ความเสี่ยง

กลุ่มเครื่องมือหลบเลี่ยงการตรวจสอบ (Proxy-avoidance-and-anonymizers): 110,960 ครั้ง การวิเคราะห์ สถิติที่สูงที่สุดในกลุ่มนี้สะท้อนถึงพฤติกรรมของผู้ใช้งาน (นักศึกษาหรือบุคลากร) ที่พยายามใช้เครื่องมือ เช่น VPN ฟรี, Web Proxy หรือ Tor Browser เพื่อหลบเลี่ยงตัวกรองความปลอดภัยของมหาวิทยาลัย ในทางวิชาการ พฤติกรรมนี้ถือเป็น "ความเสี่ยงระดับสูง" เนื่องจากเป็นการเปิดช่องทางให้นำมัลแวร์เข้ามาสู่เครือข่ายภายในโดยที่ Firewall ไม่สามารถตรวจสอบทราฟฟิกที่ถูกเข้ารหัสผ่าน Proxy เหล่านั้นได้

กลุ่มเว็บไซต์ความเสี่ยงสูง (High-risk): 54,772 ครั้ง การวิเคราะห์ หมวดหมู่นี้รวมเว็บไซต์ที่มีประวัติพฤติกรรมน่าสงสัย (Suspicious Domains) หรือเว็บไซต์ที่เพิ่งจดทะเบียนใหม่ซึ่งมักใช้ในการโจมตีแบบ Phishing การเข้าถึงในปริมาณที่สูงบ่งชี้ว่าผู้ใช้งานมีความเสี่ยงที่จะตกเป็นเหยื่อของการหลอกลวงทางดิจิทัล

กลุ่มเว็บไซต์แพร่กระจายมัลแวร์ (Malware): 16,277 ครั้ง การวิเคราะห์ เป็นเว็บไซต์ที่ถูกยืนยันแล้วว่าเป็นแหล่งแพร่กระจายไวรัส เวิร์ม หรือมัลแวร์เรียกค่าไถ่ (Ransomware) การที่ระบบตรวจพบและปิดกั้นได้กว่า 1.6 หมื่นครั้ง ช่วยป้องกันความเสียหายเชิงโครงสร้างที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ของมหาวิทยาลัยได้โดยตรง

กลุ่มการพนันและเนื้อหาสำหรับผู้ใหญ่ (Gambling and Adult): รวม 5,510 ครั้ง การวิเคราะห์ แม้จะมีสัดส่วนน้อยกว่ากลุ่มความเสี่ยงทางเทคนิค แต่การเข้าถึงเว็บไซต์กลุ่มนี้ขัดต่อระเบียบการใช้งานเครือข่ายคอมพิวเตอร์ของสถานศึกษา และเว็บไซต์เหล่านี้มักเป็นแหล่งแฝงตัวของโฆษณาที่เป็นอันตราย (Malvertising)



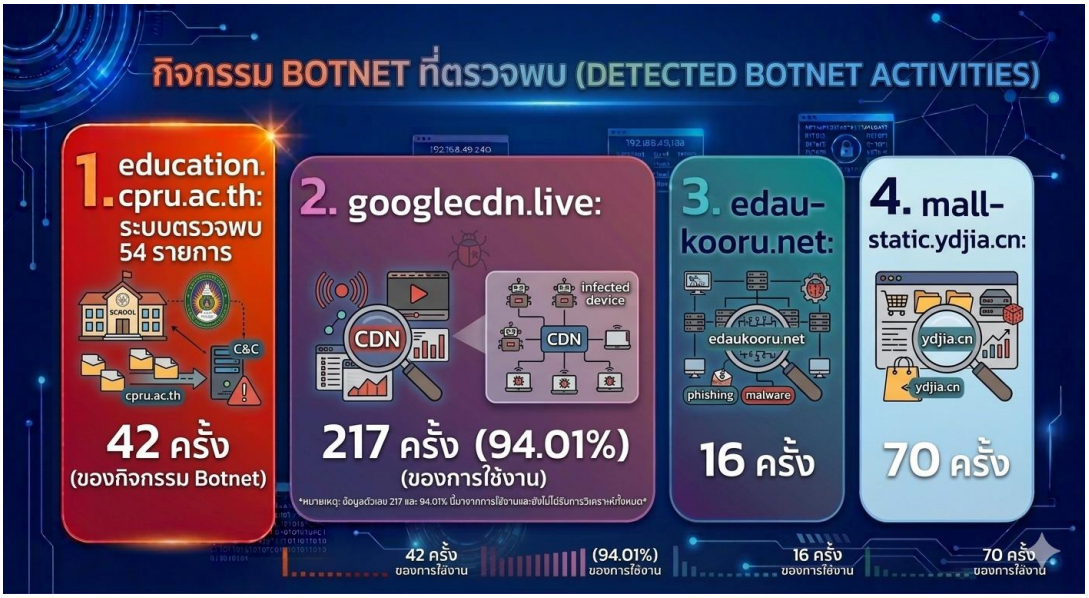
4.7 การวิเคราะห์ Botnet Activities

จากการตรวจสอบผ่านฐานข้อมูล Threat Intelligence ของ Palo Alto NGFW พบหลักฐานการสื่อสารที่เข้าข่ายกิจกรรมของบอทเน็ต (Botnet) จำนวน 54 รายการ ซึ่งในทางเทคนิคหมายถึงการที่เครื่องคอมพิวเตอร์ภายในมหาวิทยาลัยอาจถูกติดตั้งมัลแวร์และกำลังพยายามติดต่อกลับไปยังเครื่องแม่ข่ายสั่งการ (Command and Control Server) ของผู้โจมตี โดยโดเมนที่ตรวจพบการเชื่อมต่อสูงสุดมีนัยสำคัญดังนี้

mall-static.ydjia.cn (70 ครั้ง): โดเมนจากต่างประเทศที่มีพฤติกรรมน่าสงสัยในการรับ-ส่งชุดคำสั่งที่ไม่ได้มาตรฐาน มักเกี่ยวข้องกับการฝังตัวของ Adware หรือ Spyware ระดับสูงเพื่อส่งข้อมูลพฤติกรรมผู้ใช้ออกไปภายนอก

education.cpru.ac.th (42 ครั้ง): เป็นประเด็นที่น่าสนใจทางวิชาการ เนื่องจากเป็นโดเมนภายใต้มหาวิทยาลัย (cpru.ac.th) แต่ถูกระบบตรวจพบว่าเป็นกิจกรรมบอทเน็ต ชี้ให้เห็นว่าอาจมีเซิร์ฟเวอร์หรือหน้าเว็บไซต์บางส่วนของมหาวิทยาลัยถูกเจาะระบบ (Compromised) และถูกใช้เป็นฐานในการกระจายมัลแวร์ (Malware Distribution Point) หรือเป็นจุดพักข้อมูลของผู้โจมตี

googlecdn.live และ edaukooru.net (รวม 37 ครั้ง): เป็นโดเมนประเภท Malicious Domain ที่ตั้งชื่อให้คล้ายกับบริการที่น่าเชื่อถือ (Typosquatting/Mimicking) เพื่อพรางตัวจากการตรวจสอบของระบบรักษาความปลอดภัย โดยมักใช้ในการรับคำสั่งเพื่อทำกิจกรรมที่เป็นอันตราย เช่น การดึงข้อมูลออกนอกองค์กร หรือเตรียมการโจมตีแบบ DDoS


กิจกรรม BOTNET ที่ตรวจพบ (DETECTED BOTNET ACTIVITIES)
1. education.cpru.ac.th:
ระบบตรวจพบ 54 รายการ
SCHOOL
C&C
cpru.ac.th
42 ครั้ง
(ของกิจกรรม Botnet)
2. googlecdn.live:
CDN
infected device
CDN
217 ครั้ง (94.01%)
(ของการใช้งาน)
หมายเหตุ: ข้อมูลตัวเลข 217 และ 94.01% นี้มาจากการใช้งานและยังไม่ได้รับการวิเคราะห์ทั้งหมด
3. edau-kooru.net:
edaukooru.net
phishing
malware
16 ครั้ง
4. mall-static.ydjia.cn:
ydjia.cn
ydjia.cn
70 ครั้ง
42 ครั้ง ของการใช้งาน
(94.01%) ของการใช้งาน
16 ครั้ง ของการใช้งาน
70 ครั้ง ของการใช้งาน

บทที่ 5
สรุปและข้อเสนอแนะ

5.1 สรุปผลการวิเคราะห์

จากการตรวจสอบผ่านฐานข้อมูล ของ Palo Alto NGFW พบหลักฐานการสื่อสารที่เข้าข่ายกิจกรรมของบอทเน็ต (Botnet) จำนวน 54 รายการ ซึ่งในทางเทคนิคหมายถึงการที่เครื่องคอมพิวเตอร์ภายในมหาวิทยาลัยอาจถูกติดตั้งมัลแวร์และกำลังพยายามติดต่อกลับไปยังเครื่องแม่ข่ายสั่งการ (Command and Control Server) ของผู้โจมตี โดยโดเมนที่ตรวจพบการเชื่อมต่อสูงสุดมีนัยสำคัญดังนี้

5.1.1 รูปแบบและพฤติกรรมการโจมตีหลัก

ผลการศึกษาพบว่าสถาปัตยกรรมเครือข่ายของมหาวิทยาลัยราชภัฏชัยภูมิเผชิญกับภัยคุกคามประเภท Brute Force เป็นหลัก โดยเฉพาะอย่างยิ่งการโจมตีแบบ DNS ANY Queries (63%) ซึ่งในเชิงวิชาการถือเป็นการทำ DNS Amplification Attack เพื่อขัดขวางการให้บริการ (Denial of Service) สิ่งนี้สะท้อนให้เห็นว่าผู้โจมตีมุ่งเน้นการใช้ทรัพยากรระดับโครงสร้างพื้นฐาน (Infrastructure Level) ของมหาวิทยาลัยเป็นเป้าหมายและเป็นเครื่องมือในการขยายผลการโจมตี ซึ่งอาจส่งผลกระทบต่อเสถียรภาพของระบบสารสนเทศในภาพรวม

5.1.2 ภูมิศาสตร์ไซเบอร์และแหล่งกำเนิดภัยคุกคาม

แหล่งที่มาของการโจมตีมีความหนาแน่นในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยมี ประเทศไทย (21.4%) และอินโดนีเซีย (19.6%) เป็นอันดับต้นๆ ข้อสรุปนี้ชี้ให้เห็นว่าภัยคุกคามส่วนใหญ่เกิดจากเครือข่ายบอทเน็ต (Botnet) ที่ฝังตัวอยู่ในอุปกรณ์ที่ขาดการรักษาความปลอดภัยภายในภูมิภาค ซึ่งสอดคล้องกับพฤติกรรมการโจมตีแบบอัตโนมัติที่ตรวจพบในปริมาณมหาศาล

5.1.3 ประสิทธิภาพการบริหารจัดการความปลอดภัย (Security Effectiveness)

ในภาพรวม อุปกรณ์ Palo Alto PA-1410 แสดงให้เห็นถึงประสิทธิภาพเชิงรุก (Proactive Defense) โดยสามารถสกัดกั้นการเข้าถึงเว็บไซต์ที่มีความเสี่ยงสูงได้กว่า 187,700 ครั้ง และตรวจพบการสื่อสารของ Spyware/Malware กว่า 17,600 รายการ ซึ่งช่วยลดความเสี่ยงในการสูญเสียข้อมูลสำคัญและยับยั้งการแพร่ระบาดของมัลแวร์ภายในเครือข่ายได้อย่างมีนัยสำคัญ

5.2 ข้อเสนอแนะเชิงนโยบายและมาตรการป้องกัน

ผู้ศึกษาเสนอแนะแนวทางการดำเนินงานโดยแบ่งตามลำดับความสำคัญและระยะเวลา ดังนี้

5.2.1 มาตรการเร่งด่วนระยะสั้น (1-3 เดือน): การเสริมสร้างปราการด่านแรก

Hardening DNS Infrastructure: ควรเร่งกำหนดค่า Rate Limiting เพื่อจำกัดจำนวน Query ต่อวินาที และพิจารณาใช้เทคโนโลยี DNS over HTTPS (DoH) เพื่อป้องกันการดักจับหรือเปลี่ยนแปลงข้อมูลชื่อโดเมน

Dynamic Firewall Policy: ปรับเปลี่ยนนโยบายจาก Static Rules เป็น Dynamic โดยใช้ระบบ Automated IP Blacklisting และการบล็อก SSH Brute Force แบบอัตโนมัติ (Threshold-based Drop) เพื่อลดภาระการทำงานของเจ้าหน้าที่

End-point & User Sanitization: ดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้กลุ่มเสี่ยงสูง (Risky Users) 50 ลำดับแรกทันที เพื่อกำจัดมัลแวร์ที่อาจฝังตัวอยู่ และจัดอบรม Cybersecurity Awareness เฉพาะจุด

5.2.2 มาตรการระยะกลาง (3-6 เดือน)

Threat Intelligence Integration: เชื่อมต่อระบบกับฐานข้อมูลภัยคุกคามระดับโลกแบบ Real-time เพื่อให้ Firewall สามารถจำแนก Indicators of Compromise (IoC) ใหม่ๆ ได้ทันที

Network Segmentation & Zero Trust: เริ่มต้นการแบ่งส่วนเครือข่าย (Segmentation) โดยแยก Server Zone (DMZ) ออกจาก User Zone อย่างเด็ดขาด และเริ่มนำแนวคิด Zero Trust Architecture มาใช้ในการตรวจสอบสิทธิ์ทุกการเชื่อมต่อ

Centralized Log Management: ติดตั้งระบบ SIEM เพื่อรวบรวม Log จากหลายแหล่งมาวิเคราะห์ความสัมพันธ์ (Correlation) และจัดตั้งทีม SOC (Security Operations Center) เบื้องต้นเพื่อเฝ้าระวังเหตุการณ์ผิดปกติ

5.2.3 มาตรการระยะยาว (6-12 เดือน)

Human Capital Development: พัฒนาทักษะบุคลากรไอทีให้เป็นทีม Incident Response (IR) ที่มีความเชี่ยวชาญในการเผชิญเหตุและกู้คืนระบบตามมาตรฐานสากล

Infrastructure Resiliency: ยกระดับความพร้อมใช้งานด้วยระบบ High Availability (HA) สำหรับ Firewall และจัดทำแผน Disaster Recovery (DR) พร้อมระบบสำรองข้อมูลที่แยกส่วนจากเครือข่ายหลัก (Offline Backup)

Standard & Compliance: มุ่งสู่การรับรองมาตรฐาน ISO 27001 หรือมาตรฐานความปลอดภัยสารสนเทศสำหรับสถาบันการศึกษา เพื่อสร้างกระบวนการตรวจสอบ (Audit Trail) ที่โปร่งใสและน่าเชื่อถือในระดับสากล


กลยุทธ์รักษาความปลอดภัยไซเบอร์มหาวิทยาลัย
UNIVERSITY CYBERSECURITY STRATEGY
1 Short-term
2 Medium-term
3 Long-term
Quick Fixes
แก้ไขเร่งด่วน
Quick Fixes to enderse Cybersecurity strategying mitigation and probentivafe homs of quick-win metrics.
High-Risk:
(PROXY & ANONYMIZERS)
Patching:
(SYSTEM UPDATES)
CDN
42 กิจกรรม
BOTNET
(42 Botnet activities)
Intelligence & Segmentation
ข่าวกรอง & การแบ่งส่วน
Intelligence & Segmentation
Rapiectsndte &-menofatora with Intelligence & traffic inspection and war inspection.
Compliance:
(ISO 27001)
Cyber Incident Response:
(PREPAREDNESS DRILLS)
phishing
malware
Security Information & Event Management (SIEM):
(ANOMALY DETECTION)
Standards & Resilience
มาตรฐาน & ความยืดหยุ่น
Standards & Resilience
Standard university, ssscure secure university remotions and torm protection.
42 ครั้ง
ของการป้องกัน
(94.01%)
ของการใช้งาน
16 ครั้ง
ของการใช้งาน
70 ครั้ง
ของการป้องกัน

บรรณานุกรม

พงศธร รัตนสุวรรณ. (2568). การพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับมหาวิทยาลัยไทยตามแนวคิด Zero Trust. วารสารเทคโนโลยีสารสนเทศและการจัดการความรู้, 10(3), 88–105.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกช.). (2567). แนวทางปฏิบัติในการป้องกันการโจมตีทางไซเบอร์สำหรับหน่วยงานภาครัฐ. https://www.ncsa.or.th/guidelines-2024/

Bertino, E., & Islam, N. (2023). Botnets and DNS amplification attacks: A survey of detection and mitigation techniques. IEEE Communications Surveys & Tutorials, 25(1), 112–135. https://doi.org/10.1109/COMST.2023.

Check Point Research. (2025). Cyber attack trends: 2025 mid-year report. https://research.checkpoint.com/reports/cyber-attack-trends-2025/

Palo Alto Networks. (2025). Unit 42 network threat intelligence report: Volume 17. https://unit42.paloaltonetworks.com/threat-intelligence-report/

Palo Alto Networks. (2023). Next-Generation Firewall (NGFW) Administrator’s Guide: PAN-OS 11.0. Palo Alto Networks TechDocs.

Stallings, W. (2022). Computer security: Principles and practice (5th ed.). Pearson.

Zhang, L., & Gao, X. (2024). Analyzing brute force attacks in campus networks: Patterns and defense strategies. Journal of Cybersecurity and Information Management, 12(2), 45–58.