การออกแบบและพัฒนาเพื่อเพิ่มประสิทธิภาพการคัดแยกการปลอมแปลงอีเมลสำหรับอุปกรณ์อีเมลซีเคียวริตี้เกตเวย์

DESIGN AND IMPLEMENTATION OF SPOOFING EMAIL DETECTION FOR EMAIL SECURITY GATEWAY

วรวุฒิ จำปาหอม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ปีการศึกษา 2566

การออกแบบและพัฒนาเพื่อเพิ่มประสิทธิภาพการคัดแยกการปลอมแปลงอีเมลสำหรับอุปกรณ์อีเมลซีเคียวริตี้เกตเวย์

วรวุฒิ จำปาหอม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ปีการศึกษา 2566

หัวข้อวิทยานิพนธ์	การออกแบบและพัฒนาเพื่อเพิ่มประสิทธิภาพการคัดแยกการปลอมแปลงอีเมลสำหรับอุปกรณ์อีเมลซีเคียวริตี้เกตเวย์ Design and Implementation of Spoofing Email Detection for Email Security Gateway
ชื่อ – นามสกุล	นายวรวุฒิ จำปาหอม
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษา	รองศาสตราจารย์พฤศยน นินทนาวงศา, Ph.D.
ปีการศึกษา	2566

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ณฐภัทร พันธ์คง, Ph.D.)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์วันวิสา ชัชวงษ์, วศ.ด.)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ศีลวัต ร่มโพธิ์ชัย, วศ.ด.)

..... กรรมการ
(รองศาสตราจารย์พฤศยน นินทนาวงศา, Ph.D.)

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี อนุมัติวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์สรพงษ์ ภวสุปรีย์, Ph.D.)
วันที่.....เดือน.....พ.ศ.....

หัวข้อวิทยานิพนธ์	การออกแบบและพัฒนาเพื่อเพิ่มประสิทธิภาพการคัดแยกการปลอมแปลงอีเมลสำหรับอุปกรณ์อีเมลซีเคียวริตี้เกตเวย์
ชื่อ – นามสกุล	นายวรวุฒิ จำปาหอม
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษา	รองศาสตราจารย์พฤศยน นินทนาวงศา, Ph.D.
ปีการศึกษา	2566

บทคัดย่อ

อีเมลถือว่าเป็นวิธีการสื่อสารหลักในปัจจุบันเนื่องจากมีต้นทุนการดำเนินการที่ต่ำและไม่จำเป็นต้องเดินทางไปพบหน้ากันเพื่อแลกเปลี่ยนหรือส่งข้อมูลต่างๆ อย่างไรก็ตามในยุคแรกที่มีการสร้างระบบอีเมลขึ้นมานั้น ยังไม่ได้คำนึงถึงเรื่องความปลอดภัยในการปลอมแปลงอีเมลมากนัก จึงทำให้มีผู้ไม่หวังดีใช้ช่องโหว่ของระบบอีเมลนี้มาทำการโจมตีผู้ใช้งาน ซึ่งการโจมตีที่มักจะใช้ได้ผลดี คือการปลอมแปลงอีเมล หรือที่เรียกว่าอีเมล Spoofing ซึ่งเป็นการโจมตีที่จะหลอกผู้ใช้งานโดยจะทำให้พวกเขาเชื่อว่าอีเมลถูกส่งจากผู้ส่งที่น่าเชื่อถือ และการโจมตีในลักษณะนี้กำลังเพิ่มขึ้นอย่างมาก

ในงานวิจัยฉบับนี้เราได้นำเสนอวิธีการตรวจจับอีเมลหลอกลวงดังกล่าว โดยการเขียนโปรแกรมคอมพิวเตอร์ขนาดเล็กหรือที่เรียกว่าสคริปต์ ซึ่งได้รับการพัฒนาขึ้นมาเพื่อตรวจสอบว่าอีเมลขาเข้าถูกส่งโดยผู้ส่งที่น่าเชื่อถือหรือไม่ การติดตามผลหลังจากติดตั้งสคริปต์ดังกล่าวนี้บนอุปกรณ์ป้องกันการรับ-ส่งอีเมลหรือที่เรียกว่าอีเมล Security Gateway ใช้ระยะเวลาทิ้งสิ้นหกเดือน

เมื่อตรวจสอบผลของการคัดแยกอีเมลที่ไม่ปลอดภัยบนอีเมล Security Gateway จะพบอีเมลที่ไม่ปลอดภัย 30,633,332 ฉบับ จากอีเมลทั้งหมด 33,106,281 ฉบับ ซึ่งคิดเป็น 92.53% ซึ่งยังไม่รวมประเภทที่เป็นอีเมลปลอม หรือ Spoofing อีเมลที่อุปกรณ์นี้ยังไม่สามารถคัดแยกได้ เมื่อติดตั้งสคริปต์ตรวจจับอีเมลปลอมนี้เข้าไปที่อุปกรณ์และติดตามผลพบว่าสามารถคัดแยกอีเมลปลอมได้ 28,612 ฉบับ จากอีเมลที่ปลอดภัย 2,472,949 ฉบับ ซึ่งคิดเป็น 1.16% สุดท้ายนี้สคริปต์ที่ถูกพัฒนาขึ้นมานี้สามารถคัดแยก Spoofing อีเมลได้ 100% และอีเมลปลอมทั้งหมดจะถูกส่งไปยังที่กักกันโดยจะไม่ถูกส่งต่อไปยังผู้ใช้งาน ทำให้ลดโอกาสเสี่ยงที่ผู้ใช้งานจะได้รับอีเมลเหล่านี้และตกเป็นเหยื่อของผู้ไม่หวังดี

คำสำคัญ : อีเมล การปลอมแปลง การรักษาความปลอดภัย ทางเข้าออก

Thesis Title	Design and Implementation of Spoofing Email Detection for Email Security Gateway
Name – Surname	Mr. Worawoot Jampahom
Program	Electronics Engineering
Thesis Advisor	Associate Professor Prusayon Nintanavongsa, Ph.D.
Academic Year	2023

ABSTRACT

Email is undoubtedly the primary means of communication in the present time due to its low cost of operation and non-confrontational nature for receiving information. However, email spoofing, a type of attack on users that makes them believe an email is sent from a trustworthy sender, is growing exponentially.

In this study, a method was proposed to detect such spoof emails. A computer programming script had been developed to verify whether incoming emails were sent by trustworthy senders. This monitoring method was installed on the email security gateway, and it had been implemented for a period of six months.

The method intercepted 30,633,332 unsafe emails out of a total of 33,106,281 emails, which was 92.53 percent. Moreover, this method was capable of quarantining 28,612 spoofed emails out of 2,472,949 safe emails, which was 1.16 percent. Lastly, the method boasts a 100% email spoofing detection rate, and all spoofed emails destined for the organization were diverted to quarantine center. This could reduce the chance of receiving risky emails and preventing users from being victims to spammers.

Keyword: email, spoofing, security, gateway

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงตามวัตถุประสงค์ได้ด้วยความอนุเคราะห์ของรองศาสตราจารย์ พฤศยน นินทนาวงศา ที่เสียสละเวลาให้คำปรึกษาแนะนำและชี้แนะแนวทางในการปรับปรุงข้อบกพร่องจนสำเร็จลุล่วงด้วยดี ผู้วิจัยขอขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ อาจารย์นิสิต ภูครองตา คณะวิศวกรรมศาสตร์ ที่ให้คำแนะนำในการแก้ไขข้อบกพร่องของวิทยานิพนธ์

ขอขอบพระคุณบิดา มารดา ครอบครัว ญาติพี่น้อง เพื่อนพ้องและคณะครู-อาจารย์ ที่เป็นกำลังใจและให้การสนับสนุน รวมทั้งประสิทธิ์ประสาทวิชาความรู้แก่ผู้วิจัย

สุดท้ายนี้ ผู้วิจัยหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์นี้จะเป็นประโยชน์สำหรับผู้ที่สนใจ หากมีข้อบกพร่องประการใด ผู้วิจัยต้องขออภัยมา ณ โอกาสนี้ด้วย

วรวุฒิ จำปาหอม

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูป

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

ระบบอีเมลถูกสร้างในปีราว 1960 เพื่อประโยชน์ด้านความสะดวกและรวดเร็วในการสื่อสาร โดยใช้ข้อความผ่านระบบอิเล็กทรอนิกส์ ระบบอีเมลนี้ถูกพัฒนามาจนถึงยุคปัจจุบันรวมเป็นเวลากว่า 50 ปี ในยุคปัจจุบันระบบอีเมลสามารถสื่อสารผ่านระบบอินเตอร์เน็ต โดยใช้ Protocol: http, https, smtp ซึ่งมีช่องโหว่เกิดขึ้นมากมาย เพราะในตอนแรกโครงสร้างพื้นฐานของระบบอีเมลไม่ได้ถูกออกแบบมาให้มีความปลอดภัยขั้นสูง แต่ออกแบบมาเพื่อความสะดวกต่อการใช้งานเป็นหลัก จึงทำให้การส่งข้อมูลผ่านช่องทางอีเมลเป็นภัยคุกคามอันดับหนึ่งในการสร้างความเสียหายให้กับเหยื่อ การส่งอีเมลจากที่หนึ่งไปยังที่หนึ่งเกิดขึ้นทุกวันเป็นจำนวนวันละหลายพันล้านฉบับ [1] ข้อมูลจากปี 2022 มีการรับ-ส่งอีเมลมากกว่า 300 ล้านฉบับต่อวัน [2] การโจมตีทางด้านอีเมลจึงเป็นวิธีการที่สำคัญที่ Attacker ใช้ในการโจมตีผู้ใช้งาน เนื่องจากเป็นวิธีการโจมตีที่ง่ายแต่สามารถส่งผลกระทบกับเหยื่อได้อย่างมาก ไม่ว่าจะเป็นความเสียหายต่อส่วนบุคคล หรือต่อทั้งองค์กร อ้างอิงจากเว็บไซต์ BBC แม้กระทั่งบริษัทที่ดำเนินธุรกิจเกี่ยวกับด้านเทคโนโลยี อย่างเช่น Google, Facebook ก็ยังถูกโจมตีด้วยอีเมลเช่นกันเดียวกัน

ภัยคุกคามทางด้านอีเมลที่มีนัยยะสำคัญแบ่งเป็นประเภท 3 ประเภท คือ 1. Phishing Email 2. Business Email Compromise 3. Email Spoof Attack โดยผู้ไม่หวังดีจะใช้ระบบการโจมตีอัตโนมัติหรือที่เรียกว่า Dynamic Threat เช่น มีการฝังระบบ Virus ไว้ในไฟล์เอกสารแนบของอีเมลที่มีการ Setup Macro ไว้ภายในไฟล์ เมื่อผู้ใช้งานทำการเปิดไฟล์เอกสาร ก็จะทำให้ Virus สามารถเข้ามาติดตั้งที่เครื่องของผู้ใช้งานได้โดยง่ายดาย และผู้ไม่หวังดีจะทำการขโมย Credential ของเหยื่อเพื่อทำการเรียกค่าไถ่(Ransome) หรือสร้างความเสียหายให้กับธุรกิจของเหยื่อเพื่อนำไปรับเงินจากธุรกิจคู่แข่งเหยื่อที่ได้รับความเสียหาย มีตั้งแต่องค์กรที่เป็นธนาคาร องค์กรของรัฐบาล บริษัทเอกชน หรือแม้แต่สถานศึกษาเองก็ยังถูกผู้ไม่หวังดีโจมตีทางด้านอีเมลเช่นเดียวกัน

เทคโนโลยีที่เกี่ยวข้องกับความปลอดภัยทางด้านอีเมล จึงถูกสร้างขึ้นเพื่อใช้ในการป้องกันการโจมตีทางอีเมลผ่านทาง SMTP Server และ Email Gateway จากข้อมูลพบว่าผู้โจมตีมีหลากหลายมากขึ้น มาจากหลากหลายประเทศ ซึ่งหนึ่งในการโจมตีที่ผู้ไม่หวังดีนิยมใช้ คือ Email Spoof Attack หรือเรียกอีเมลประเภทนี้ว่า Spoofing Email โดยจะทำให้ผู้รับอีเมลหลงเชื่อว่าเป็นอีเมลจากผู้ส่งตัวจริงแล้วแฝง Link หรือ เอกสารแนบที่มี Virus เมื่อผู้รับ Click ที่ Link หรือเปิดไฟล์แนบก็จะทำให้เครื่องคอมพิวเตอร์ติด Virus ได้ในทันที [3] ซึ่งการโจมตีประเภทนี้จะตรวจสอบได้ยากและอุปกรณ์

Email Security Gateway ในยุคปัจจุบันยังไม่มีความสามารถในการคัดแยกการโจมตีประเภทนี้เลย

จากช่องโหว่ของอุปกรณ์ Email Security Gateway ในปัจจุบันที่ยังไม่สามารถคัดแยกอีเมลที่เป็นประเภท Spoofing Email ได้ งานวิจัยฉบับนี้จึงได้ทำการศึกษาและพัฒนา Script เพื่อให้ Email Security Gateway สามารถคัดแยกอีเมลประเภทนี้ได้ โดยจะทำการศึกษาการใช้งานอีเมลขององค์กรแห่งหนึ่งภายใต้สังกัดการบริหารงานของรัฐบาลในประเทศไทย ซึ่งยังใช้ระบบการรับส่งอีเมลเป็นแบบ On Premise หรือ Legacy มีการรับส่งอีเมลมากกว่า 100,000-500,000 ฉบับต่อวัน และมีผู้ใช้งานมากกว่า 10,000 User ซึ่งทางผู้ดูแลระบบได้ตรวจสอบพบว่าผู้ใช้งานได้รับอีเมลที่เป็นประเภท Spoofing Email เป็นจำนวนมาก และสร้างผลกระทบกับผู้ใช้งานในบางหลายเนื่องจากเครื่องคอมพิวเตอร์ถูกติดตั้ง Virus ซึ่งแฝงมากับเอกสารแนบในอีเมลทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ได้ในทุก Folder และติดตามการใช้งาน Internet รวมถึงได้รหัสผ่านในการเข้าทำธุระกรรมบน Website ต่างๆ อีกด้วย

1.2 วัตถุประสงค์การวิจัย

1.2.1 เพื่อศึกษาและวิเคราะห์รูปแบบการโจมตีทางด้านอีเมลในลักษณะของการทำ Email Spoof Attack

1.2.2 เพื่อศึกษาความสามารถของอุปกรณ์ Email Security Gateway ในยุคปัจจุบันกับการคัดแยกอีเมลที่เป็นประเภท Spoofing Email

1.2.3 พัฒนาและติดตั้ง Script เพื่อเพิ่มประสิทธิภาพของ Email Security Gateway ในการคัดอีเมลที่เป็นประเภท Spoofing Email

1.3 สมมุติฐานของงานวิจัย

งานวิจัยฉบับนี้เป็นการวิเคราะห์รูปแบบการโจมตีในลักษณะของการทำ Email Spoof Attack และทำการพัฒนา Script เพื่อนำไปติดตั้งบนอุปกรณ์ Email Security Gateway ให้สามารถคัดแยกอีเมลที่เป็น Spoofing Email ได้ เนื่องจากเดิมอุปกรณ์ Email Security Gateway ในยุคปัจจุบันยังไม่สามารถคัดแยกอีเมลประเภทนี้ได้ ทำให้เกิดความเสียหายต่อหลายๆ องค์กรทั่วโลก

1.4 ขอบเขตของการวิจัย

1.4.1 ศึกษาการใช้งานอีเมลขององค์กรแห่งหนึ่งภายใต้สังกัดการบริหารงานของรัฐบาลในประเทศไทย ซึ่งยังใช้ระบบการรับส่งอีเมลเป็นแบบ On Premise หรือ Legacy

1.4.2 ศึกษาการทำงานของการคัดแยกอีเมลที่ไม่ปลอดภัยของอุปกรณ์ Email Security Gateway ยี่ห้อ Cisco Email Security Gateway

1.4.3 ศึกษาลักษณะ Header ของอีเมลที่เป็นประเภท Spoofing Email

1.4.4 พัฒนาและทดสอบ Script ที่สามารถคัดแยกอีเมลที่เป็น Spoofing Email และนำไปติดตั้งบนอุปกรณ์ Email Security Gateway

1.5 ขั้นตอนการวิจัย

1.5.1 ศึกษาระบบการคัดแยกอีเมลบนอุปกรณ์ Email Security Gateway

1.5.2 ศึกษาและวิเคราะห์อีเมลที่มีลักษณะเป็น Spoofing Email ที่ทางผู้ใช้งานได้รับ

1.5.3 ศึกษาภาษาที่จะนำมาเขียน Script บนอุปกรณ์ Email Security Gateway

1.5.4 พัฒนาและทดสอบ Script บนอุปกรณ์ Email Security Gateway ใน Test Environment

1.5.5 ติดตั้ง Script ที่ผ่านการทดสอบบนอุปกรณ์ Email Security Gateway ขององค์กร

1.5.6 เก็บข้อมูลการคัดแยกอีเมลด้วย Script จากรายงานบนอุปกรณ์ Email Security Gateway

1.5.7 ติดตามผลการใช้งานอีเมลของผู้ใช้งานในองค์กร

1.5.8 สรุปและอภิปรายผลการติดตั้ง Script บนอุปกรณ์

1.5.9 เขียนวิทยานิพนธ์ฉบับสมบูรณ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทำให้เกิดความรู้เกี่ยวกับขั้นตอนทางเทคนิคในการรับ-ส่ง อีเมล

1.6.2 ทำให้เกิดความรู้เกี่ยวกับการทำงานของอุปกรณ์ Email Security Gateway ในการคัดแยกอีเมล

1.6.3 ทำให้เกิดความรู้เกี่ยวกับการทำงานของ Protocol ที่ใช้คัดแยก Spoofing Email

1.6.4 ทำให้เกิดความรู้เกี่ยวกับการเขียน Script บนอุปกรณ์ Email Security Gateway

1.6.5 ทำให้ทราบเกี่ยวกับพฤติกรรมของผู้ไม่หวังดีที่ใช้การโจมตีผ่านทางอีเมลและทำให้ตระหนักในการใช้งานอีเมลและ Internet

บทที่ 2
ทฤษฎีที่เกี่ยวข้องและงานวิจัยที่เกี่ยวข้อง

Spoofing Email เป็นปัญหาที่รุนแรงในโลกยุคปัจจุบันที่ใช้การส่งอีเมลเป็นหลักในการติดต่อเชิงธุรกิจ โดย Spoofing Email นี้มักถูกนำมาใช้เพื่อการฉ้อโกง การขโมยข้อมูล หรือการโจมตีระบบ โดยผู้ไม่หวังดีสามารถปลอมแปลงข้อมูลใน Header หรือใช้โปรแกรมปลอมแปลงอีเมล Address หรือ Domain ที่ใช้ในการส่งเพื่อสร้างความเชื่อมั่นให้กับผู้รับอีเมล เมื่อผู้รับเปิดอ่านอีเมล, Link แนบ หรือเอกสารแนบก็จะทำให้เสี่ยงต่อการโจมตีทาง Cyber หรือมีความเสี่ยงต่อความเสียหายในส่วนอื่นๆ อีกมากมาย

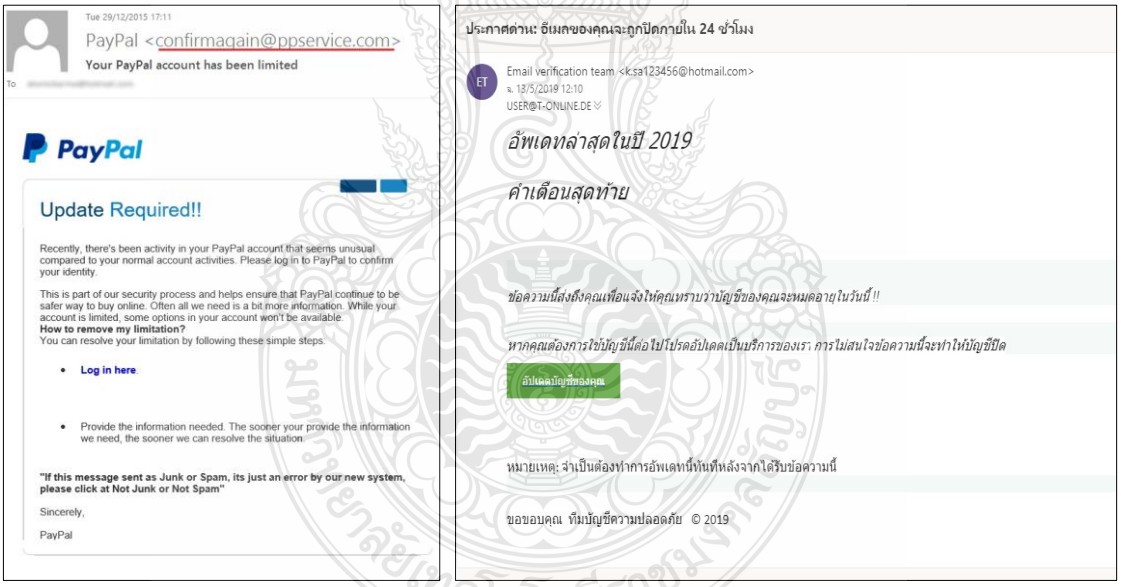
2.1 ประเภทของภัยคุกคามทางไซเบอร์ (Cyber Threats)

ภัยคุกคามทางไซเบอร์ (Cyber Threats) มีหลายประเภท แต่ละประเภทมีวิธีการ วัตถุประสงค์ และผลกระทบที่แตกต่างกัน ไม่ว่าจะเป็น 1) Malware ซอฟต์แวร์ที่มีจุดประสงค์ในการทำให้คอมพิวเตอร์หรือระบบไม่สามารถใช้งานได้หรือขโมยข้อมูลของเหยื่อ 2) Ransomware ชนิดของ Malware ที่จะเข้ารหัสข้อมูลแล้วขอค่าไถ่เพื่อปลดปล่อยข้อมูล 3) Man-in-the-Middle Attacks คือ ภัยคุกคามที่อยู่ระหว่างการส่งผ่านข้อมูลซึ่งจะทำการดักฟังหรือแก้ไขข้อมูลระหว่างทาง 4) Denial of Service (DoS) and Distributed Denial of Service (DDoS) เป็นการโจมตีเพื่อทำให้ระบบอินเทอร์เน็ตหรือแอพพลิเคชันไม่สามารถให้บริการได้ 5) Brute-force Attack การพยายามเข้าถึงระบบโดยการทดลองรหัสผ่านจนกว่าจะเจอ 6) SQL Injection คือ การโจมตีระบบ Database โดยการแทรกคำสั่ง SQL ผ่านช่องโหว่ที่อยู่ในแอพพลิเคชัน 7) Zero-day Attack การโจมตีที่เกิดขึ้นก่อนหรือในวันเดียวกันที่ค้นพบช่องโหว่ 8) Credential Reuse Attack การใช้รหัสผ่านหรือข้อมูลสิทธิ์จากระบบหนึ่งเพื่อเข้าถึงระบบอื่น 9) Social Engineering การใช้จิตวิทยาในการหลอกลวงหรือควบคุมผู้ใช้ให้เปิดเผยข้อมูลส่วนตัวหรือข้อมูลที่ครอบครองอยู่ 10) Phishing เป็นการส่งอีเมลหรือข้อความที่อาจดูเหมือนจะมาจากแหล่งที่เชื่อถือได้ แต่จริงๆ แล้วมีจุดประสงค์ในการหลอกให้ผู้รับเปิดไฟล์หรือลิงก์ที่อาจจะมี Malware มีเป้าหมายหลักคือการหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลส่วนตัวหรือข้อมูลความปลอดภัย ซึ่งรวมถึง username, password, หรือข้อมูลบัตรเครดิต [7] โดยวิธีการหลักของการทำ Phishing จะมีอยู่ 4 ประเภท 1) Email Phishing คือ การส่งอีเมลที่ออกแบบให้คล้ายกับอีเมลจากองค์กรหรือบริษัทที่ถูกต้อง แต่มักจะมีข้อความหรือลิงก์ที่เป็นอันตราย 2) Spear Phishing คือ การโจมตีที่เจาะจงถึงบุคคล

หรือองค์กรเฉพาะ มักใช้ข้อมูลของเหยื่อในการแอบอ้าง 3) Smishing (SMS Phishing) การใช้ข้อความ SMS ในการหลอกลวง 4) Vishing (Voice Phishing) การใช้การโทรศัพท์ในการหลอกลวง ซึ่งวิธีการที่ใช้ได้ผลมากที่สุดและทำให้องค์กรหรือบริษัทต่างๆ ได้รับผลกระทบมากที่สุดคือ การทำ Email Phishing

ลักษณะทั่วไปของ Email Phishing มักจะมีลักษณะดังนี้ ชื่อผู้ส่งอีเมลที่ดูเหมือนจริง อีเมลดูเหมือนจะมาจากแหล่งที่เชื่อถือได้ เช่น ธนาคารหรือองค์กรรัฐบาล ข้อความเร่งด่วนหรือมีลักษณะที่สร้างความต้องการในการดำเนินการทันที ดังแสดงในรูปที่ 2.1 มักจะมีลิงก์หรือปุ่มที่ขอให้คุณคลิกเพื่อ "ยืนยันข้อมูล" หรือ "เข้าสู่ระบบ" หากตกเป็นเหยื่อจะเกิดการสูญเสียข้อมูลส่วนบุคคล ผู้ไม่หวังดีอาจใช้ข้อมูลในการกระทำอาชญากรรม จนนำไปสู่ความเสียหายที่เกิดขึ้นกับชื่อเสียงและความน่าเชื่อถือขององค์กร

Phishing เป็นหนึ่งในวิธีการโจมตีที่เป็นที่รู้จักและใช้งานอย่างแพร่หลาย เป็นส่วนหนึ่งของปัญหาความปลอดภัยทางไซเบอร์ที่ไม่หยุดนิ่งและต้องมีการปรับปรุงและป้องกันตัวอย่างต่อเนื่อง



รูปที่ 2.1 ตัวอย่าง Email Phishing

การโจมตีทางไซเบอร์ในปัจจุบันมีแนวโมเพิ่มขึ้นเรื่อย ๆ และผู้ไม่หวังดีจะคิดหาวิธีการใหม่ๆ ออกมาโจมตีผู้ใช้งานอย่างต่อเนื่องยกตัวอย่างเช่น การโจมตีแบบ Ransomware มีแนวโน้มเพิ่มขึ้น และผู้โจมตีอาจเริ่มต้นจากการเรียกค่าไถ่เล็กๆ แล้วเพิ่มขึ้นอย่างรวดเร็ว ผู้โจมตีอาจใช้ระบบของคุณในการขุด cryptocurrency โดยไม่ได้รับอนุญาต Phishing และ Social Engineering ประเภทของการโจมตีที่ใช้จิตวิทยาเพื่อหลอกให้คนเปิดเผยข้อมูลส่วนตัว และความไม่ปลอดภัยของ IoT (Internet of

Things) ในปัจจุบันได้เพิ่มขึ้นตามไปด้วยเนื่องจากอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตเพิ่มขึ้นอย่างรวดเร็วแต่ขาดมาตรการความปลอดภัยที่เพียงพอ ข้อมูลส่วนบุคคลหรือข้อมูลธุรกิจมักถูกขโมยและนำไปขายในตลาดมืด หรือที่เรียกว่า Data Breaches แม้กระทั่ง AI และ Machine Learning ก็จะถูกนำมาใช้ทั้งในการโจมตีและการป้องการเพิ่มมากขึ้นอีกด้วย การโจมตีแบบ Zero-Day ก็เพิ่มขึ้น เนื่องจากช่องโหว่ที่ยังไม่ได้รับการ Update patch

ในยุคดิจิทัลการคำนึงถึงความปลอดภัยทางไซเบอร์เป็นสิ่งที่ไม่สามารถละเลยได้ การ update และปรับปรุงมาตรการความปลอดภัยในระบบ IT เป็นสิ่งที่จำเป็นอย่างยิ่ง การจัดการความเสี่ยงที่ไม่เพียงพอในองค์กรมักขาดการจัดการความเสี่ยงที่เหมาะสม ซึ่งทำให้เกิดช่องโหว่ในระบบของพวกเขา จนนำไปสู่การโจมตีที่มีแรงจูงใจทางการเมืองหรือระดับชาติ (APT: Advanced Persistent Threats) ผู้นำของการโจมตีนี้มักมีการสนับสนุนหรือสนิทสนมกับรัฐบาล

การป้องกันการโจมตีทางไซเบอร์มีหลายวิธีและมีหลายระดับ รวมถึงปัจจัยทั้งที่เกี่ยวข้องกับเทคโนโลยี พนักงาน และกระบวนการภายในองค์กรดังนี้

1. ด้านเทคโนโลยี

1.1 Firewall และ IDS/IPS ใช้ Firewall และระบบตรวจจับ/ป้องกันการโจมตีเพื่อควบคุมการเข้าถึงระบบ

1.2 การป้องกัน Malware ใช้โปรแกรมป้องกันไวรัสและ Malware ที่ป้องกันได้หลากหลายประเภทของโจมตี

1.3 การอัพเดทและ Patching อัพเดทระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ

1.4 การสำรองข้อมูล สำรองข้อมูลอย่างสม่ำเสมอและเก็บในที่ปลอดภัย

2. ด้านพนักงาน

2.1 ฝึกอบรมในเรื่องความปลอดภัยไซเบอร์เพื่อป้องกันการโจมตีที่เกี่ยวข้องกับคน

2.2 จัดทำนโยบายให้มีนโยบายความปลอดภัยที่ชัดเจนและบังคับใช้

2.3 การติดตามและตรวจสอบพฤติกรรมการใช้งานของพนักงานเพื่อตรวจสอบว่าไม่มีการใช้งานที่น่าสงสัย

3. ด้านกระบวนการ

3.1 การจัดการความเสี่ยงควรประเมินความเสี่ยงและจัดการด้วยวิธีการที่เหมาะสม

3.2 การตอบสนองต่อเหตุการณ์ต้องมีแผนการตอบสนองต่อเหตุการณ์ความปลอดภัยที่ชัดเจน

3.3 การตรวจสอบและประเมินมาตรการความปลอดภัยอย่างสม่ำเสมอ

4. ด้านอื่นๆ

4.1 การใช้ Multi-Factor Authentication (MFA) เพื่อยืนยันตัวตนหลายขั้นตอนเพิ่มความปลอดภัย

4.2 จำกัดสิทธิ์การใช้งาน ให้สิทธิ์ที่จำเป็นต่อพนักงานเท่านั้น ไม่ควรให้สิทธิ์สูงในการเข้าถึงระบบแก่ทุกคน

4.3 การเข้ารหัสข้อมูลต้องใช้เทคนิคการเข้ารหัสเพื่อป้องกันข้อมูลจากการถูกขโมยหรือดักฟัง

การป้องกันการโจมตีทางไซเบอร์เป็นกระบวนการที่ต้องดำเนินการอย่างต่อเนื่องและให้ความสำคัญในทุกด้าน ทั้งเทคโนโลยี คน และกระบวนการเพื่อให้เกิดประสิทธิภาพสูงสุดและป้องกันภัยคุกคามได้จริง

2.2 การโจมตีโดยการปลอมแปลงผู้ส่งอีเมล (Email Spoofing Attack)

Email Spoofing Attack หมายถึงการโจมตีทางด้านระบบอีเมลโดยการสร้างอีเมลปลอมขึ้นมาให้ดูเหมือนว่าส่งมาจากแหล่งต้นทางที่เป็นของจริง โดยเนื้อหาของอีเมลจะถูกปลอมแปลงให้ดูเหมือนมาจากแหล่งที่ถูกต้อง ซึ่ง Protocol หลักที่ใช้ในระบบอีเมลคือ SMTP จะไม่มีกลไกการตรวจสอบตัวตนใดๆ ดังนั้นระบบอีเมลจึงมีความเสี่ยงต่อการทำ Spoofing และ Phishing โดยที่ Header ของอีเมลมักถูกปลอมแปลงเพื่อหลอกผู้ใช้ Header ของอีเมลจึงมีความสำคัญสามารถใช้ในการตรวจสอบเพื่อระบุตัวตนของผู้ส่งว่ามาจากแหล่งที่ถูกต้องหรือไม่ ทั้งนี้การคัดแยกหรือตรวจสอบการโจมตีในลักษณะนี้จะทำได้ยาก [4] ทำให้ในปัจจุบันยังมีผู้ใช้งานถูกโจมตีด้วยการทำ Email Spoofing Attack อยู่

การดำเนินการของผู้ไม่หวังดีในการโจมตีแบบ Email Spoof Attack นั้น จะมีขั้นตอนการดำเนินการดังนี้

1. สำรวจข้อมูล ผู้โจมตีจะสำรวจข้อมูลเกี่ยวกับเป้าหมายของตน รวมถึงชื่อผู้ส่งที่อาจน่าเชื่อถือในสายตาของเหยื่อเป้าหมาย

2. ตั้งค่า SMTP (Simple Mail Transfer Protocol) ผู้โจมตีจะใช้ Server SMTP ที่เป็นประเภท Open Relay หรือใช้ข้อมูลรับส่งอีเมล(SMTP credentials) ที่ถูกขโมยมา

3. สร้างอีเมล Headers ส่วนนี้จะบอกถึงรายละเอียดของอีเมลเช่น ผู้ส่ง, ผู้รับ, วันที่ และเนื้อหา ผู้โจมตีจะเปลี่ยนแปลงข้อมูลในส่วน "From" ให้เป็นที่อยู่อีเมลของผู้ที่เหยื่อจะหลงเชื่อ เช่น ผู้บริหาร, ผู้จัดการบัญชีและการเงิน หรือบุคคลอื่นๆ ที่ดูน่าเชื่อถือ

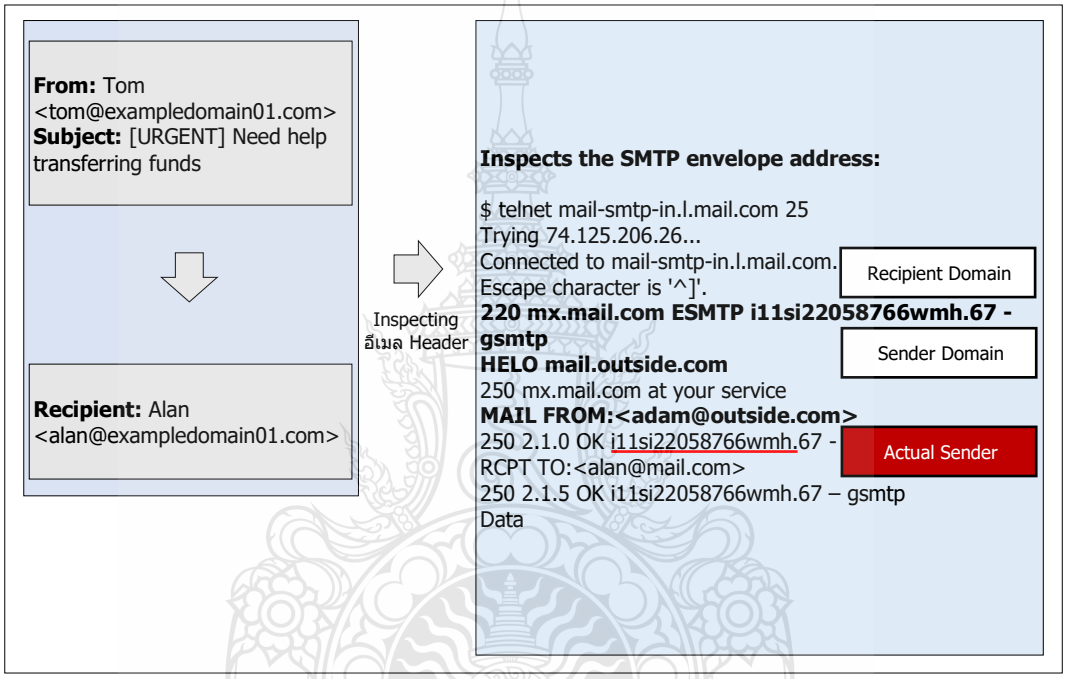
4. สร้างเนื้อหาอีเมล โดยจะมีเนื้อหาที่ถูกออกแบบมาเพื่อความน่าเชื่อถือ อาจจะเป็นแบบฟอร์มเข้าสู่ระบบ ข้อความที่ถามข้อมูลส่วนตัว หรือลิงก์ที่นำไปยังเว็บไซต์ที่ถูกแฮก

5. ส่งอีเมลใช้ Sever SMTP ในการส่งอีเมลปลอมไปยังเป้าหมาย

6. การดำเนินการของเป้าหมาย ถ้าเป้าหมายเปิดอีเมลและดำเนินการตามที่อีเมลนั้นขอให้ทำ เช่น คลิกลิงก์ ป้อนรหัสผ่าน ผู้โจมตีจะได้รับข้อมูลนั้น

7. รับข้อมูลของเหยื่อ ในกรณีที่เป้าหมายตอบสนองตามที่อีเมลขอให้ทำ ผู้โจมตีจะรับข้อมูลและใช้ในการแฮก, การเรียกค่าไถ่เพื่อปลดล็อคไฟล์ของแผนกบัญชีหรือการเงิน

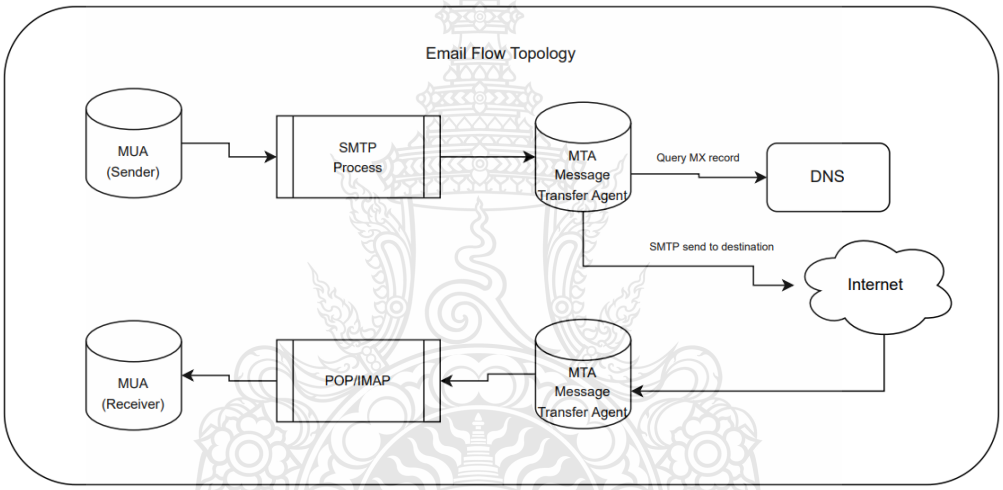
เมื่อนำ Header ของ Spoofing Email มาวิเคราะห์จากการใช้ Telnet จะได้ดังรูปที่ 2.2



รูปที่ 2.2 อีเมล Header ของ Spoofing Email ที่วิเคราะห์จากการใช้ telnet

2.3 ขั้นตอนการ ส่ง-รับ อีเมลเชิงเทคนิค (Email Flow)

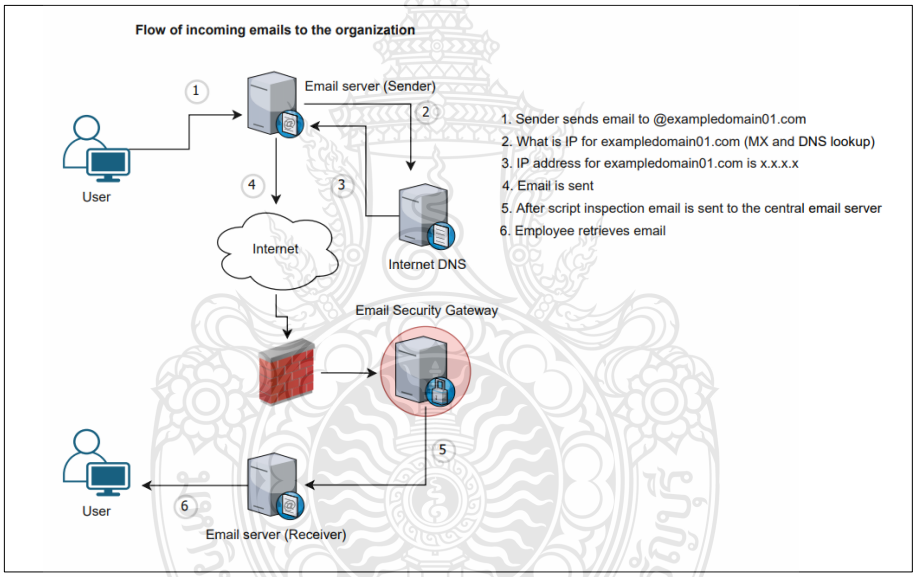
ระบบอีเมลเกิดขึ้นในยุค 60s เมื่อเริ่มมีการใช้ SMTP หรือ Simple Mail Protocol [1] ก่อนหน้าที่ระบบ Internet และโครงสร้างของระบบ Interface จะแพร่ขยายเป็นที่นิยมไปทั่วโลก ระบบอีเมลมีการสร้างบทสนทนาระหว่างเครื่องคอมพิวเตอร์สองเครื่องเป็น Text Massage โดยส่วนประกอบที่สำคัญของระบบอีเมลนั้น จะประกอบด้วย 3 ส่วนหลักๆ 1. Mail User Agent (MUA) ซึ่งจะทำหน้าที่เป็นเครื่องมือที่ผู้ใช้งานจะใช้ติดต่อกับอีเมล Server ผ่านทางหน้าจอ Interface ที่สามารถใช้งานได้ง่าย 2. อีเมล Server ซึ่งภายในอีเมล Server นี้มีกระบวนการเกิดขึ้นมามากมาย เช่น MSA, MTA, MDA, MRA โดยกระบวนการที่สำคัญที่จะกล่าวถึงต่อไปคือ MTA 3. DNS Server โดยลักษณะทางกายภาพของขั้นตอนการ ส่ง-รับ อีเมลนั้นจะเป็นดังรูปที่ 2.3



รูปที่ 2.3 ลักษณะทางกายภาพของขั้นตอนการ ส่ง-รับ อีเมล

เมื่อเราทำการติดตั้งอีเมล Server แล้วต้องทำการตั้ง Hostname ให้กับอีเมล Server ด้วย จากนั้นนำ Hostname นี้มาตั้งค่าไว้ที่ MX Record ที่อยู่บน DNS Server โดยผูก Hostname เข้ากับ IP Address เพื่อประกาศให้เครือข่ายทั่วโลกรู้จักกับ Hostname ของเรา ตัวอย่าง Hostname เช่น mail.exampledomain.com กระบวนการของการรับ-ส่งอีเมลจะเริ่มขึ้นจาก เมื่อผู้ส่งจากบริษัท A สมมุติชื่อ Harry ใช้อีเมล Address: harry@company1.com ต้องการส่งอีเมลไปหา Jenny อีเมล Address jenny@company2.com ที่อยู่ที่บริษัท B หลังจากที่ Harry ทำการกดปุ่ม “ส่ง” อีเมลบน MUA แล้วนั้น อีเมลจะถูกส่งต่อไปที่อีเมล server ผ่าน SMTP Protocol ภายในอีเมล Sever MSA จะตรวจสอบความถูกต้องของ Address จากนั้นจะส่งต่อไปยัง MTA ซึ่ง MTA ก็จะไปตรวจสอบกับโลก Internet ว่า @company2.com ของ jenny นั้นอยู่ที่ใด แต่ในทางเทคนิคแล้วอีเมล Server

จะไปตรวจสอบที่ DNS Sever Local ก่อน โดยจะตรวจสอบ MX Record ของ @company2.com ว่า hostname คืออะไรและอยู่ที่ใด หาก DNS Sever มีข้อมูลนี้เก็บไว้ที่ Cache ก็จะตอบกลับไปที่อีเมล Server ได้เลย แต่หาก DNS Server ไม่มีข้อมูลเหล่านี้ก็จะไปตรวจสอบบนโลก Internet แล้วจึงจะตอบกลับไปที่อีเมล Server เมื่ออีเมล Server มีข้อมูลเหล่านี้แล้ว จะทำการ Establish SMTP session และส่งอีเมลไปยังอีเมล server ของผู้รับอีเมล server ของผู้รับนั้นประกอบด้วย MTA เช่นเดียวกัน MTA จะส่งต่อไปยัง MDA เพื่อทำการส่งอีเมลไปเก็บไว้ยัง Inbox ของ jenny@company2.com เมื่อ jenny login เข้าอีเมลของเขาบนอุปกรณ์ต่างๆ ที่สามาถใช้งาน MTU ได้ jenny จะพบอีเมลที่ส่งมาจาก harry@company1.com โดยที่สามารถเข้าถึงอีเมลผ่าน Protocol POP หรือ IMAP ก็ได้ [5] ทั้งนี้ขึ้นอยู่กับนโยบายและการตั้งค่าขององค์กรนั้นๆ รูปที่ 2.4 จะแสดงตัวอย่างอีเมล Flow ขององค์กรที่ใช้งานโดยทั่วไปตั้งแต่การส่งอีเมลไปจนถึงฝั่งผู้รับอีเมล



รูปที่ 2.4 อีเมล Flow ขององค์กรโดยทั่วไป

2.4 โปรแกรมสำหรับการรับส่งอีเมลของผู้ใช้งาน (Mail Client)

Microsoft Outlook ถือว่าเป็นโปรแกรม Mail Client ที่มีชื่อเสียง เหมาะสำหรับระบบปฏิบัติการ Microsoft Window นอกจากนี้ยังสามารถจัดการข้อมูลส่วนตัวหรือเป็น Organizer ที่ช่วยจัดการเกี่ยวกับปฏิทิน งาน และข้อมูลติดต่อ ถ้ามีการใช้งานร่วมกับ Microsoft Exchange Server ก็จะมีฟีเจอร์เพิ่มเกี่ยวกับการจัดการงานกลุ่มหรือ Groupware เช่น การนัดการประชุม การแชร์ปฏิทินงานและการแชร์ Mailbox

Outlook Express เป็นโปรแกรมอีเมลและสมุดบันทึกข้อมูลติดต่อที่มีมาพร้อมกับ Internet Explorer ซึ่งติดตั้งโดยอัตโนมัติใน Window ทุก version การทำเช่นนี้ก็มีข้อดีคือ สามารถแลกเปลี่ยนข้อมูลกันได้ แต่ข้อเสียก็จะเกี่ยวกับการรักษาความปลอดภัย หาก Outlook มีช่องโหว่ก็จะมีเหมือนกันในทุกๆ ระบบ จุดมุ่งหมายของ Microsoft ก็เพื่อพัฒนาระบบอีเมลและการจัดการข้อมูลส่วนตัวที่เป็นมาตรฐานเดียวกันและง่ายต่อการใช้งาน แต่ข้อเสียคือการพัฒนาโปรแกรมให้ใช้งานง่ายหรือเป็นไปแบบอัตโนมัติ ก็ทำให้มีช่องโหว่เกิดขึ้น และเป็นสาเหตุให้ Virus, Worm และ Malicious Code สามารถแพร่กระจายผ่านทางอีเมลได้อย่างง่ายดาย ความเสี่ยงที่เกิดจากการใช้ Mail Client ได้แก่

1. Virus, Worm, Trojan Horse และ Code ประสงค์ร้ายอื่นๆ มักจะมากับอีเมลในรูปแบบของไฟล์ที่แนบมา

2. Spam คือ อีเมลที่ผู้รับไม่พึงประสงค์

3. Web beaconing เป็นการ Monitor ว่าอีเมลถูกเปิดอ่านโดยผู้ใช้แล้วหรือยัง ซึ่งเป็นเทคนิคการตรวจสอบความถูกต้องของอีเมลAddress ของผู้ไม่หวังดี

โดย Microsoft Outlook และ Outlook Express version ล่าสุด สามารถป้องกันความเสี่ยงต่างๆ ที่กล่าวไว้ข้างต้นหากมีการ Config ที่ถูกต้อง

การป้องกันมีหลายอย่างที่สามารถ Config Microsoft Outlook และ Outlook Express version เพื่อลดความเสี่ยงเนื่องจาก version ใหม่ๆ จะมีฟังก์ชันหรือฟีเจอร์ที่ดีและปลอดภัยกว่าเสมอ ดังนั้นการอัพเดตเป็น version ล่าสุดจึงเป็นสิ่งที่ควรทำเสมอ ซึ่งขั้นตอนในการป้องกันมีดังนี้

1. ติดตามการอัพเดต Window เป็นประจำจาก http://windowsupdate.microsoft.com/ และควรติดตั้ง Patch ใหม่ที่สำคัญๆ เป็นประจำ

2. เปิดการอัพเดตแบบอัตโนมัติ (Automatic Update) เพื่อป้องกันการลืมติดตั้ง Patch ใหม่ๆ

3. เปิดการใช้งาน Message Preview Pane เพื่อป้องกันการแสดงเนื้อความของอีเมลโดยอัตโนมัติ โดยการคลิกเมนู View แล้วไปที่ Layout และไม่เลือก “Show preview pane”

4. เพิ่มความเข้มงวดเกี่ยวกับการตรวจสอบอีเมลที่เข้ามา โดยการคลิกเมนู Tools แล้วไปที่ Options แล้วคลิกที่ Security tab แล้วคลิกเลือก “Restricted sites Zone (More secure)” แล้วปรับให้เป็น “high” แล้วคลิกปุ่ม Apply และ OK

การป้องกันไฟล์แนบที่อาจมี Virus Outlook ทุก Version นั้นมีฟีเจอร์ที่ใช้ได้ผลในการป้องกันไฟล์แนบที่มี Virus โดย Default แล้วไฟล์ที่แนบมาถ้ามีนามสกุลเป็น .exe, .com, และ .vbs เป็นต้น จะถูกบล็อคโดยอัตโนมัติ ดังนั้น การแนบไฟล์ประเภทนี้ควรใช้เครื่องมือสำหรับซิปไฟล์อย่างเช่น WinZip หรือวิธีอื่นในการส่งไฟล์ เช่น FTP เป็นต้น

การป้องกันจาก Spam Mail Outlook มีฟีเจอร์สำหรับป้องกัน Spam Mail อย่างได้ผล ในการ Config นั้นสามารถทำได้โดยเปิด Outlook แล้วไปที่ เมนู Actions แล้วไปที่ Junk E-mail แล้ว ไปที่เมนู Junk E-mail Options ใน Option เหล่านี้จะมีการป้องกัน Spam Mail 4 แบบ คือ

1. No Automatic Filtering คือ การยกเลิกไม่ใช้การฟิลเตอร์ Spam Mail

2. Low (default setting) ค่อนข้างใช้ได้ผลดี เพราะมันจะย้าย Spam Mail ไปไว้ใน โฟลเดอร์ Junk E-mail และอาจมีบางครั้งที่อาจย้ายอีเมลที่ไม่ใช่ Spam Mail

3. High ค่อนข้างเคร่งครัดเกี่ยวกับการฟิลเตอร์ Spam Mail เพราะจะย้าย Spam Mail เกือบทั้งหมดไปไว้ใน โฟลเดอร์ Junk E-mail แต่ก็เป็นไปได้ที่อาจย้ายอีเมลที่ดีไปด้วย ถ้าเลือก Option นี้ควรมีการตรวจสอบอีเมลใน โฟลเดอร์นี้เป็นประจำ

4. Safe Lists Only จะเลือกเอาเฉพาะอีเมลที่มาจากผู้ส่งที่กำหนดไว้ก่อนหน้าเท่านั้น และจะสามารถส่งอีเมลไปหาเฉพาะผู้รับที่กำหนดไว้ล่วงหน้าก่อนเช่นกัน วิธีนี้เป็นการป้องกันที่ดีที่สุด แต่อาจต้องเสียเวลาในการกำหนดผู้รับผู้ส่งก่อน ซึ่งบางครั้งอาจทำได้ยากหรือไม่ได้เลย

ส่วน Microsoft Outlook และ Outlook Express version ก่อนหน้านี้ จะไม่มีฟีเจอร์ใน การฟิลเตอร์ Spam Mail ได้ แต่สามารถกำหนดรายชื่ออีเมลที่ต้องการบล็อคได้ โดยคลิกเมนู Tools แล้วไปที่ Message Rules แล้วเลือก Blocked Senders List

การป้องกัน Malware ที่มีมาในตัวเนื้อความของอีเมลข้อความอีเมลที่ไม่อยู่ในรูปแบบ text ธรรมดา อย่างเช่น HTML และ RTF นั้นอาจมี Malware แฝงตัวมาด้วยก็ได้ ซึ่งจะไม่เหมือน plain text ธรรมดาซึ่งไม่สามารถทำได้ วิธีที่ง่ายและได้ผลที่สุดในการป้องกันโค้ดประสงค์ร้ายเหล่านี้ก็ โดยการอ่าน ทุกอีเมลในโหมด plain text วิธีการ Config ใน Outlook ให้คลิกเมนู Tools แล้วไปที่ Options แล้วเลือก Preference Tab แล้วคลิกปุ่ม E-mail Options แล้วเลือก Read all standard mail in plain text และ Read all digital signed mail in plain text แล้วคลิกปุ่ม OK

การป้องกัน Web Beaconing เป็นเทคนิคในการตรวจสอบว่าอีเมลนั้นได้ถูกเปิดอ่านโดยผู้รับ แล้วหรือยัง และถ้าตรวจสอบได้ก็แสดงว่าอีเมลนั้นเป็นอีเมลจริง และสามารถใช้ได้ในครั้งต่อไป เทคนิคนี้ ทำได้โดยการใส่ภาพเล็กๆ ประมาณ 1x1 pixel ในเนื้อความอีเมลที่อยู่ในรูปแบบ HTML เทคนิคนี้นิยม ใช้มากในพวกที่ส่ง Spam Mail หรือการส่งอีเมลเพื่อการโฆษณา เทคนิคนี้นอกจากจะใช้สำหรับการ ยืนยันการเปิดอ่านอีเมลแล้ว Web Beaconing ยังสามารถใช้สำหรับการ เก็บข้อมูลอื่นเกี่ยวกับผู้ใช้และ ระบบ เช่น IP, ภาษา หรือ version ของเว็บบราวเซอร์ เป็นต้น การป้องกัน Web Beaconing ใน Outlook มีขั้นตอนดังนี้ เปิด Outlook แล้วคลิกเมนู Select Tools แล้วไปที่ Options เลือก Security Tab คลิกปุ่ม Change Automatic Download Setting แล้วคลิกที่ Don't download pictures or other content automatically, in HTML e-mail and warn me before downloading content

when editing, forwarding, or replying to e-mail แล้วคลิกปุ่ม OK อย่างไรก็ Outlook นั้นได้เซตค่านี้เป็นค่า Default อยู่แล้ว

พฤติกรรมของผู้ใช้มีจุดอ่อนที่สำคัญที่สุดของระบบการรักษาความปลอดภัยคือ ส่วนที่เกี่ยวข้องกับผู้ใช้ ดังนั้น การทำตามข้อแนะนำที่ดีที่สุดจึงเป็นสิ่งที่สำคัญในการใช้งานอีเมล เมื่อได้รับอีเมลที่มีไฟล์แนบมาด้วยนั้น ถึงแม้จะมาจากอีเมลที่เชื่อถือได้ แต่ก่อนที่จะเปิดอ่านนั้นก็ควรให้แน่ใจก่อนว่าไฟล์เหล่านั้นไม่มีไวรัส หรือ Malware อื่นๆ ดังนั้น เมื่อได้รับไฟล์แนบ ก็ควรบันทึกไฟล์ไว้ที่โฟลเดอร์อื่นที่ไม่ใช่โฟลเดอร์ My Documents เนื่องจากโฟลเดอร์นี้ส่วนใหญ่ Virus จะใช้เป็นจุดเริ่มต้นในการแพร่กระจายตัวเอง และไม่ควรเปิดไฟล์แนบที่ไม่คาดหวังว่าจะได้ ถึงแม้ว่าจะส่งมาจากคนที่รู้จัก แม้กระทั่งไฟล์ .doc และ .xls ไฟล์ก็ อาจมี VBA macros ที่อาจทำอันตรายให้กับระบบก็ได้ ถ้าจำเป็นต้องเปิดไฟล์เหล่านี้ก็ควรปิดการใช้งานมา Macro โปรแกรมออฟฟิศก่อน ควรมีการตรวจสอบลายเซ็นอิเล็กทรอนิกส์ หรือดิจิตอลซิกเนเจอร์ที่มีมาพร้อมกับไฟล์ประเภทที่รันได้ เพื่อให้แน่ใจว่าไฟล์เหล่านั้นมาจากแหล่งที่เชื่อถือได้

การป้องกันไวรัสโปรแกรมป้องกันไวรัสสามารถช่วยป้องกัน Virus, Worm, Trojan Horse และโปรแกรมประสงค์ร้ายอื่นๆ ได้ แต่ก็ควรมีการอัพเดตไวรัสซิกเนเจอร์เป็นประจำ อย่างน้อยสัปดาห์ละหนึ่งครั้ง เพื่อป้องกันไวรัสตัวใหม่ๆ ที่ออกมาซอฟต์แวร์ป้องกันไวรัสใหม่ๆ ส่วนใหญ่จะอัพเดตให้เราโดยอัตโนมัติ และควรกำหนดให้มีการสแกนไฟล์ทั้งหมดในระบบอย่างน้อย สัปดาห์ละหนึ่งครั้งเช่นกัน ซอฟต์แวร์ป้องกันไวรัสบางยี่ห้อสามารถสแกนอีเมลที่รับเข้ามา และอีเมลที่ส่งออกไปได้ ดังนั้นก่อนที่จะใช้งานอีเมลควรมีการติดตั้งโปรแกรมป้องกันไวรัส version ล่าสุดก่อน เนื่องจากไวรัสหลายชนิดที่แพร่กระจายผ่านทางอีเมลจะมาในรูปแบบของไฟล์ที่แนบมา หรืออาจจะเป็นสคริปต์ที่อาจถูกรันเมื่อผู้ใช้เปิดอ่านอีเมล

อัพเดต Microsoft Outlook และ Outlook Express มีการอัพเดตหลายครั้งในแต่ละปี เพื่อปรับปรุงบิวท์อินฟังก์ชัน ปิดช่องโหว่ และการป้องกัน รักษาความปลอดภัย สามารถตรวจสอบและดาวน์โหลด version ล่าสุดได้ที่ http://www.microsoft.com/windows/oe/ เพื่อให้แน่ใจว่า Outlook และโปรแกรมออฟฟิศอื่นๆ นั้นเป็น Version ล่าสุด ก็สามารถตรวจสอบได้จาก http://office.microsoft.com/en-us/officeupdate/default.aspx เว็บไซต์นี้จะตรวจสอบโดยอัตโนมัติว่ามีอัพเดตที่สำคัญ และอัพเดตที่แนะนำให้ติดตั้งหรือไม่ [6]

2.5 การวิเคราะห์ Header ของอีเมล (Email Header Analysis)

อีเมล Header เป็นส่วนสำคัญของอีเมลซึ่งประกอบด้วยข้อมูลที่ใช้ในการสื่อสารระหว่างอีเมล server และตัวอุปกรณ์ที่ใช้ส่งและรับอีเมลการวิเคราะห์อีเมล Header สามารถช่วยตรวจสอบ

ข้อมูลที่สำคัญในอีเมลได้ เช่น ผู้ส่งอีเมล, ผู้รับอีเมล, วันเวลาที่ส่ง, สถานที่ที่ส่ง, ตัวอุปกรณ์ที่ใช้ส่งอีเมล เป็นต้น ทั้งนี้อีเมล Header ยังสามารถใช้ตรวจสอบหลักฐานที่บ่งชี้ถึงการปลอมแปลงส่วนหนึ่งหรือทั้งหมดของอีเมล Header เพื่อเข้าใจวิธีการโจมตีและพัฒนาเทคนิคในป้องกันการปลอมแปลงอีเมล Header ของผู้ไม่หวังดี

Message Details	
Envelope and Header Summary	
Received Time:	[redacted] 2022 14:45:17 (GMT +07:00)
MID:	[redacted]
Message Size:	5.75 (KB)
Subject:	[Outlook junk mail report] ALERT! I'm hacked your computer and stolen you information!!
Envelope Sender:	[redacted].th Victim's Email Domain
Envelope Recipients:	[redacted] Victim's Email Domain
Message ID Header:	<[redacted].th>
SMTP Auth User ID:	N/A
Attachments	N/A
Sending Host Summary	
Reverse DNS Hostname:	(unverified)
IP Address:	[redacted]
SBRS Score:	rfc1918

รูปที่ 2.5 ตัวอย่าง Email Header ของหน่วยงานรัฐบาลแห่งหนึ่งที่ถูกโจมตีด้วย Email Spoofing

รูปที่ 2.6 ตัวอย่าง Payload ของ Spoof อีเมล

2.6 การตรวจสอบลายเซ็นดิจิตอล (Digital Signature Verification)

การตรวจสอบลายเซ็นดิจิตอลเป็นกระบวนการที่สำคัญในการยืนยันความถูกต้องและความน่าเชื่อถือของเอกสารหรือข้อมูลที่ถูกลงลายเซ็นดิจิตอลด้วยคีย์สาธารณะของผู้ลงนามดิจิตอล (Digital Signature) ดังนั้นการตรวจสอบนี้ต้องทำอย่างระมัดระวังเพื่อป้องกันการปลอมแปลงหรือการแก้ไขข้อมูลที่ลงลายเซ็นดิจิตอลแล้ว ขั้นตอนการตรวจสอบลายเซ็นดิจิตอลปกติมีดังนี้

1. ทำความเข้าใจหลักการของลายเซ็นดิจิตอล ลายเซ็นดิจิตอลประกอบด้วยข้อมูลของเอกสารและลายเซ็นดิจิตอลของผู้ลงนาม ซึ่งถูกนำมาผ่านอัลกอริทึมการเข้ารหัสเพื่อสร้างลายเซ็นดิจิตอล ลายเซ็นดิจิตอลสามารถยืนยันความถูกต้องและความน่าเชื่อถือของเอกสารเนื้อหาไม่เปลี่ยนแปลงและไม่ถูกปลอมแปลง

2. รับข้อมูลเอกสารและลายเซ็นดิจิตอล ในกรณีที่ได้รับเอกสารและลายเซ็นดิจิตอลจากอีเมลหรือแหล่งอื่นๆ ควรเก็บข้อมูลเอกสารและลายเซ็นดิจิตอลไว้ในรูปแบบข้อมูลดิจิตอล

3. ตรวจสอบความสมบูรณ์ของเอกสาร ต้องตรวจสอบว่าเอกสารไม่ถูกแก้ไขหรือเปลี่ยนแปลงใดๆ หลังจากที่ถูกลงลายเซ็นดิจิตอล

4. สกัดลายเซ็นดิจิตอล ลายเซ็นดิจิตอลบ่งบอกถึงความถูกต้องของเอกสารควรสกัดลายเซ็นดิจิตอลออกจากเอกสารเพื่อใช้ในขั้นตอนต่อไป

5. ยืนยันลายเซ็นดิจิตอล การยืนยันลายเซ็นดิจิตอลทำโดยใช้คีย์สาธารณะของผู้ลงนามดิจิตอล ต้องใช้อัลกอริทึมการยืนยันลายเซ็นดิจิตอลเพื่อตรวจสอบว่าลายเซ็นดิจิตอลถูกสร้างโดยคีย์ส่วนตัวของผู้ลงนามดิจิตอลและว่ามีความถูกต้องตามมาตรฐานที่รองรับ

6. ตรวจสอบสภาพความสมบูรณ์ของลายเซ็นดิจิตอล ตรวจสอบว่าลายเซ็นดิจิตอลยังคงมีความสมบูรณ์ โดยไม่มีการเปลี่ยนแปลงหรือการเสียหาย

7. ตรวจสอบใบรับรองดิจิตอล (Digital Certificate) (ถ้ามี) ในบางกรณี ลายเซ็นดิจิตอลอาจมาพร้อมกับใบรับรองดิจิตอล ซึ่งเป็นเอกสารที่รับรองความถูกต้องของคีย์สาธารณะของผู้ลงนามดิจิตอล ควรตรวจสอบใบรับรองดิจิตอลว่าถูกลงลายเซ็นดิจิตอลโดยองค์กรที่น่าเชื่อถือ

8. ตรวจสอบความถูกต้องของคีย์สาธารณะ ตรวจสอบความถูกต้องของคีย์สาธารณะที่ใช้ในการสร้างลายเซ็นดิจิตอล โดยตรวจสอบว่าคีย์สาธารณะนี้ถูกเก็บในระบบสาธารณะและไม่ถูกเปลี่ยนแปลง

9. การยืนยันเอกสาร หลังจากที่ตรวจสอบทุกอย่างและพบว่าลายเซ็นดิจิตอลถูกต้อง เราสามารถยืนยันเอกสารว่ามีความถูกต้องและความน่าเชื่อถือ

การตรวจสอบลายเซ็นดิจิตอลเป็นกระบวนการที่ซับซ้อนและต้องทำอย่างระมัดระวังเพื่อป้องกันการปลอมแปลงและการแก้ไขข้อมูล ในบางกรณี คุณอาจต้องใช้ซอฟต์แวร์หรือบริการออนไลน์

ที่เชี่ยวชาญในการตรวจสอบลายเซ็นดิจิตอลเพิ่มเติม เพื่อให้มั่นใจในความถูกต้องของลายเซ็นดิจิตอล และเอกสารที่เกี่ยวข้อง

2.7 การตรวจสอบช่องโหว่โดยใช้ Sender Policy Framework (SPF)

Sender Policy Framework หรือ SPF เป็นมาตรการหนึ่งที่ใช้สำหรับการตรวจสอบความถูกต้องของอีเมลที่ส่งออกมาจาก Domain ในอีเมลนั้นๆ โดยมีการเริ่มนำมาใช้งานในราวปี 2000 และได้รับมาตรฐานในปี 2014 [8] เป้าหมายของ SPF คือ เพื่อป้องกันการปลอมแปลงที่เกี่ยวข้องกับ Domain อีเมลส่งผลให้ผู้รับสามารถตรวจสอบว่าอีเมลที่ได้รับมาจาก Domain นั้นๆ เป็นอีเมลที่ถูกต้องจากผู้ส่ง (sender) ที่ได้รับอนุญาตกับ Domain นั้นๆ หรือไม่

SPF ทำงานโดยการใช้ Domain Name System (DNS) เพื่อตรวจสอบว่าอีเมลที่ถูกส่งมานั้นมาจาก Domain ใดโดยองค์กรหรือ Domain ที่ของผู้ส่งจะต้องกำหนดค่า SPF ในระบบ DNS ของตน เพื่อเป็นการระบุรายการอนุญาตสำหรับอีเมล server ที่มีอำนาจส่งอีเมลในนามของ Domain นั้นๆ

เมื่ออีเมลถูกส่งไปยังอีเมล server ของผู้รับอีเมล server จะดึงรายการ SPF ที่อยู่ใน DNS record ของ Domain ผู้ส่งมาตรวจสอบ หากองค์กรใดใช้อุปกรณ์ Email security gateway มาทำการคัดกรองอีเมลก่อนส่งไปยังอีเมล server อุปกรณ์ Email security gateway นี้จะทำหน้าที่ในการตรวจสอบ SPF record แทน

การตรวจสอบจะตรวจสอบที่รายการอนุญาต (allowed) หรือรายการปฏิเสธ (denied) ที่กำหนดไว้ใน SPF record ของ Domain ผู้ส่ง ถ้าหาก IP address ของ Server ที่ส่งอีเมลตรงกับรายการอนุญาตใน SPF record จะถือว่าเป็นอีเมลที่ถูกต้อง และ Server ของผู้รับจะรับอีเมลนี้และส่งต่อให้ผู้ใช้งานต่อไป ในกรณีที่ IP address ไม่ตรงกับรายการอนุญาต จะถือว่าเป็นอีเมลที่ไม่ถูกต้อง และ Server ของผู้รับสามารถปฏิเสธการรับอีเมลนี้ได้

```
v=spf1 <mechanisms> <modifiers>
```

รูปที่ 2.7 รูปแบบ syntax โดยทั่วไปของ SPF

```
v=spf1 a mx ip4:192.0.2.1 include:example.com -all
```

รูปที่ 2.8 ตัวอย่าง SPF record

โดยสามารถอธิบาย Mechanisms แต่ละรายการดังนี้

1. "v=spf1" ระบุ Version ของ SPF ที่ใช้ ในที่นี้คือ SPF version 1

2. "a" ระบุให้ตรวจสอบ IP address ของ Server ที่เกี่ยวข้องกับ Domain ที่กำหนดไว้ใน SPF record นี้ ซึ่งจะอนุญาตให้สามารถส่งอีเมลได้

3. "mx" ระบุให้ตรวจสอบ IP address ของ Server ที่ระบุใน MX records ของ Domain นี้ ซึ่งจะอนุญาตให้สามารถส่งอีเมลได้

4. "ip4:192.0.2.1" ระบุ IP address ของ Server ที่อนุญาตให้ส่งอีเมลได้ ยกตัวอย่างเช่น 192.0.2.1 เป็น Server ที่สามารถส่งอีเมลที่ถูกต้องสำหรับ Domain นั้นๆ

5. "include:example.com" ระบุเพื่อให้ตรวจสอบเงื่อนไข SPF จาก Domain example.com และใช้นโยบาย SPF จาก Domain นี้เป็นส่วนหนึ่งของนโยบาย SPF สำหรับ Domain ปัจจุบัน

6. "-all" คำสั่งนี้ คือ กำหนดว่าถ้าอีเมลที่ต้องการส่ง ไม่ผ่านเงื่อนไข SPF ใดๆ ทั้งหมด ให้ปฏิเสธการส่งอีเมลนั้นในทันที โดยสามารถกำหนดตัว Modifier นี้ได้ 3 รูปแบบ

   1. "+all" คือ อนุญาตให้ Server ทั้งหมดสามารถส่งอีเมลได้

   2. "-all" คือ ปฏิเสธ Server ทั้งหมดยกเว้นที่อนุญาตเอาไว้โดยชัดเจน

   3. "~all" คือ Soft fail ทำเครื่องหมายว่ามีความเสี่ยง ว่าจะเป็นอีเมลที่ไม่ปลอดภัย

เมื่ออีเมล server มีอีเมลที่ต้องส่ง ก็จะเข้าสู่ขั้นตอน SPF โดยมีขั้นตอนและกระบวนการดังนี้

1. ตรวจสอบ SPF Record โดยอีเมล server จะดึง SPF record จาก DNS (Domain Name System) ของ Domain ผู้ส่ง อีเมล

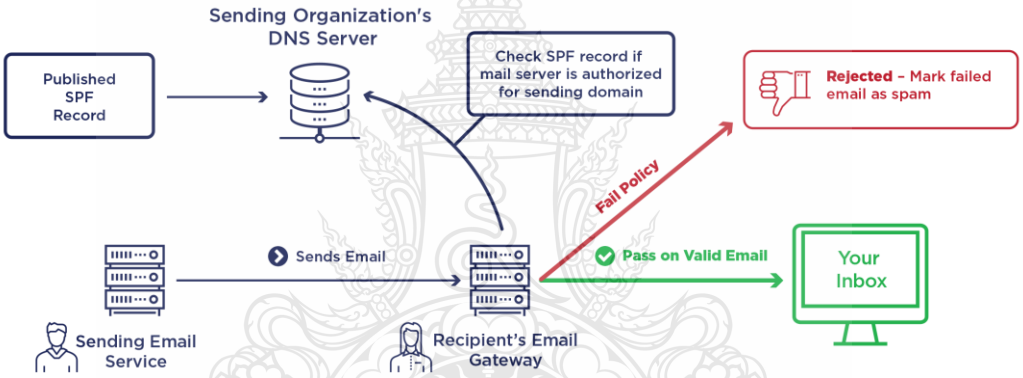
2. ตรวจสอบ IP address โดยที่อีเมล server จะตรวจสอบ IP address ของตนเองที่ใช้ส่งอีเมล

3. ตรวจสอบรายการอนุญาตอีเมล server จะตรวจสอบรายการอนุญาต (allowed) ใน SPF record ที่ระบุว่า server ที่ใช้ส่งอีเมลได้รับอนุญาตหรือไม่

4. Server ผู้รับตัดสินใจการรับหรือปฏิเสธ โดยอ้างอิงจากผลลัพธ์ของตรวจสอบ SPF ถ้า IP address ของ Server ตรงกับรายการอนุญาตอีเมลจะถูกยอมรับและส่งต่อไปยังผู้รับ แต่ถ้า IP address ไม่ตรงกับรายการอนุญาต อาจถูกปฏิเสธและไม่นำเข้าส่งไปยังผู้รับ

5. การจัดการผลการตรวจสอบ ผู้รับอีเมลสามารถกำหนดนโยบายในการจัดการกับอีเมลที่ไม่ผ่านการตรวจสอบ SPF ได้ตามที่ต้องการ อาจจะเป็นการตั้งค่าให้อีเมลถูกส่งไปยัง Junk อีเมลหรือการปฏิเสธการรับอีเมลเหล่านั้นทั้งหมด

6. ส่งอีเมลหลังจากผ่านขั้นตอนการตรวจสอบ SPF และการจัดการผลการตรวจสอบอีเมลจะถูกส่งไปยังผู้รับหรือปฏิเสธการรับอีเมลในกรณีที่ไม่ผ่านการตรวจสอบ SPF



รูปที่ 2.9 Standard Framework ของ Sender Policy Framework (SPF)

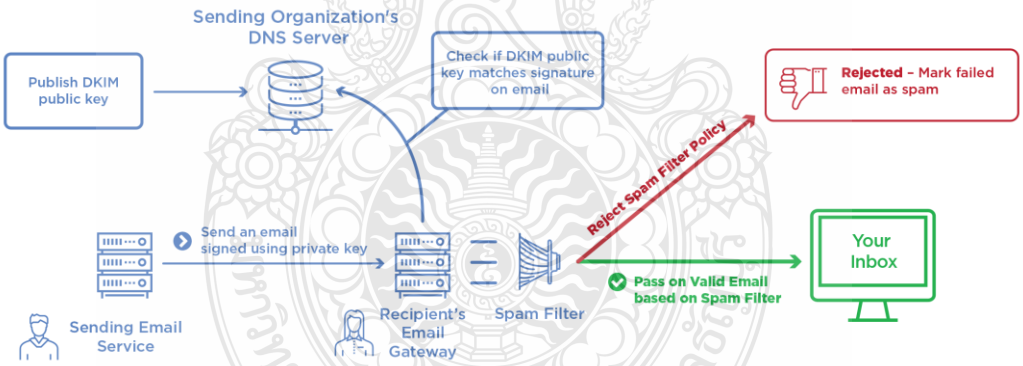
การใช้ SPF ช่วยลดความเสี่ยงที่อีเมลจะถูกปลอมแปลงหรือถูกส่งมาจาก Server ที่ไม่ได้รับอนุญาต โดยมีความหวังว่าผู้รับจะสามารถตรวจสอบความถูกต้องของอีเมลโดยอ้างอิงจาก SPF record ที่ระบุไว้ใน DNS ของ Domain ต้นทาง ทำให้ผู้รับสามารถตัดสินใจเกี่ยวกับการจัดการอีเมลดังกล่าวได้อย่างมีประสิทธิภาพและถูกต้อง ทำให้ SPF เป็นเครื่องมือสำคัญในการป้องกันการปลอมแปลงอีเมลและการ Phishing ซึ่งเป็นการโจมตีทางอีเมลที่จำลองให้ผู้รับเชื่อมั่นว่ามาจากองค์กรหรือบุคคลที่น่าเชื่อถือ แต่แท้จริงแล้วเป็นอีเมลที่อาจมีเจตนาไม่ดี เช่น การขโมยข้อมูลส่วนตัว หรือการหลอกลวงให้เปิดเผยข้อมูลที่ลับ อย่างไรก็ตาม ความซับซ้อนของการตั้งค่า SPF และการจัดการผลการตรวจสอบขึ้นอยู่กับนโยบายและการกำหนดค่าที่ตั้งค่าโดยผู้ดูแลระบบอีเมลและอาจแตกต่างกันไปตามความต้องการและนโยบายของแต่ละองค์กร ผู้ดูแลระบบและผู้ใช้งานอีเมลควรรับรู้เกี่ยวกับการตั้งค่า SPF และนโยบายการจัดการขององค์กรของตนเพื่อให้สามารถป้องกันการปลอมแปลงอีเมลได้อย่างมีประสิทธิภาพ

2.8 การตรวจสอบช่องโหว่โดยใช้ DomainKeys Identified Mail (DKIM)

Domain Keys Identified Mail หรือ DKIM เป็นเทคโนโลยีการเซ็นดิจิทัลที่ใช้ในอีเมลโดยได้รับมาตรฐานปี 2011 [9] เมื่ออีเมลถูกส่งออกจาก Server ของผู้ส่งจะถูกเซ็นด้วยลายเซ็นต์ดิจิทัลที่เข้ารหัสไว้ใน Domain ของผู้ส่ง ผู้รับอีเมลสามารถตรวจสอบลายเซ็นต์ DKIM เพื่อตรวจสอบความถูกต้องและความปลอดภัยของอีเมลหากลายเซ็นต์ไม่ถูกต้องหรือขาดหาย อาจเป็นสัญญาณว่าอีเมลฉบับนั้นอาจเป็น Spoof Email หรือ Fraud Email ซึ่งขั้นตอนการทำงานของ Domain Keys Identified Mail (DKIM) มีดังนี้

1. การกำหนด Key เจ้าของ Domain (Domain owner) จะสร้าง Key สำหรับการเข้ารหัสดิจิตอล ซึ่งประกอบด้วย Key สาธารณะ (Public key) และ Key ส่วนตัว (Private key) โดยทั่วไปแล้วอีเมล server จะรองรับการสร้าง Key เหล่านี้ให้โดยอัตโนมัติ

2. เข้ารหัสดิจิตอล เมื่ออีเมลถูกส่งจากเครื่องส่งอีเมล server ใน Domain ที่ส่ง Package ข้อมูลจะถูกเข้ารหัสด้วย Key ส่วนตัว (Private key) ที่ถูกเก็บไว้ใน Domain ดังกล่าว โดยใช้วิธีการเข้ารหัสดิจิตอลเชิงสาธารณะ เพื่อสร้างลายมือดิจิตอล (Digital signature) บน Header DKIM-Signature ของอีเมล



รูปที่ 2.10 Standard Framework ของ DomainKeys Identified Mail (DKIM)

3. การส่งอีเมล อีเมลที่ถูกเข้ารหัสดิจิตอลแล้วจะถูกส่งไปยังอีเมล server ของผู้รับ พร้อมกับ Header DKIM-Signature ที่มีลายมือดิจิตอล

4.การตรวจสอบลายมือดิจิตอล อีเมล server ของผู้รับจะดึง Key สาธารณะ (Public key) จาก Domain ที่ส่งอีเมลมา เพื่อใช้ในการตรวจสอบความถูกต้องของลายมือดิจิตอล โดยการถอดรหัสข้อมูลใน Header DKIM-Signature ด้วย Key สาธารณะ

5. การตรวจสอบเฉพาะเนื้อหา เมื่อลายมือดิจิตอลถูกถอดรหัสแล้ว จะมีการตรวจสอบว่าข้อมูลในเนื้อหาของอีเมลไม่ถูกแก้ไขหรือปลอมแปลง โดยใช้เทคนิค Document hashing หรือวิธีการอื่นๆ ที่เกี่ยวข้องกับส่วนเนื้อหาของอีเมลต่อไป

2.9 การตรวจสอบช่องโหว่โดยใช้ Domain-based Message Authentication, Reporting, and Conformance (DMARC)

เป็นมาตรฐานที่ออกแบบมาเพื่อเสริมสร้างความน่าเชื่อถือและความปลอดภัยในการสื่อสารทางอีเมลซึ่งทดสอบการใช้งานในราวปี 2015 และได้รับการรับรองมาตรฐานในปี 2015 [10] โดยเฉพาะอย่างยิ่งในเรื่องการป้องกันการปลอมแปลงอีเมลและการ Spam อีเมล โดย DMARC รวมความสามารถของ SPF (Sender Policy Framework) และ DKIM (DomainKeys Identified Mail) เข้าด้วยกันเพื่อเพิ่มประสิทธิภาพและความเชื่อถือของการตรวจสอบการส่งอีเมลของ Domain ซึ่งขั้นตอนการทำงานของ DMARC ประกอบด้วยขั้นตอนต่อไปนี้

1. การตั้งค่า DMARC เจ้าของ Domain (Domain owner) จะตั้งค่า DMARC Record โดยกำหนดนโยบาย DMARC ที่สอดคล้องกับ Domain ของตน เช่น "reject" (ปฏิเสธการส่งอีเมลที่ไม่ผ่านการตรวจสอบ) หรือ "quarantine" (ส่งไปยัง Folder ที่แยกอยู่ระหว่างการตรวจสอบ) รวมถึงกำหนดรายการที่อนุญาตให้ส่งอีเมลในกรณีที่ผ่านการตรวจสอบ

2. การตรวจสอบ SPF อีเมล server ของผู้รับ จะตรวจสอบ SPF record เพื่อตรวจสอบว่าอีเมลที่มาจาก Domain นั้นๆ มีสิทธิ์ในการส่งอีเมลหรือไม่ โดยเปรียบเทียบ IP address ของอีเมล server กับรายการที่กำหนดใน SPF record

3. การตรวจสอบ DKIM อีเมล server จะตรวจสอบลายมือดิจิตอลที่อยู่ใน Header DKIM-Signature เพื่อตรวจสอบความถูกต้องของอีเมลโดยใช้คีย์สาธารณะที่ได้รับมาจาก Domain

4. การตรวจสอบ DMARC อีเมล server จะตรวจสอบ DMARC record ที่มีอยู่ใน Domain ของผู้ส่ง และดำเนินการตามนโยบายที่ได้กำหนด เช่น ปฏิเสธการส่ง (reject) หรือส่งไปยังโฟลเดอร์แยก (quarantine) โดยขึ้นอยู่กับผลลัพธ์การตรวจสอบ SPF และ DKIM

5. การรายงาน DMARC สามารถสร้างรายงานที่รวบรวมข้อมูลเกี่ยวกับผลการตรวจสอบของอีเมลและส่งไปยังผู้ใช้ที่กำหนดได้ เพื่อให้ผู้ส่งอีเมลทราบถึงสถิติและข้อมูลเชิงลึกเกี่ยวกับการส่งอีเมลจาก Domain ของตน

เมื่ออีเมลผ่านขั้นตอนเหล่านี้ของ DMARC จะสามารถช่วยในการป้องกันการปลอมแปลงอีเมลและ Spam อีเมลและเสริมสร้างความน่าเชื่อถือในการสื่อสารทางอีเมลระหว่าง Domain ได้

2.10 งานวิจัยที่เกี่ยวข้อง

Hang Hu และคณะ [7] การปลอมแปลงอีเมลเป็นขั้นตอนสำคัญในการโจมตีแบบ Phishing โดยที่ผู้โจมตีแอบอ้างเป็นบุคคลที่เหยื่อรู้จักหรือมีความไว้วางใจ แม้กระทั่งทุกวันนี้ผู้ให้บริการอีเมลก็ยังคงเผชิญกับความท้าทายที่สำคัญกับการตรวจจับหรือป้องกันการปลอมแปลง แม้ว่าจะพยายามคิดค้นออกแบบแนวทางป้องกันมาหลายปีก็ตาม รวมถึงพัฒนาโปรโตคอลป้องกันการปลอมแปลง (เช่น SPF, DKIM, DMARC) แต่ปัญหาสำคัญคือโปรโตคอลต่อต้านการปลอมแปลงยังไม่เป็นที่แพร่หลายและนำมาใช้ โดยเฉพาะอย่างยิ่งสำหรับโปรโตคอล DMARC ใหม่ มีการนำไปใช้เพียง 5.1% ในบทความนี้เราพยายามที่จะเข้าใจเหตุผลที่อยู่เบื้องหลังความตกต่ำเหล่านี้ อัตราการยอมรับโปรโตคอลเหล่านี้ การป้องกันการปลอมแปลงอีเมลเหล่านี้ เราดำเนินการเรียนรู้เรื่องนี้กับผู้ดูแลระบบอีเมล จากสถาบันต่างๆ จำนวน 9 สถาบัน เพื่อทำความเข้าใจการรับรู้ของพวกเขาต่อโปรโตคอลต่อต้านการปลอมแปลง ผลลัพธ์ของเราแสดงให้เห็นว่าผู้ดูแลระบบอีเมลทราบและกังวลเกี่ยวกับจุดอ่อนทางเทคนิคใน SPF, DKIM และ DMARC ที่สามารถทำให้เกิดข้อผิดพลาดได้ง่าย (เช่น การบล็อกที่ถูกต้องตามกฎหมายอีเมล) ผู้ดูแลระบบอีเมลเชื่อว่าการนำโปรโตคอลมาใช้ในปัจจุบันขาดตัวแปรที่สำคัญเนื่องจากข้อบกพร่องของโปรโตคอล สิ่งจูงใจและความท้าทายในการใช้งานจริงขึ้นอยู่กับสิ่งเหล่านี้ ผลลัพธ์นั้นคือสิ่งเราจะหารือถึงผลกระทบหลักต่อผู้ออกแบบโปรโตคอล ผู้ให้บริการอีเมลและผู้ใช้ และแนวทางการวิจัยในอนาคตเพื่อบรรเทาภัยคุกคามจากการปลอมแปลงอีเมล

J.Ramprasath และคณะ [11] ความปลอดภัยของอินเทอร์เน็ตถูกคุกคามอย่างรุนแรงจากการโจมตีทางด้านอีเมลซึ่งคือการทำ Phishing อีกอย่างหนึ่งบนโลกอินเทอร์เน็ต กระบวนการปกปิดหรือปลอมแปลงข้อมูลผู้ส่งเมล Phishing มีความยืดหยุ่นมากสามารถในปลอมแปลงเนื้อหาในอีเมลและโครงสร้างโดยรวมของอีเมลได้ Email Phishing เป็นการโจมตีทางไซเบอร์ประเภทหนึ่ง เมื่อผู้โจมตีส่งอีเมลที่ดูเหมือนจะเป็นแหล่งที่เชื่อถือได้ไปให้ผู้รับปลายทาง โดยหลอกให้ผู้รับคลิกลิงก์ที่เป็นอันตรายหรือให้ข้อมูลที่ละเอียดอ่อน เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต จุดมุ่งหมายหลักของ Email Phishing มักจะเป็นการเข้าถึงข้อมูล/ข้อมูลที่ละเอียดอ่อน และแพร่กระจาย Malware หรือหลอกลวงเหยื่อด้วยการรีดไถเงิน การตรวจจับ Email Phishing โดยใช้การเรียนรู้ของ Machine learning โดยต้องทำการฝึกอบรมโมเดลบนชุดข้อมูลขนาดใหญ่ทั้ง Email Phishing และอีเมลที่ถูกต้อง แล้วใช้โมเดลนั้นเพื่อแยกประเภทอีเมลขาเข้าที่เป็นอีเมลในรูปแบบ Phishing ได้โดยอัตโนมัติและแม่นยำมากยิ่งขึ้น

Sourena Maroofi และคณะ [12] การส่งอีเมลปลอมโดยใช้ประโยชน์จากการปลอมแปลงโดเมนเป็นเทคนิคทั่วไปที่ผู้โจมตีใช้ เนื่องมาจากยังไม่มีแผนการป้องกันการปลอมแปลงอีเมลที่เหมาะสมหรือมีการกำหนดค่าที่ไม่ถูกต้อง ทำให้การโจมตีแบบ Phishing หรือสแปมสามารถทำได้สำเร็จ

ในบทความนี้ เราจะประเมินขอบเขตของ SPF และการปรับใช้ DMARC โดยใช้การวัดผลจากข้อมูลขนาดใหญ่ที่มีอัตราการยอมรับทั่วโลกด้วยการสแกน 236 ล้านโดเมน และโดเมนที่มีชื่อเสียงสูงใน 139 ประเทศ ซึ่งเราได้ทำการคิดค้นอัลกอริทึมสำหรับระบุโดเมนที่ลงทะเบียนเพื่อการป้องกันและนับโดเมนที่มีการตั้งค่ากฎ SPF ที่กำหนดค่าไม่ถูกต้อง โดยการจำลอง SPF check_function เราทำการกำหนดโมเดลของภัยคุกคามขึ้นมาใหม่เป็นครั้งแรก และแบบจำลองที่เกี่ยวข้องกับการปลอมแปลงโดเมนย่อย และนำเสนอวิธีการเพื่อป้องกันการปลอมแปลงโดเมน ซึ่งเป็นการผสมผสานแนวปฏิบัติเข้าด้วยกัน สำหรับการจัดการบันทึก SPF และ DMARC และวิเคราะห์การบันทึก DNS ในส่วนของการวัดผล เราจะแสดงให้เห็นว่าโดเมนส่วนใหญ่ กำหนดค่ากฎ SPF และ DMARC ไม่ถูกต้องซึ่งช่วยให้ผู้โจมตีสามารถส่งอีเมลปลอมไปยังผู้ใช้ได้สำเร็จ สุดท้ายนี้เราจะรายงานการแก้ไขและผลกระทบ โดยการนำเสนอผลที่ได้รับจากงานวิจัยไปยัง CSIRT ที่รับผิดชอบ ซึ่งจะมีข้อมูลของโดเมนที่ได้รับผลกระทบส่งไปเพื่อประกอบการตรวจสอบด้วย

Nisha T N และคณะ [13] Business Email Compromise (BEC) เป็นวิธีการที่ผู้โจมตีหลอกลวงองค์กรและผู้มีส่วนได้ส่วนเสียทั้งหมดโดยใช้อีเมลธุรกิจที่พนักงานใช้อย่างไม่ระมัดระวัง เอกสารนี้อภิปรายเกี่ยวกับการโจมตีทางด้านอีเมลด้วยวิธีการที่เรียกว่า Business Email Compromise หรือ BEC ที่สามารถระบุและจัดหมวดหมู่กว้างๆ ได้เป็นห้าประเภท ได้แก่ การฉ้อโกงของ CEO, โครงการใบแจ้งหนี้ปลอม, การประนีประนอมบัญชี, การแอบอ้างบุคคลอื่นของทนายความ และการโจรกรรมข้อมูล การวิจัยมุ่งเน้นไปที่การค้นหาเทคนิคที่ใช้สำหรับ BEC เทคนิคการตรวจจับที่สามารถนำมาใช้ในการแก้ไขการโจมตี และค้นหามาตรการรับมือที่เป็นไปได้ในการป้องกันการโจมตีแบบ BEC เทคนิคสำคัญที่ผู้โจมตีและอาชญากรใช้ในการโจมตีแบบ BEC มักจะเป็นวิธีการเก็บข้อมูลประจำตัวและวิธีส่งอีเมลเท่านั้น เทคนิคการขโมยข้อมูลประจำตัวรวมถึงเทคนิคต่างๆ เช่น เทคนิคที่เกี่ยวข้องกับ Phishing และเทคนิคที่เกี่ยวข้องกับ Malware เทคนิคที่เกี่ยวข้องกับการทำ Phishing อาจรวมถึงการใช้วิธีการต่างๆ เช่น จากลิงก์โดยตรง ไฟล์ PDF HTML หรือบริการโฮสต์ไฟล์ การตรวจจับการโจมตีดังกล่าวสามารถทำได้หลายวิธี เช่น ตัวแยกประเภทการเลียนแบบ ตัวแยกประเภทเนื้อหา ตัวแยกประเภทข้อความ ตัวแยกประเภทลิงก์ อัลกอริทึมตัวแยกประเภท มี BEC-Guard ที่สามารถติดตั้งเพื่อติดตามวิธีการเหล่านี้ได้ การจับคู่ชื่อและชื่อเล่นเป็นวิธีการในการตรวจจับการปลอมแปลงชื่อของประเภทการแอบอ้างบุคคลอื่นจะต้องจับคู่ชื่อผู้ส่งกับชื่อของพนักงาน มาตรการตอบโต้เป็นวิธีที่ดีที่สุดที่เป็นไปได้ในการป้องกันการโจมตีของ BEC ตั้งแต่แรก และการป้องกันที่ดีที่สุดสำหรับมาตรการตอบโต้ก็คือบุคลากรต้องมีความรอบรู้ มาตรการรับมือส่วนใหญ่ที่ใช้ ได้แก่ โปรแกรมการฝึกอบรมและการรับรู้เทคนิคการโจมตีของผู้ไม่หวังดี การฝึกอบรมการโจมตีแบบ Phishing การใช้ SPF, DKIM, การป้องกันการปลอมแปลง DMARC และเทคนิคการตรวจสอบสิทธิ์อีเมล

บทที่ 3
วิธีและขั้นตอนในการทำวิจัย

3.1 เครื่องมือที่ใช้ในการวิจัย

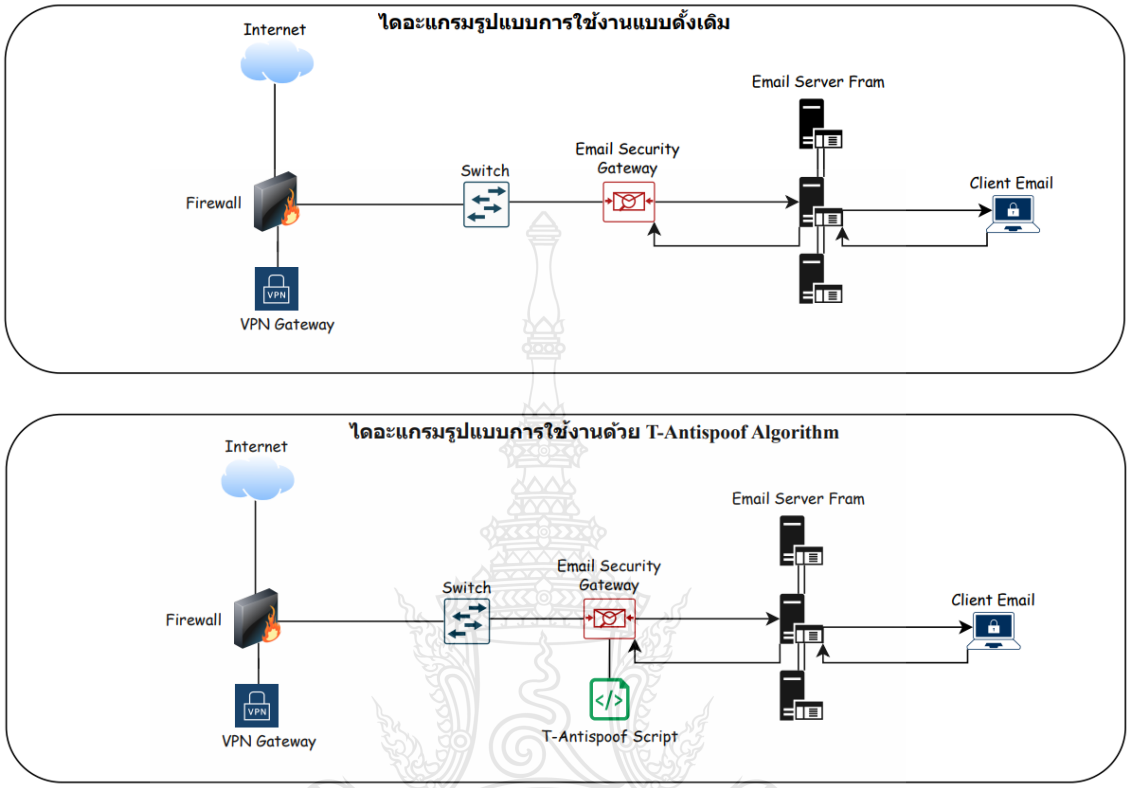
1. Email Security Gateway คือ ระบบที่ใช้สำหรับป้องกันและจัดการความปลอดภัยของอีเมล โดยจะกรองสแปม, ตรวจสอบมัลแวร์, และป้องกันข้อความหลอกลวง เพื่อให้การสื่อสารทางอีเมลขององค์กรหรือผู้ใช้งานมีความปลอดภัยและเชื่อถือได้

2. อีเมล Server คือ คอมพิวเตอร์เซิร์ฟเวอร์ที่ทำหน้าที่จัดการและส่งอีเมล ระหว่างผู้ส่งและผู้รับ โดยจะมีฟังก์ชันในการเก็บ, ส่ง, และรับข้อความอีเมล และอาจมีเครื่องมือเพิ่มเติมสำหรับการจัดการความปลอดภัย หรือการกรองสแปมในระบบ

3. อีเมล Client คือ ซอฟต์แวร์หรือแอปพลิเคชันที่ใช้สำหรับการจัดการอีเมล รวมถึงการส่ง, รับ, อ่าน, และจัดเก็บข้อความ แอปพลิเคชันนี้จะทำการเชื่อมต่อกับอีเมล server โดยใช้มาตรฐานการสื่อสารที่กำหนด อาทิ SMTP สำหรับการส่งอีเมล และ POP3 หรือ IMAP สำหรับการรับอีเมล ตัวอย่างของอีเมล Client ได้แก่ Microsoft Outlook, Mozilla Thunderbird, และ Apple Mail

4. SSL VPN Gateway คือ อุปกรณ์หรือซอฟต์แวร์ที่ใช้ในการสร้างเชื่อมต่อ VPN (Virtual Private Network) โดยใช้ SSL (Secure Sockets Layer) หรือ TLS (Transport Layer Security) เป็นโปรโตคอลในการเข้ารหัสและป้องกันข้อมูล ทั้งนี้เพื่อให้ผู้ใช้งานสามารถเข้าถึง resource ภายในองค์กรผ่านอินเทอร์เน็ตอย่างปลอดภัยและเชื่อถือได้

3.2 วิธีในการดำเนินการวิจัย



รูปที่ 3.1 ไดอะแกรมรูปแบบการทดลองโดยไม่มี T-Antispoof Script

จากการทำงานของอุปกรณ์ประเภท Email security gateway ในปัจจุบันที่ยังไม่สามารถ คัดแยกอีเมลที่เป็นประเภท Spoof Email หรือ Fraud อีเมลภายใต้โครงสร้างพื้นฐานทางด้าน (IT Infrastructure) ในรูปแบบที่แตกต่างกันในแต่ละประเทศรวมถึงข้อจำกัดด้านเทคโนโลยีที่ไม่สามารถนำเทคโนโลยีสมัยใหม่มาปรับใช้กับระบบ Infrastructure ในองค์กรที่ยังมีลักษณะการทำงานเป็นแบบ Hybrid กล่าวคือ มีทั้งอุปกรณ์ที่เป็น technology แบบเก่า และอุปกรณ์ที่เป็น technology แบบใหม่ที่ต้องทำงานร่วมกัน งานวิจัยฉบับนี้จึงได้ทำการศึกษาและพัฒนา Script เพื่อให้อีเมล Security Gateway สามารถคัดแยกอีเมลSpoof ได้ภายใต้ข้อจำกัดนี้

โดยจะทำการศึกษาการใช้งานอีเมลขององค์กรแห่งหนึ่งภายใต้สังกัดการบริหารงานของรัฐบาลในประเทศไทย ซึ่งยังใช้ระบบการรับส่งอีเมลเป็นแบบ On Premise หรือแบบ Legacy มีการรับส่งอีเมลมากกว่า 100,000-500,000 ฉบับต่อวัน และมีผู้ใช้งานมากกว่า 10,000 User ซึ่งตรวจสอบพบว่าผู้ใช้งานได้รับอีเมลที่เป็นประเภท Spoof อีเมลหรือ Fraud อีเมลเป็นจำนวนมาก และสร้างผลกระทบกับผู้ใช้งานในบางรายเนื่องจากเครื่องคอมพิวเตอร์ได้รับ Virus ซึ่งแฝงมากับเอกสารแนบใน

อีเมลทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ได้ในทุก Folder และติดตามการใช้งาน Internet รวมถึงได้รหัสผ่านในการเข้าทำธุรกรรมบน Website ต่างๆ อีกด้วย

3.3 หลักการทำงานของ Email Security Gateway ระบบการคัดแยกอีเมลบนอุปกรณ์ Email Security Gateway

การตรวจจับ Spoofing อีเมลในปัจจุบัน ทำได้โดยใช้อุปกรณ์ที่เรียกว่า Email Security Gateway ที่มีความสามารถทางด้านการคัดแยกอีเมลที่ไม่น่าไว้วางใจต่างๆ ซึ่งมีความแม่นยำในการคัดแยกอีเมลที่เป็น Spam อีเมลได้ถึง 0-90% อีก10% ที่เหลือ จะแบ่งเป็น 5% ไม่สามารถระบุประเภทได้ ส่วนอีก 5% ระบุประเภทผิด และยังพบว่าความสมารถของอุปกรณ์นี้ในปัจจุบันยังไม่สามารถทำการคัดแยกอีเมลที่เป็นประเภท Spoof อีเมลหรือ Fraud อีเมลได้

ระบบการคัดแยกอีเมลบนอุปกรณ์ Email Security Gateway (ESG) เป็นส่วนสำคัญของโครงสร้างรักษาความปลอดภัยสำหรับอีเมลขององค์กร ระบบ ESG ทำหน้าที่ตรวจสอบและคัดแยกอีเมลเพื่อป้องกันอีเมลที่มีความเสี่ยงหรืออันตรายจากการเข้าสู่ระบบอีเมลขององค์กรของคุณ ดังนั้นการทำงานของระบบ ESG มีขั้นตอนดังนี้

1. รับอีเมลเข้าระบบ เมื่ออีเมลถูกส่งมายังเซิร์ฟเวอร์ขององค์กร ระบบ ESG จะรับอีเมลนั้นเข้าระบบของตน

2. ตรวจสอบหัวข้อ (message header) ของผู้ส่ง ระบบ ESG จะตรวจสอบหัวข้อของอีเมลและข้อมูลผู้ส่งเพื่อตรวจหาสัญญาณของอีเมลสแปมหรืออีเมลที่มีลักษณะของการโจมตีแบบพยายามหลอกลวงผู้รับ

3. ตรวจสอบเนื้อหา ระบบ ESG จะสแกนเนื้อหาของอีเมล เช่น เนื้อหาข้อความและไฟล์แนบเพื่อตรวจหาไวรัส, มัลแวร์, หรือลิงก์ที่อาจส่งผ่านไปยังเว็บไซต์ที่เป็นอันตราย

4. ตรวจสอบลิงก์ ระบบ ESG จะตรวจสอบลิงก์ในอีเมลเพื่อตรวจหาลิงก์ที่อาจนำไปสู่เว็บไซต์แบบฉ้อโกงหรือเว็บไซต์ที่มีความเสี่ยง

5. สร้างบันทึก ระบบ ESG อาจจะสร้างบันทึกของการตรวจสอบและการกระทำต่างๆ ที่เกี่ยวข้องกับอีเมล ซึ่งอาจถูกนำไปใช้ในการวิเคราะห์หรือการตรวจสอบความปลอดภัยในอนาคต

6. การตัดสินใจ หลังจากตรวจสอบทุกข้อมูลและคัดแยกการกระทำที่เป็นไปได้ ระบบ ESG จะตัดสินใจเรื่องการจัดการอีเมลนี้อาจหมายความถึงการรับ, ปฏิเสธ, หรือการส่งไปยังกล่องจดหมายขาเข้าของผู้รับ

7. การแจ้งเตือนผู้ดูแลระบบ ในกรณีที่ระบบ ESG ตรวจพบการละเมิดความปลอดภัยหรือสถานการณ์ที่ควรสนใจ ระบบสามารถแจ้งเตือนผู้ดูแลระบบหรือผู้ใช้ที่เกี่ยวข้องเพื่อให้มีการดำเนินที่เหมาะสม

8. จัดการกับอีเมลที่ตรวจพบว่าเป็นอันตราย หากตรวจพบว่าอีเมลเป็นอันตราย ระบบ ESG สามารถทำการบล็อก, ลบ, หรือจัดการในทางอื่นตามนโยบายความปลอดภัยขององค์กร

9. จัดการกับอีเมลสแปม ในกรณีที่อีเมลถูกตรวจพบว่าเป็นสแปม ระบบ ESG สามารถบล็อกหรือถูกส่งไปยังโฟลเดอร์สแปมเพื่อไม่ต้องแสดงให้ผู้รับเห็น

10. บันทึกและสถิติ ระบบ ESG สามารถบันทึกและสร้างสถิติเกี่ยวกับการตรวจสอบและการจัดการอีเมลเพื่อให้ผู้ดูแลระบบสามารถติดตามและวิเคราะห์ข้อมูลเพื่อปรับปรุงความปลอดภัยในอนาคต

11. ป้องกันสแปม ระบบจะกรองอีเมลที่เป็นสแปมออกไป ทำให้ผู้ใช้ไม่ต้องเสียเวลาจัดการกับอีเมลขยะ

12. ป้องกันมัลแวร์และไวรัส หากมีไฟล์แนบหรือลิงก์ที่อาจจะเป็นมัลแวร์หรือไวรัส ระบบจะตรวจสอบและกักกันหรือลบออก

13. ป้องกันฟิชชิ่งและแอตแท็กที่เกี่ยวข้อง อีเมลที่พยายามดึงข้อมูลส่วนบุคคลหรือข้อมูลขององค์กรจะถูกกักกันไว้

14. ควบคุมการเข้าถึงข้อมูล สามารถป้องกันการส่งข้อมูลที่สำคัญหรือละเอียดอ่อนออกจากองค์กรโดยไม่ได้รับอนุญาต

15. ปรับเปลี่ยนกฎและนโยบาย ระบบนี้มักจะมีความยืดหยุ่นในการปรับเปลี่ยนกฎและนโยบายตามความจำเป็นหรือรูปแบบของอีเมลที่องค์กรต้องการ

16. ลดภาระของเซิร์ฟเวอร์ โดยการกรองอีเมลขยะและอีเมลที่อาจจะเป็นอันตราย ทำให้สามารถลดภาระของเซิร์ฟเวอร์ในการจัดการข้อมูล

17. รองรับการปฏิบัติตามข้อกำหนด สามารถตั้งค่าระบบให้สอดคล้องกับข้อกำหนดหรือมาตรฐานขององค์กรหรือข้อกำหนดทางกฎหมาย

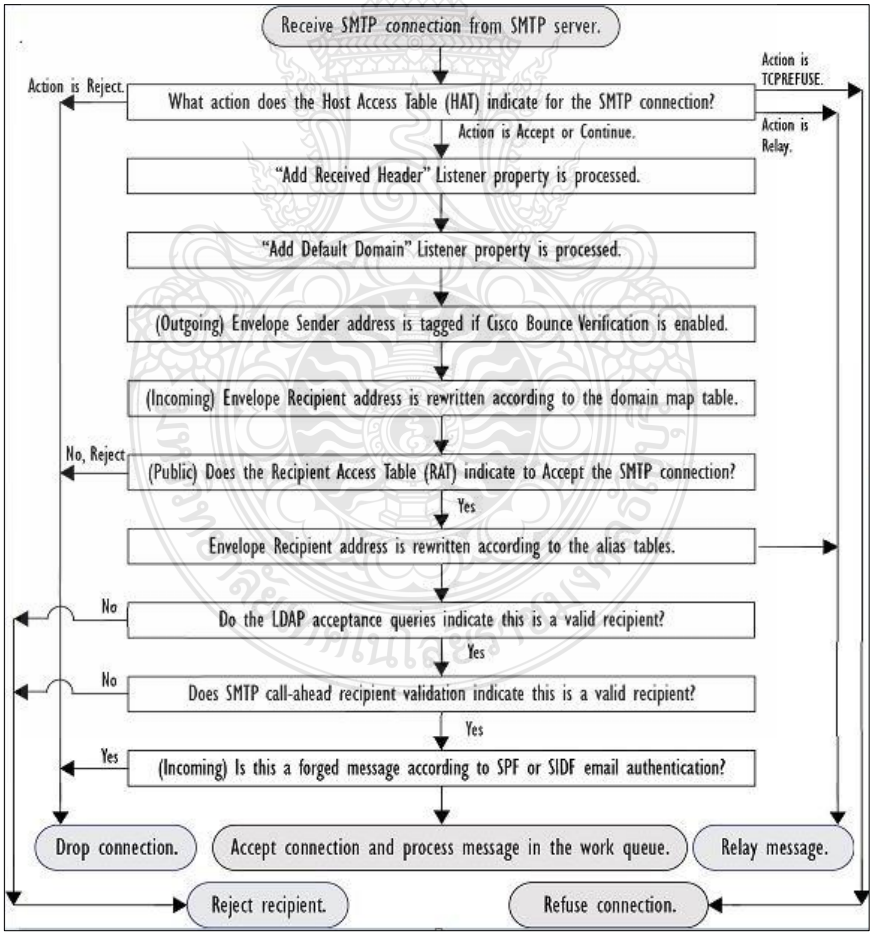
3.4 ภาพรวมของกระบวนการส่งอีเมล

กระบวนการส่งอีเมลเป็นการไหลของอีเมลเมื่อมันถูกประมวลผ่านอุปกรณ์ มีสามช่วงดังนี้ 1)การรับ เมื่ออุปกรณ์เชื่อมต่อกับโฮสต์ระยะไกลเพื่อรับอีเมลเข้ามา อุปกรณ์จะปฏิบัติตามข้อกำหนดที่กำหนดและนโยบายการรับที่กำหนดไว้ เช่น การตรวจสอบว่าโฮสต์สามารถส่งอีเมลให้ผู้ใช้ได้หรือไม่, การบังคับขีดจำกัดการเชื่อมต่อเข้าและขีดจำกัดข้อความ และการตรวจสอบผู้รับของข้อความ เป็นต้น

2)คิวงาน การทำงานของอุปกรณ์ประมวลอีเมลเข้าและออกสามารถทำได้หลายรูปแบบ เช่น การกรอง, การสแกนรายชื่อ Blacklist และรายชื่อ Whitelist, การสแกนอีเมล-สแปมและอีเมลมัลแวร์, ตัวกรองข้อมูลออกเข้าตัวกรองเข้าออก และการกักกัน เป็นต้น 3)การส่ง เมื่ออุปกรณ์เชื่อมต่อเพื่อส่งอีเมลออกไป มันจะปฏิบัติตามขีดจำกัดการส่งและนโยบายการส่งที่กำหนดไว้ เช่น การบังคับขีดจำกัดการเชื่อมต่อขาออกและการประมวลข้อความที่ไม่สามารถส่งได้ตามที่กำหนด

3.5 กระบวนการทำงานของอีเมลเกตเวย์

ภาพด้านล่างเป็นการแสดงภาพรวมของวิธีการประมวลผ่านระบบอีเมล ตั้งแต่การรับส่งไปยังการนำส่ง แต่ละคุณสมบัติถูกประมวลลงในลำดับ (จากบนลงไปล่าง) เราสามารถทดสอบการกำหนดค่าในกระบวนการนี้โดยใช้คำสั่ง Smtp command ที่ Cli ที่ตัวอีเมลเกตเวย์ โดย Pipeline ของกระบวนการรับอีเมลของอีเมลเกตเวย์จะแสดงในรูปที่ 3.2 และมีรายละเอียดดังต่อไปนี้



รูปที่ 3.2 Pipeline กระบวนการรับอีเมลของอีเมลเกตเวย์

1. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบและรับ SMTP Packet จากอีเมล server (SMTP Server)

2. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบ SMTP Packet โดยใช้นโยบายการรับ-ส่ง SMTP Packet จาก Host Access Table ว่าสามารถพิจารณารับอีเมลได้หรือไม่ ในกรณีที่รับได้เข้าสู่กระบวนการถัดไป ในกรณีรับไม่ได้ จะทำการ Drop packet

3. อุปกรณ์อีเมลเกตเวย์ดำเนินการเพิ่ม ผู้รับไว้ที่ Header และส่งต่อไปยังกระบวนการถัดไปของ Listener

4. อุปกรณ์อีเมลเกตเวย์ดำเนินการเพิ่ม Default Domain และส่งต่อไปยังกระบวนการถัดไปของ Listener

5. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบผู้ส่ง ในกรณีที่เข้านโยบาย Bounce อุปกรณ์จะดำเนินการติดเครื่องหมาย Bounce Tag

6. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบผู้รับจากตารางกลุ่มผู้รับและผู้ส่งที่ได้รับอนุญาต

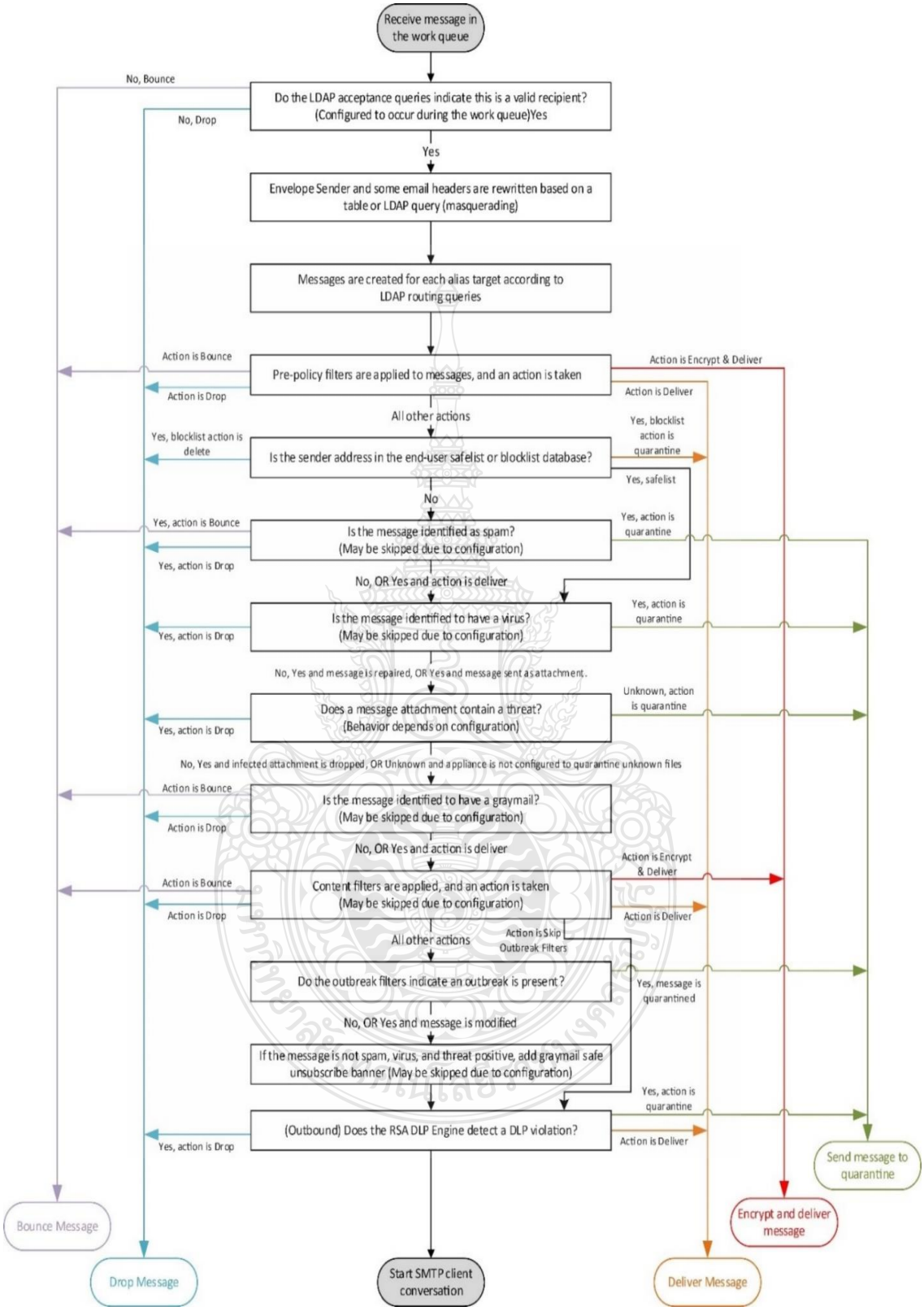
7. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบตารางกลุ่มผู้รับ (RAT) ถ้าถูกต้องดำเนินการรับและส่งต่อไปยังกระบวนการถัดไปของ Listener ถ้าไม่ถูกต้อง Drop Packet

8. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบและเขียนชื่อของผู้รับใหม่เพื่อให้เข้ากันได้กับการทำงานของอุปกรณ์อีเมลเกตเวย์ในหัวข้อถัดไป

9. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบผู้รับว่ามีอยู่ใน LDAP Table หรือไม่ถ้ามีดำเนินการรับและส่งต่อไปยังกระบวนการถัดไปของ Listener ถ้าไม่ถูกต้อง Drop Packet

10. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบอีเมลที่ถูกส่งมายังระบบของคุณเป็นอีเมลที่ถูกต้องและถูกส่งมาถึงผู้รับที่มีอยู่จริงในระบบหรือไม่ ถ้าถูกต้องดำเนินการรับและส่งต่อไปยังกระบวนการถัดไปของ Listener ถ้าไม่ถูกต้อง Drop Packet

11. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบอีเมลผู้ส่งว่าเป็นอีเมลปลอมหรือถูกแก้ไขข้อมูลระหว่างทางหรือไม่โดยเทียบกับ SPF Record หรือ SIDF



รูปที่ 3.3 การทำงานของ Work queue ของอีเมลเกตเวย์

หลักการทำงานและองค์ประกอบที่เกี่ยวข้องกับการจัดการอีเมลและความปลอดภัยของอีเมล ในระบบเกตเวย์อีเมลในส่วนของการจัดเรียงลำดับในการตรวจสอบความปลอดภัย (Work Queue) จะแสดงดังรูปที่ 3.3 และมีรายละเอียดดังนี้

1. LDAP Recipient Acceptance ใช้ LDAP เพื่อกำหนดวิธีการจัดการที่อยู่อีเมลของผู้รับของข้อความขาเข้า

2. Sender Verification Exception Table ตารางข้อยกเว้นนี้ช่วยให้ระบุโดเมนหรือที่อยู่อีเมลที่ควรยอมรับหรือปฏิเสธเมล แม้ว่าจะมีการตรวจสอบ DNS ของผู้ส่งซอง

3. Received Header สามารถตั้งค่าไม่ให้รวมส่วนหัว "Received" ในอีเมลที่ Listener รับ

4. Default Domain ตั้งค่า Listener ให้เติมโดเมนเริ่มต้นให้กับที่อยู่อีเมลที่ไม่ได้ระบุชื่อโดเมนเต็ม

5. Bounce Verification สำหรับอีเมลขาออก ระบบจะใส่คีย์พิเศษเพื่อตรวจสอบหากอีเมลถูกส่งกลับเป็นอีเมล Re-bounce

6. Domain Map สามารถสร้างตาราง domain map เพื่อเปลี่ยนแปลงที่อยู่ผู้รับอีเมลในอีเมลที่ตรงกับโดเมนในตาราง

7. Recipient Access Table (RAT) เฉพาะสำหรับอีเมลขาเข้า RAT อนุญาตให้ระบุโดเมนท้องถิ่นทั้งหมดที่เกตเวย์อีเมลจะยอมรับ

8. Alias Tables ตารางนี้ช่วยในการเปลี่ยนทิศทางข้อความไปยังผู้รับอื่นๆ

9. SMTP Call-Ahead Recipient Validation หยุดการสนทนา SMTP และตรวจสอบที่อยู่อีเมลของผู้รับจากเซิร์ฟเวอร์ SMTP

10. Work Queue / Routing คิวงานที่จัดการและกรองอีเมลก่อนการส่งต่อ

11. LDAP Routing ใช้ข้อมูลจาก LDAP เพื่อกำหนดเส้นทางข้อความ

12. Message Filters ตั้งค่ากรองข้อความในรูปแบบที่ต้องการ

13. Safelist/Blocklist รายชื่อที่ผู้ใช้จัดทำเอง ถูกเก็บในฐานข้อมูลและถูกตรวจสอบก่อนการสแกนป้องกันสแปม ผู้ใช้แต่ละคนสามารถระบุโดเมนหรือที่อยู่อีเมลที่ต้องการจัดเป็นสแปมหรือไม่จัดเป็นสแปม

14. Anti-Spam การสแกนป้องกันสแปมให้ความปลอดภัยครอบคลุมแบบอินเทอร์เน็ตและทำงานเซิร์ฟเวอร์ไซด์สามารถตั้งค่าได้

15. Anti-Virus ระบบสแกนไวรัสถูกบูรณาการไว้ สามารถตั้งค่าและดำเนินการต่างๆ เมื่อตรวจพบไวรัส

16. Graymail ยกเลิกการสมัครใช้งานอย่างปลอดภัยสามารถตั้งค่าระบบให้ตรวจจับข้อความ graymail และยกเลิกการสมัครใช้งานอีเมลให้กับผู้ใช้

17. การสแกนความน่าเชื่อถือของไฟล์และการวิเคราะห์ไฟล์สามารถตั้งค่าระบบให้สแกนไฟล์แนบในข้อความเพื่อค้นหาภัยคุกคามที่ emerging และ targeted

18. ฟิลเตอร์เนื้อหาสามารถสร้างฟิลเตอร์เนื้อหาเพื่อปรับเนื้อหาในข้อความฟิลเตอร์ระบบตรวจจับการระบาดเป็นฟิลเตอร์พิเศษที่สามารถตั้งค่าได้ในการตรวจจับและระงับข้อความที่อาจจะเป็นอันตรายการจัดการการส่งขั้นตอนสุดท้ายของระบบจัดการอีเมล มีการตั้งค่าเกี่ยวกับจำกัดการเชื่อมต่อและอื่นๆ

19. Virtual Gateways เทคโนโลยีนี้ช่วยให้ผู้ใช้สามารถแยกอีเมลเกตเวย์ออกเป็นหลายที่อยู่การจำกัดของการส่งออกสามารถตั้งค่าจำนวนการเชื่อมต่อสูงสุดและจำนวนผู้รับสูงสุดสำหรับแต่ละโดเมน

20. การรับส่งอีเมลขาเข้าและขาออก

21. ขั้นตอนการรับในกระบวนการอีเมลเกี่ยวข้องกับการเชื่อมต่อเริ่มต้นจากโฮสต์ของผู้ส่งโดเมนของแต่ละข้อความสามารถถูกตั้งค่า ผู้รับจะถูกตรวจสอบและข้อความจะถูกส่งต่อไปยังคิวงาน

กระบวนการส่งอีเมลของอีเมลเกตเวย์ (Delivering Email) จะแสดงดังรูปที่ 3.4 ซึ่งมีรายละเอียดดังต่อไปนี้

1. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบการ "SMTP Client Conversation" หรือการสื่อสารของ Client SMTP" คือกระบวนการที่ไคลเอนท์อีเมล (อาจจะเป็นโปรแกรมอีเมลบนคอมพิวเตอร์ของคุณหรือเซิร์ฟเวอร์อีเมล) สื่อสารกับเซิร์ฟเวอร์ SMTP (Simple Mail Transfer Protocol) เพื่อส่งอีเมล

2. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบ Packet ที่ส่งเข้ามาว่ามีนโยบายในการเข้ารหัสข้อความหรือไม่ถ้ามีดำเนินการเข้ารหัสถ้าไม่มีดำเนินการในกระบวนการถัดไป

3. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบ Packet ที่ส่งเข้ามาผ่าน Interface ของอุปกรณ์อีเมลเกตเวย์

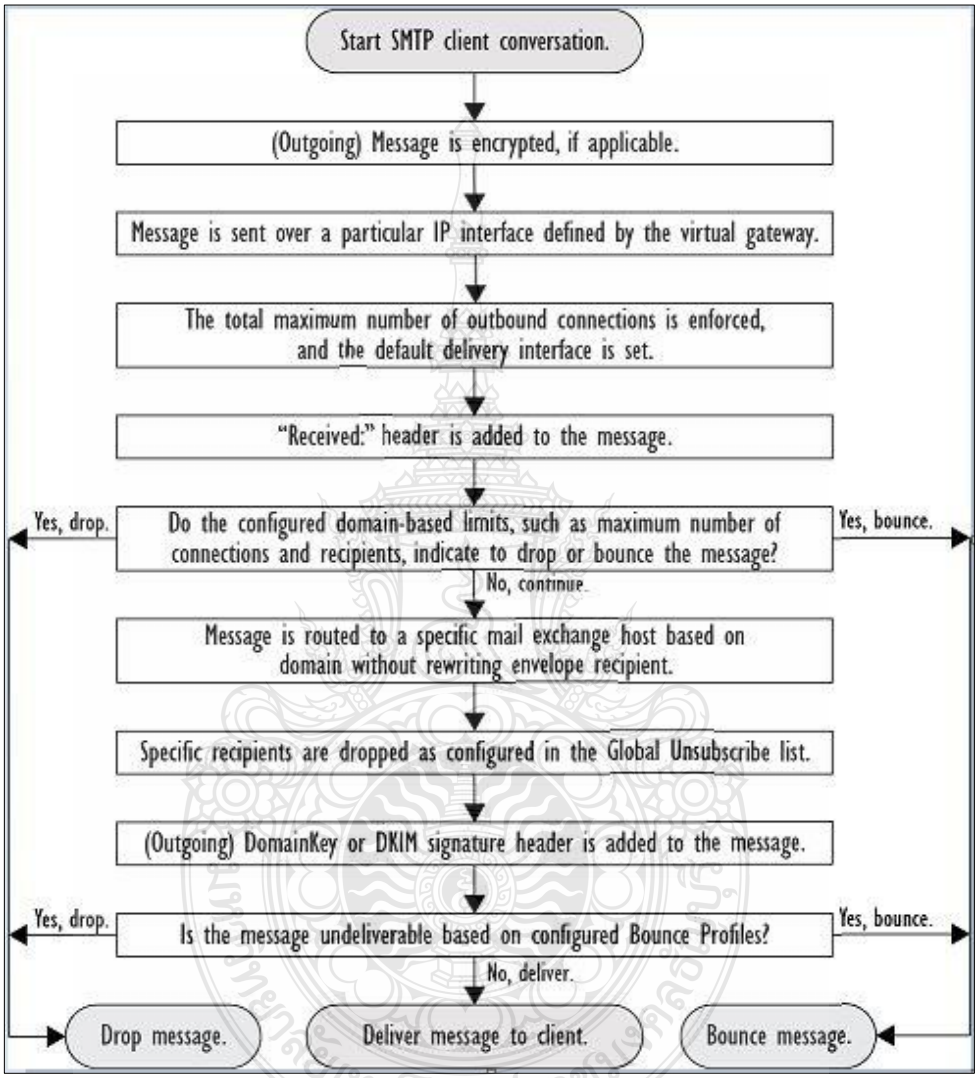
4. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบจำนวน Maximum ที่ถูกตั้งค่าไว้ที่ขาออกว่าเกินขีดจำกัดหรือไม่และส่งไป gateway ที่ถูกต้องหรือไม่

5. อุปกรณ์อีเมลเกตเวย์ดำเนินการเพิ่ม Receive Header ไปที่ข้อความใน packet

6. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบข้อจำกัดของผู้ส่งตามนโยบายที่ได้ตั้งค่าไว้หากเข้าข่าย Bounce Message ให้ส่งไปที่กระบวนการทำงานการตรวจสอบ Bounce Verification หากเข้าข่ายข้อจำกัดในการส่งให้ Drop ข้อความ หากไม่เข้าข่ายทั้งสองให้ส่งไปกระบวนการถัดไป

7. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบ Packet เพื่อทำการยืนยันที่อยู่ของผู้รับ

8. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบ Packet เพื่อทำการยืนยันที่อยู่ของผู้รับอีกครั้ง เพื่อตรวจสอบว่าตรงกับ การตั้งค่า Global Unsubscribe List หรือไม่



รูปที่ 3.4 กระบวนการส่งอีเมลของอีเมลเกตเวย์ (Delivering Email)

9. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบผู้รับในส่วนของการยืนยันข้อความด้วยกระบวนการทำ PKI ในส่วนของ DKIM หากมีการตั้งค่า DKIM ระบบจะดำเนินการเพิ่ม Private Key ไว้ที่ Header ของข้อความ

10. อุปกรณ์อีเมลเกตเวย์ดำเนินการตรวจสอบการตรวจสอบว่าข้อความอีเมลที่ถูกส่งออกไปสามารถส่งถึงผู้รับได้จริงหรือไม่ โดยอาศัย (Bounce Profile) ซึ่งเป็นกฎหรือเงื่อนไขที่ได้ตั้งขึ้นเพื่อ

จัดการกับอีเมลที่ไม่สามารถส่งได้ (Undeliverable) ถ้าไม่ตรงกับเงื่อนไขของ Bounce Profile และไม่ตรงกับเงื่อนไขอีเมลที่ไม่สามารถส่งได้ ดำเนินการส่งข้อความไปที่ปลายทาง

3.6 ภาพรวมของการกำหนดค่าอีเมลเกตเวย์เพื่อรับอีเมล

อุปกรณ์ทำหน้าที่เป็นเกตเวย์อีเมลสำหรับองค์กร ให้บริการการเชื่อมต่ออีเมล การยอมรับข้อความ และส่งต่อไปยังระบบที่เหมาะสม อุปกรณ์สามารถให้บริการการเชื่อมต่ออีเมลจากอินเทอร์เน็ตไปยังโฮสต์ผู้รับภายในเครือข่าย และจากระบบภายในเครือข่ายไปยังอินเทอร์เน็ต โดยทั่วไปคำขอการเชื่อมต่ออีเมลใช้โปรโตคอล Simple Mail Transfer Protocol (SMTP) อุปกรณ์ให้บริการการเชื่อมต่อ SMTP โดยใช้ค่าเริ่มต้น และทำหน้าที่เป็นเกตเวย์ SMTP หรือ "MX" สำหรับเครือข่าย

Listener คืออุปกรณ์ที่ใช้เพื่อให้บริการคำขอการเชื่อมต่อ SMTP ขาเข้าและขาออก และบริการประมวลอีเมลที่กำหนดค่าบนอินเทอร์เฟซด้วย IP Listener ใช้กับอีเมลที่เข้ามาในอุปกรณ์จากอินเทอร์เน็ตหรือจากระบบภายในเครือข่ายของคุณที่พยายามเชื่อมต่อไปยังอินเทอร์เน็ต สามารถใช้ Listener เพื่อระบุเกณฑ์ที่ข้อความและการเชื่อมต่อซึ่งต้องเป็นไปตามมาตราฐานเพื่อให้สามรถยอมรับได้และให้ข้อความถูกส่งต่อไปยังโฮสต์ผู้รับ ซึ่งจะสามารถสร้าง Listener ประเภทต่อไปนี้ได้

1. Listener สาธารณะ (Public) ได้รับการตรวจสอบและยอมรับข้อความอีเมลที่เข้ามาจากอินเทอร์เน็ต Listener สาธารณะรับการเชื่อมต่อจากโฮสต์หลายๆ รายและส่งข้อความไปยังจำนวนผู้รับที่จำกัด

2. Listener ส่วนบุคคล (Private) ได้รับการตรวจสอบและยอมรับข้อความอีเมลที่เข้ามาจากระบบภายในเครือข่าย โดยทั่วไปจากเซิร์ฟเวอร์กลุ่มภายในและเซิร์ฟเวอร์อีเมล (POP/IMAP) สำหรับผู้รับภายนอกเครือข่าย Listener ส่วนบุคคลรับการเชื่อมต่อจากโฮสต์จำนวนจำกัด (ที่รู้จัก) และส่งข้อความไปยังผู้รับ

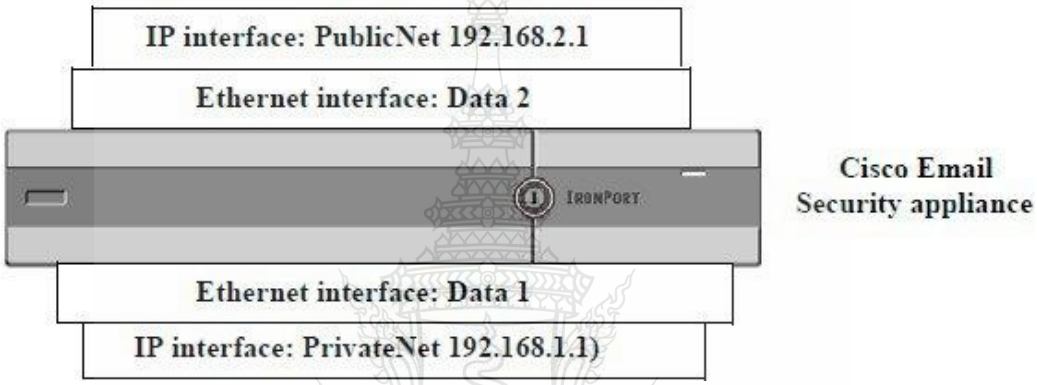
เมื่อทำการสร้าง Listener เรียบร้อยแล้ว ต้องทำการระบุข้อมูลตามรายละเอียดที่แสดงด้านล่าง

1. คุณสมบัติของ Listener กำหนดคุณสมบัติโดยทั่วไปที่ใช้กับ Listener ทั้งหมดและคุณสมบัติเฉพาะแต่ละ Listener เช่น คุณสามารถระบุอินเทอร์เฟซ IP และพอร์ตที่ใช้สำหรับ Listener และว่ามันเป็น Listener สาธารณะหรือส่วนบุคคล

2. โฮสต์ที่อนุญาตให้เชื่อมต่อกับ Listener กำหนดกฎที่ควบคุมการเชื่อมต่อขาเข้าจากโฮสต์ระยะไกล ยกตัวอย่างเช่น คุณสามารถกำหนดโฮสต์ระยะไกลและว่าพวกเขาสามารถเชื่อมต่อกับ Listener หรือไม่ ดูข้อมูลเพิ่มเติมเกี่ยวกับวิธีการทำเช่นนี้ที่กำหนดแต่ละโฮสต์ที่อนุญาตให้เชื่อมต่อโดยใช้ Host Access Table (เฉพาะ Listener สาธารณะเท่านั้น) โดเมนท้องถิ่นที่ Listener ยอมรับ

ข้อความกำหนดผู้รับที่ได้รับการยอมรับโดย Listener สาธารณะ เช่น หากองค์กรของคุณใช้โดเมน company.com และมีการใช้ oldcompany.com มาก่อน คุณอาจยอมรับข้อความสำหรับทั้ง company.com และ oldcompany.com ดูข้อมูลเพิ่มเติมเกี่ยวกับวิธีการทำเช่นนี้ที่การยอมรับหรือปฏิเสธการเชื่อมต่อโดยใช้ชื่อโดเมนหรือที่อยู่ผู้รับ

การตั้งค่าที่กำหนดไว้ใน Listener รวมถึง Host Access Table และ Recipient Access Table มีผลต่อวิธีการที่ Listener สื่อสารกับเซิร์ฟเวอร์ SMTP ระหว่างการสนทนา SMTP นี้ ช่วยให้อุปกรณ์สามารถบล็อกโฮสต์ที่ส่งสแปมก่อนที่การเชื่อมต่อจะถูกปิดลง



รูปที่ 3.5 Public and Private interfaces

รูปที่ 3.6 Relationship between Listeners, IP Interfaces, and Physical Ethernet Interfaces

3.7 การทำงานกับ Listener

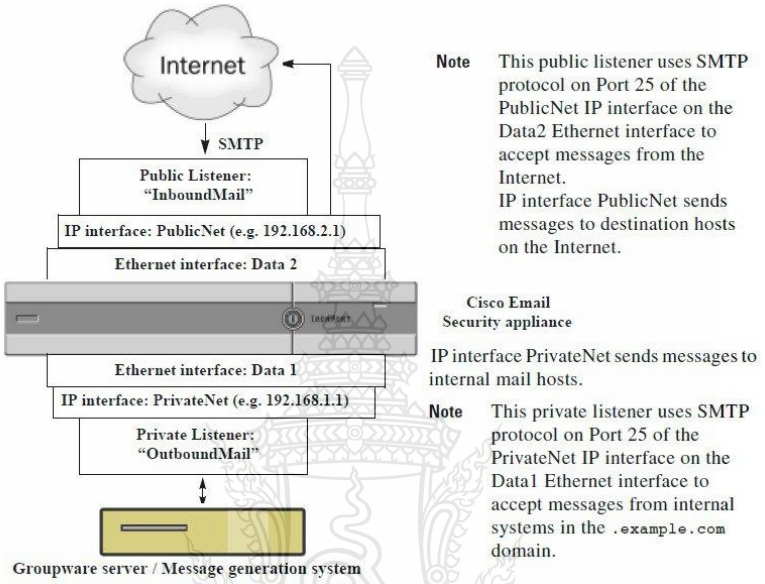
กำหนดค่า Listener บนหน้า Network แล้วไปที่ Listeners ใน GUI หรือใช้คำสั่ง listener config ใน CLI คุณสามารถกำหนดค่าการตั้งค่าที่ใช้สำหรับ Listener ทั้งหมดได้ โดยพิจารณากฎและข้อแนะนำต่อไปนี้เมื่อทำงานและกำหนดค่า Listener บนอุปกรณ์ สามารถกำหนด Listener หลายรายการต่ออินเทอร์เฟซ IP ที่กำหนดค่าไว้ แต่ Listener แต่ละรายการต้องใช้พอร์ตที่แตกต่างกันตามค่าเริ่มต้น Listener ใช้ SMTP เป็นโปรโตคอลอีเมลเพื่อให้บริการการเชื่อมต่ออีเมล อย่างไรก็ตาม สามารถกำหนดค่าอุปกรณ์ให้บริการการเชื่อมต่ออีเมลโดยใช้โปรโตคอล Quick Mail Queuing Protocol (QMQP) ได้ โดยใช้คำสั่ง listenerconfig ใน CLI

Listener รองรับทั้ง Internet Protocol เวอร์ชั่น 4 (IPv4) และเวอร์ชั่น 6 (IPv6) สามารถใช้โปรโตคอลเวอร์ชันใดเวอร์ชั่นหนึ่งหรือทั้งสองใน Listener เดียวกัน Listener ใช้เวอร์ชั่นโปรโตคอลเดียวกันกับเวอร์ชั่นที่มีการเชื่อมต่อโฮสต์ ยกตัวอย่างเช่น หาก Listener ได้รับการกำหนดค่าสำหรับ IPv4 และ IPv6 และเชื่อมต่อกับโฮสต์ที่ใช้ IPv6 Listener จะใช้ IPv6 อย่างไรก็ตามหาก Listener ได้รับการกำหนดค่าให้ใช้เฉพาะที่อยู่ IPv6 เท่านั้น มันจะไม่สามารถเชื่อมต่อกับโฮสต์ที่ใช้เฉพาะที่อยู่ IPv4 ได้อย่างน้อยหนึ่ง Listener (ด้วยค่าเริ่มต้น) จะถูกกำหนดค่าบนอุปกรณ์หลังจากการเรียกใช้ System Setup Wizard อย่างไรก็ตาม เมื่อคุณสร้าง Listener ด้วยตนเอง AsyncOS จะไม่ใช้ค่า SBRS ที่กำหนดเริ่มต้นเหล่านี้

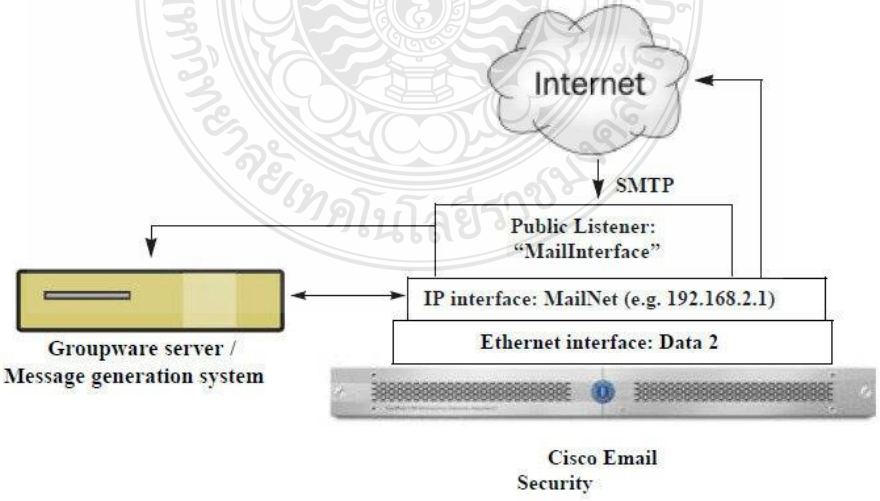
อุปกรณ์อีเมลเกตเวย์ ด้วยค่าเริ่มต้น System Setup Wizard จะนำคุณผ่านการกำหนดค่า Listener สาธารณะหนึ่งรายการสำหรับการรับอีเมลจากอินเทอร์เน็ตและสำหรับการส่งอีเมลจากเครือข่ายภายในของคุณ กล่าวคือ Listener หนึ่งรายการสามารถดำเนินการทั้งสองฟังก์ชันได้
เพื่อช่วยทดสอบและแก้ปัญหาอุปกรณ์คุณสามารถสร้าง Listener ประเภท "blackhole" แทน Listener สาธารณะหรือส่วนบุคคลได้ เมื่อคุณสร้าง Listener ประเภท blackhole คุณสามารถเลือกว่าข้อความจะถูกเขียนลงดิสก์หรือไม่ก่อนที่จะถูกลบ การเขียนข้อความลงดิสก์ก่อนที่จะลบเข้าช่วยให้คุณสามารถวัดอัตราการรับและความเร็วของคิว Listener ที่ไม่เขียนข้อความลงดิสก์ก่อนลบช่วยให้คุณสามารถวัดอัตราการรับแบบบริสุทธิ์จากระบบสร้างข้อความของคุณ Listener ประเภทนี้สามารถใช้ได้เฉพาะผ่านคำสั่ง listener config ใน CLI

รูปที่ 3.7 จะแสดงรายละเอียดของ Listener สาธารณะและส่วนบุคคลบนรุ่นอุปกรณ์ที่มีอินเทอร์เฟสมากกว่าสองอินเทอร์เฟส แสดงให้เห็นการกำหนดค่าเกตเวย์อีเมลปกติที่ถูกสร้างขึ้นโดย System Setup Wizard บนรุ่นอุปกรณ์ที่มีอินเทอร์เฟสมากกว่าสอง มี Listener สองรายการที่ถูกสร้าง Listener สาธารณะเพื่อให้บริการการเชื่อมต่อขาเข้าบนอินเทอร์เฟสหนึ่ง และ Listener ส่วนบุคคลเพื่อให้บริการการเชื่อมต่อขาออกบนอินเทอร์เฟส IP ที่สอง

รูปที่ 3.8 จะแสดงรายละเอียดของ Listener สาธารณะบนรุ่นอุปกรณ์ที่มีอินเทอร์เฟสสองอินเทอร์เฟส แสดงให้เห็นการกำหนดค่าเกตเวย์อีเมลปกติที่ถูกสร้างขึ้นโดย System Setup Wizard บนรุ่นอุปกรณ์ที่มีอินเทอร์เฟสสองอินเทอร์เฟสเท่านั้น มี Listener สาธารณะหนึ่งรายการบนอินเทอร์เฟส IP เดียวเพื่อให้บริการการเชื่อมต่อขาเข้าและขาออกทั้งคู่



รูปที่ 3.7 Public and Private Listeners on Appliance Models with More than Two Ethernet Interfaces



รูปที่ 3.8 Public Listener on Appliance Models with Only Two Ethernet Interfaces

สรุประบบ Email Security Gateway ทำหน้าที่เป็นผู้คอยตรวจสอบและกรองอีเมลที่เข้าและออกจากองค์กร เพื่อป้องกันสแปม, มัลแวร์, ฟิชชิ่ง และข้อความที่อาจมีความรุนแรงหรือไม่เหมาะสม ระบบนี้ยังช่วยควบคุมข้อมูลที่สำคัญไม่ให้หลุดออกจากองค์กรโดยไม่ได้รับอนุญาต ทั้งนี้เพื่อรักษาความปลอดภัยของข้อมูลและลดภาระทางการจัดการสำหรับเซิร์ฟเวอร์อีเมล

หลักการของระบบคือการใช้มาตรการทั้งที่เป็นลักษณะสถิติและพฤติกรรมเพื่อตรวจสอบและวิเคราะห์ข้อมูลในอีเมล มีการปรับเปลี่ยนกฎและนโยบายได้เพื่อให้เหมาะสมกับการใช้งานและข้อกำหนดขององค์กร และสามารถช่วยให้องค์กรปฏิบัติตามข้อกำหนดหรือมาตรฐานที่เกี่ยวข้องกับความปลอดภัยของข้อมูลตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฉบับปี 2562 ได้

3.8 การวิเคราะห์อีเมลที่มีลักษณะเป็น Spoofing Email ที่ทางผู้ใช้งานได้รับ

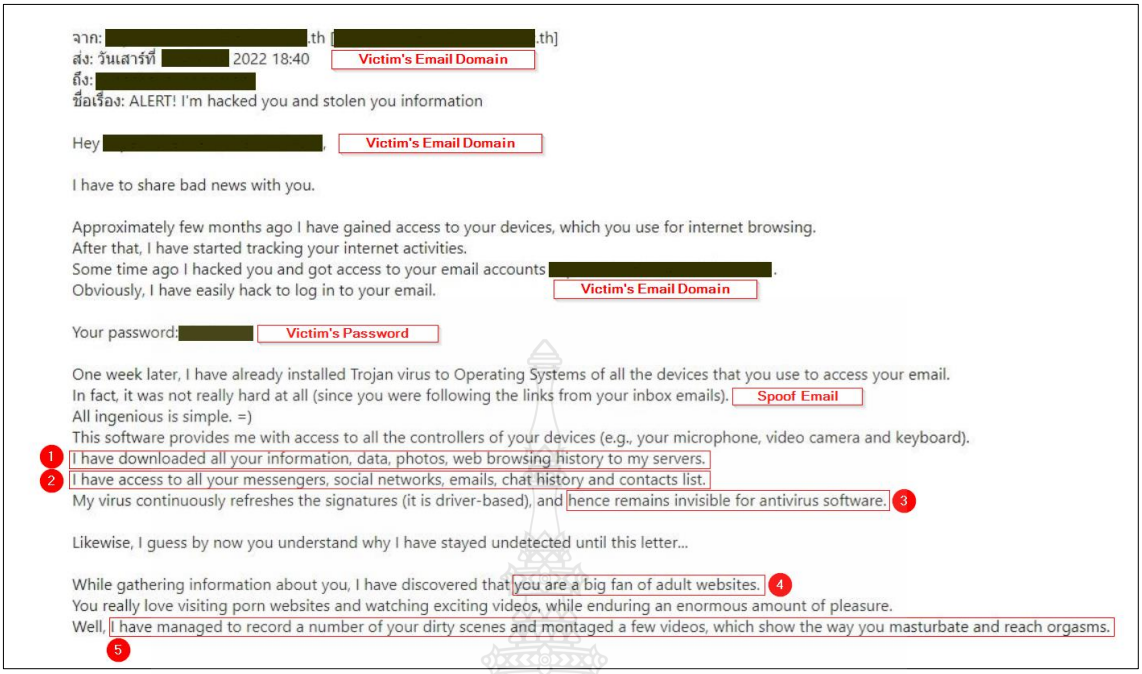
จากการศึกษาลักษณะ Spoof อีเมลขององค์กรแห่งนี้พบว่าจะเป็นอีเมลที่เป็นการส่งจากผู้ใช้งานอีเมล address นั้นๆ เอง แต่เป็นการส่งมาจากต่างประเทศ โดยที่ผู้ส่งไม่ได้เดินทางไปที่ต่างประเทศ ณ ขณะเวลาที่ส่งอีเมลดังนั้นอีเมลฉบับดังกล่าวจึงควรถูกระบุให้เป็น Spoof อีเมลแต่ Email security gateway จะระบุให้อีเมล นี้เป็นอีเมลที่ปลอดภัย เนื่องจากตรวจสอบผู้ส่งว่าส่งมาจาก Domain ที่ปลอดภัย ซึ่งโดยปกติการตั้งค่าของผู้ส่งจาก Domain เดียวกันจะตั้งค่าให้สามารถรับอีเมลได้เป็นปกติ

โดยหลักการในการวิเคราะห์อีเมลที่เป็น Spoof อีเมลที่ผู้ใช้งานได้รับ ต้องเริ่มจากการตรวจสอบที่อยู่ของผู้ส่งอีเมล ตรวจสอบว่าอีเมลดังกล่าวมาจากแหล่งที่น่าเชื่อถือหรือไม่ ซึ่งสามารถใช้เทคนิคที่เรียกว่า SPF, DKIM, และ DMARC ในการตรวจสอบได้

หลังจากนั้น คือการวิเคราะห์ลิงก์และไฟล์ที่แนบมากับอีเมล ให้ตรวจสอบ URL และไฟล์แนบโดยใช้ซอฟต์แวร์ป้องกันไวรัส หรือแม้แต่เครื่องมือออนไลน์ที่ช่วยวิเคราะห์ลิงก์และไฟล์ แต่ถ้าสามารถทำได้ ควรที่จะวิเคราะห์เนื้อหาของอีเมลเหล่านี้อย่างละเอียด ดูว่ามีข้อความหรือคำศัพท์ใดที่ดูเหมือนจะผิดปกติหรือไม่

ตัวอย่างอื่นที่สำคัญคือ การตรวจสอบรูปแบบและสไตล์การเขียน หากเคยได้รับอีเมลจากองค์กรหรือบุคคลดังกล่าวมาก่อน ลองเปรียบเทียบว่ารูปแบบและสไตล์การเขียนนั้นตรงกับอีเมลที่เคยได้รับหรือไม่ ซึ่งอาจช่วยสร้างความน่าสงสัยหรือแม้แต่คอนเฟิร์มว่าอีเมลนั้นเป็น Spoof อีเมล

ถ้าพบว่าอีเมลนั้นมีลักษณะของ Spoof อีเมลควรที่จะรายงานให้กับทีมดูแลระบบหรือฝ่ายความปลอดภัยขององค์กรให้ทราบ และจำเป็นต้องดำเนินการเพื่อป้องกันการเกิดอุบัติการณ์ไม่พึงประสงค์ในอนาคต ซึ่งอาจรวมถึงการปรับเปลี่ยนระบบป้องกันอีเมล การฝึกอบรมพนักงาน หรือการเปลี่ยนแปลงนโยบายความปลอดภัยในองค์กร



รูปที่ 3.9 ตัวอย่างอีเมลแจ้งเตือนการถูกโจรกรรมข้อมูลที่ส่งมาจากผู้ไม่หวังดี

3.9 การออกแบบ T-Antispoof Algorithm บนอุปกรณ์ Email Security Gateway บนสภาพแวดล้อมจำลอง (Test Environment)

เนื่องจากระบบอีเมล เป็นระบบการทำงานที่จำเป็นต้องใช้อุปกรณ์ของฝั่งผู้รับและผู้ส่งทำงานร่วมกัน ทางฝั่งของผู้รับจึงไม่สามารถ Filter และเปิด Security Feature ของทางฝั่งผู้รับด้านเดียวได้ เหมือนกับอุปกรณ์ Network Security อื่นๆ ยกตัวอย่างเช่น หากเราจำเป็นต้อง turn on SPF DKIM และ DMARC เพื่อทำการ scanอีเมลขาเข้าที่ส่งเข้ามาในองค์กรของเรา แต่ทางฝั่งผู้ส่ง ไม่ได้ใช้งาน SPF DKIM จากทางฝั่งผู้ส่ง ดังนั้นองค์กรของเราเองก็มีความเสี่ยงที่จะได้รับอีเมลปลอมแปลง จากผู้ส่งรายดังกล่าว และในยุคคปัจจุบันจากปัญหาที่ได้กล่าวมาข้างต้น องค์กรส่วนใหญ่จำเป็นต้องทำธุรกิจกับหลายหน่วยงานหลายองค์กร รวมถึงมีลูกค้าที่หลากหลาย ทำให้เราไม่สามารถ enable SPF DKIM DMARC เพื่อทำการ quarantine หรือ reject อีเมลของผู้ส่งได้ทุกราย เพราะเราก็ยังจำเป็นต้องติดต่อสื่อสารกับผู้ใช้งานรายใหม่ๆ ที่มาร่วมทำธุรกิจกับฝั่งผู้รับเอง

การตรวจจับ Spoofing อีเมลในปัจจุบันจึงทำได้โดยใช้ Email Security Gateway ที่มีความสามารถทางด้านการคัดแยกอีเมลที่ไม่น่าไว้วางใจต่างๆ เช่น Phishing อีเมล, Spoofing อีเมลเป็นต้น อุปกรณ์ Email Security Gateway ที่ใช้ในการศึกษาในที่นี้จะใช้เป็น Cisco อีเมล Gateway ภายใต้ระบบการใช้งานอีเมล server แบบ On premise ซึ่งยังเป็นที่นิยมในองค์กรรัฐบาลของหลาย

ประเทศที่ยังไม่มีงบประมาณในการใช้งานอีเมล server แบบ Cloud จากการ implement Cisco อีเมล Gateway ตามการตั้งค่าแบบมาตรฐานปกติของอุปกรณ์ แล้วติดตามผลเป็นระยะเวลา 120 วัน พบว่าสามารถคัดแยกสามารถคัดแยกอีเมลที่ไม่ปลอดภัยได้อย่างมีประสิทธิภาพ แต่จากที่กล่าวมาข้างต้น ยังไม่อีเมลที่น่าสงสัยว่าไม่ปลอดภัยบางฉบับถูกส่งไปยังผู้ใช้งาน ซึ่งนั่นคือ Spoofing อีเมล

```
If sendergroup is not in "registered IPv4 relay list" then
   If (mail-from matches "@exampledomain01\.com$")
      OR (mail-from matches "exampledomain01\.co\.th$")
      OR (mail-from matches "exampledomain02\.com$")
      OR (header("From") matches "@exampledomain01\.com$")
      OR (header("From") matches "exampledomain01\.co\.th$")
      OR (header("From") matches "exampledomain02\.com$")
   Then
      Quarantine the email using "quarantine profile name"
      Log "Antispoof Email Details: MID " + MID + " " + RemoteIP + " " + remotehost + " " +
EnvelopeFrom
   End If
End If
```

รูปที่ 3.10 Algorithm: T-Antispoof ที่ใช้คัดแยก Spoofing อีเมลแบบ pseu-do-code

เราจึงทำการตรวจสอบไปยังอุปกรณ์ Cisco อีเมล Gateway พบว่าอีเมลเหล่านั้นส่งมาจาก IP Address ที่เป็นของต่างประเทศ เมื่อทำการตรวจสอบ Header ของอีเมลที่ถูกระบุว่าปลอดภัยโดยละเอียดพบว่า มีอีเมลในลักษณะนี้เป็นจำนวนมาก ทำให้เราพบช่องโหว่ของอุปกรณ์นี้ ว่าไม่สามารถคัดแยกอีเมลที่เป็น Spoofing อีเมลได้ ดังนั้นเราจึงคิดค้น Script ตามรูปที่ 3.9 เพื่อมาช่วยเพิ่มประสิทธิภาพของอุปกรณ์ Cisco อีเมล Gateway นี้ให้สามารถคัดแยกอีเมลที่เป็นภัยคุกคามในรูปแบบ Spoofing อีเมลได้

โดยการตรวจสอบของ Script นี้เริ่มจากการตรวจสอบ IP Address ของผู้ส่ง ว่าถ้าหากไม่ได้อยู่ในส่วนที่ตั้งค่าไว้ว่าปลอดภัย หรือกล่าวคือ เป็น IP Address ที่ไม่ใช่ IP Address ที่ใช้ภายในองค์กรนี้ ให้ไปตรวจสอบที่เงื่อนไขต่อไป คือ ตรวจสอบอีเมลDomain ว่าเป็น Domain ขององค์กรแห่งนี้หรือไม่ ถ้าเงื่อนไขนี้เป็นจริงให้ทำการ Quarantine และทำการเก็บ Log ไว้

Algorithm: T-AntiSpoof for Email Filtering
Objective:
To identify and quarantine emails that are likely to be spoofed based on the sender's IP and the email headers, mail-from and from.

Inputs:
senderGroup: The group to which the sender's IP address belongs.
registeredIPV4RelayList: A list of registered IPv4 addresses or groups allowed to relay mail.
mailFrom: The domain in the mail-from header in the email.
headerFrom: The domain in the from header in the email.
MID: Message ID of the email.
RemoteIP: The remote IP address from which the email was sent.
remoteHost: The remote host from which the email was sent.
EnvelopeFrom: The envelope from address in the email.
Output:
A Boolean flag indicating whether the email was quarantined.
A log entry containing details of the quarantined email, if applicable.
Method:
Initialization

isQuarantined = False
Check the Sender's Group

If senderGroup is NOT in registeredIPV4RelayList then:
Else:
Return isQuarantined
Check the mail-from and From Headers

If mailFrom matches any of the following:
"@exampledomain01.com"
"exampledomain01.co.th"
"exampledomain02.com"
OR headerFrom matches any of the following:
"@exampledomain01.com"
"exampledomain01.co.th"
"exampledomain02.com"
Then:
- Quarantine the email using the designated profile.
- isQuarantined = True
- Generate a log entry:
- "Antispoof Email Details: MID " + MID + ", " + RemoteIP + ", " + remoteHost + ", " + EnvelopeFrom

Return Result

Return isQuarantined

รูปที่ 3.11 อธิบายหลักการทำงานของ T-Antispoof Algorithm step by step

```
#include <stdio.h>
#include <stdbool.h>
#include <string.h>

// Function to simulate 'matches' (here, we're using exact string comparison)
bool matches(const char *str, const char *pattern) {
   return strcmp(str, pattern) == 0;
}

// The main anti-spoofing algorithm
bool T_AntiSpoof(const char *senderGroup, const char *mailFrom, const char
*headerFrom,
                 const char *MID, const char *RemoteIP, const char *remoteHost, const char
*EnvelopeFrom) {

   bool isQuarantined = false;

   // Simulated Registered IPv4 Relay List (replace with actual list)
   const char *registeredIPV4RelayList[] = {"registeredGroup1", "registeredGroup2",
NULL};

   // Check senderGroup against registeredIPV4RelayList
   bool senderGroupIsRegistered = false;
   for (int i = 0; registeredIPV4RelayList[i] != NULL; i++) {
      if (matches(senderGroup, registeredIPV4RelayList[i])) {
         senderGroupIsRegistered = true;
         break;
      }
   }

   if (!senderGroupIsRegistered) {
      // Check mailFrom and headerFrom against predefined domains
      if (matches(mailFrom, "@exampledomain01.com") || matches(mailFrom,
"exampledomain01.co.th") || matches(mailFrom, "exampledomain02.com") ||
         matches(headerFrom, "@exampledomain01.com") || matches(headerFrom,
"exampledomain01.co.th") || matches(headerFrom, "exampledomain02.com")) {

         // Perform Quarantine action (This is just a placeholder)
         printf("Email Quarantined.\n");

         // Log Entry (This is just a placeholder)
         printf("Antispoof Email Details: MID %s, %s, %s, %s\n", MID, RemoteIP,
remoteHost, EnvelopeFrom);
```

รูปที่ 3.12 อธิบายหลักการทำงานของ T-Antispoof Algorithm เขียนโดยภาษา C

```
            isQuarantined = true;
        }
    }

    return isQuarantined;
}

int main() {
    // Sample Test
    if (T_AntiSpoof("unregisteredGroup", "@exampledomain01.com",
"@exampledomain01.com", "MID123", "192.168.1.1", "remoteHost1", "envelopeFrom1"))
{
        printf("The email was successfully identified as spoofed and quarantined.\n");
    } else {
        printf("The email passed the anti-spoofing checks.\n");
    }

    return 0;
}
```

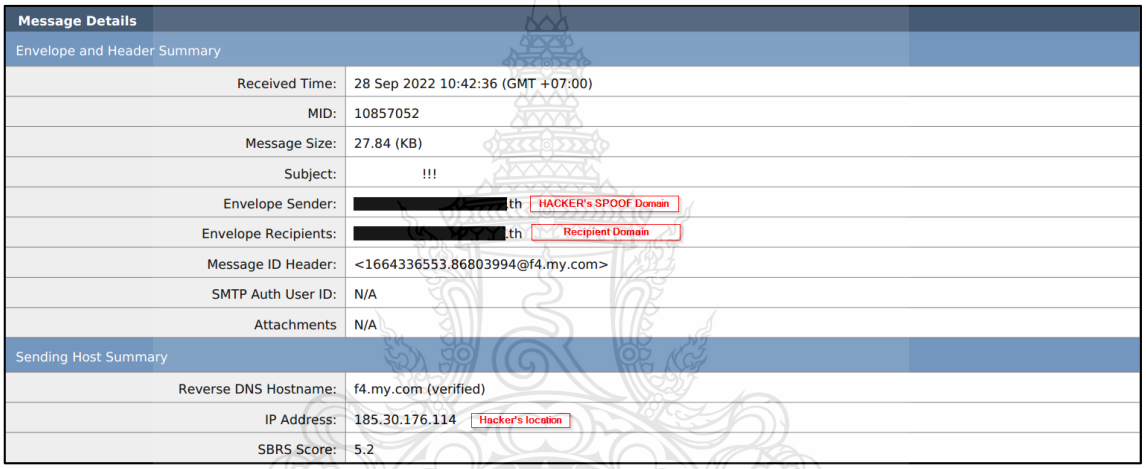
รูปที่ 3.12 อธิบายหลักการทำงานของ T-Antispoof Algorithm เขียนโดยภาษา C (ต่อ)

```
def matches(string, pattern):
   return string == pattern

def T_AntiSpoof(senderGroup, mailFrom, headerFrom, MID, RemoteIP, remoteHost,
EnvelopeFrom):
   isQuarantined = False

   # Simulated Registered IPv4 Relay List (replace with actual list)
   registeredIPV4RelayList = ["registeredGroup1", "registeredGroup2"]

   # Check senderGroup against registeredIPV4RelayList
   senderGroupIsRegistered = senderGroup in registeredIPV4RelayList

   if not senderGroupIsRegistered:
      # Check mailFrom and headerFrom against predefined domains
      if (matches(mailFrom, "@exampledomain01.com") or matches(mailFrom,
"exampledomain01.co.th") or matches(mailFrom, "exampledomain02.com") or
         matches(headerFrom, "@exampledomain01.com") or matches(headerFrom,
"exampledomain01.co.th") or matches(headerFrom, "exampledomain02.com")):

         # Perform Quarantine action (This is just a placeholder)
         print("Email Quarantined.")

         # Log Entry (This is just a placeholder)
         print(f"Antispoof Email Details: MID {MID}, {RemoteIP}, {remoteHost},
{EnvelopeFrom}")

         isQuarantined = True

   return isQuarantined

# Sample Test
if T_AntiSpoof("unregisteredGroup", "@exampledomain01.com",
"@exampledomain01.com", "MID123", "192.168.1.1", "remoteHost1", "envelopeFrom1"):
   print("The email was successfully identified as spoofed and quarantined.")
else:
   print("The email passed the anti-spoofing checks.")
```

รูปที่ 3.13 อธิบายหลักการทำงานของ T-Antispoof Algorithm เขียนโดยภาษา python

3.10 การติดตั้งและทดสอบ T-Antispoof Algorithm บนอุปกรณ์ Email Security Gateway ภายในองค์กร

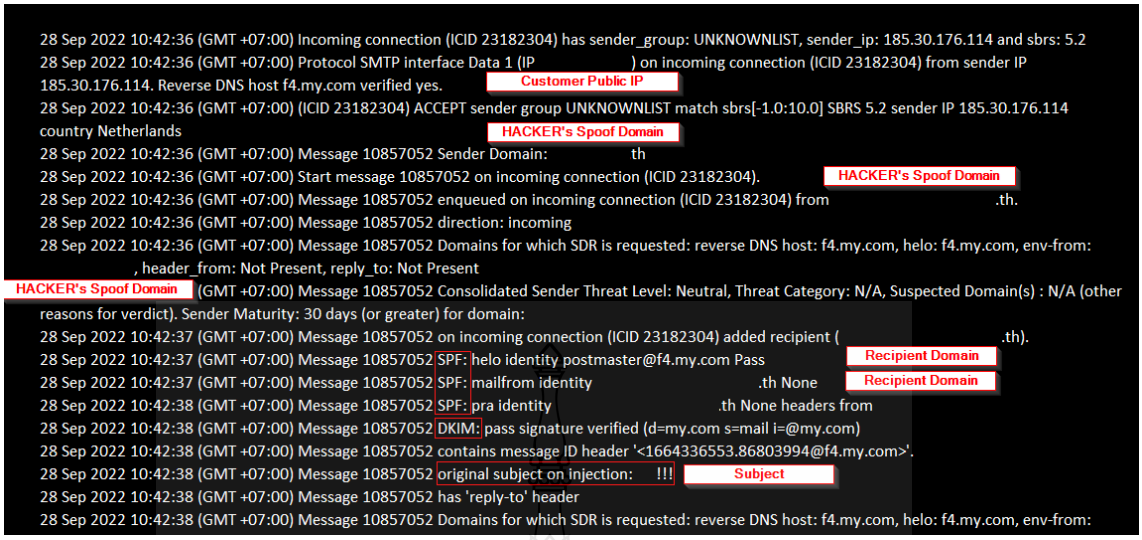
เดิมทางองค์กรแห่งนี้ได้ให้เจ้าหน้าที่ IT Administrator ทำการตั้งค่าการคัดกรองอีเมลที่ไม่ปลอดภัย (Threat อีเมล) บนระบบอีเมล server แต่ก็ไม่สามารถป้องกัน Threat อีเมลได้ ต่อมาทางองค์กรได้ทำการติดตั้งระบบ Email Security Gateway เพื่อนำมาคัดกรอง Threat อีเมลก่อนที่ระบบอีเมล server จะนำอีเมลส่งต่อไปยังผู้ใช้งาน โดยระบบ Email Security Gateway นี้ สามารถคัดแยก Threat อีเมลได้ในทุกประเภทของการโจมตีทางด้านอีเมลตามที่ได้กล่าวมาข้างต้น ยกเว้นแต่การโจมตีโดย Spoof อีเมลหรือ Fraud อีเมล



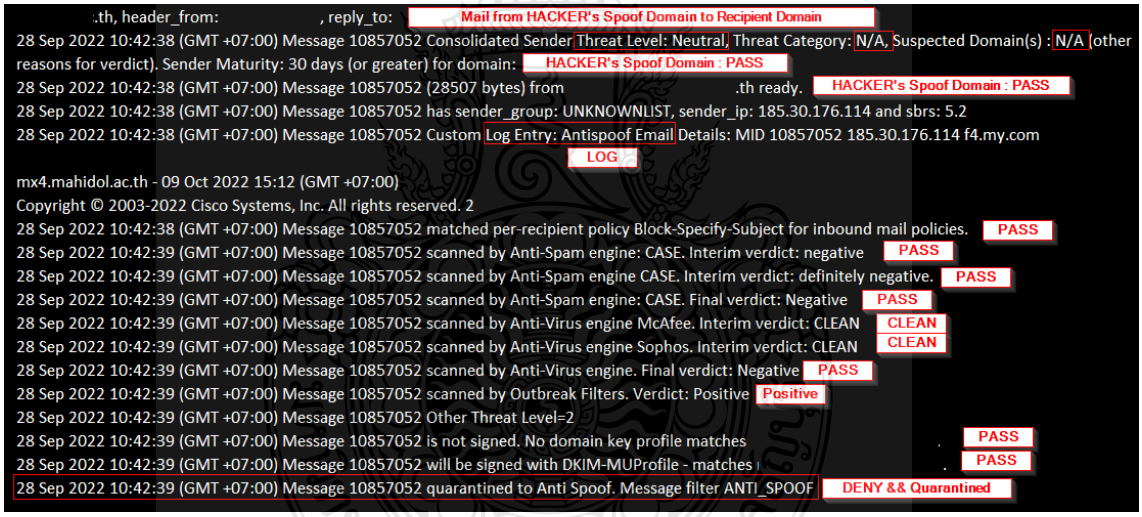
Message Details	
Envelope and Header Summary	
Received Time:	28 Sep 2022 10:42:36 (GMT +07:00)
MID:	10857052
Message Size:	27.84 (KB)
Subject:	!!!
Envelope Sender:	[redacted]th HACKER's SPOOF Domain
Envelope Recipients:	[redacted]th Recipient Domain
Message ID Header:	<1664336553.86803994@f4.my.com>
SMTP Auth User ID:	N/A
Attachments	N/A
Sending Host Summary	
Reverse DNS Hostname:	f4.my.com (verified)
IP Address:	185.30.176.114 Hacker's location
SBRS Score:	5.2

รูปที่ 3.14 ตัวอย่างรายละเอียดของ Email Header จากอุปกรณ์ Email security gateway

เมื่อทำการทดสอบ Script ที่ได้พัฒนาขึ้นมาใน Test Environment เรียบร้อยแล้ว จึงนำมาตั้งค่าบนอุปกรณ์ Email security gateway ขององค์กรแห่งนี้และติดตามผลเป็นระยะเวลา 120 วัน พบว่าอุปกรณ์นี้สามารถคัดแยก Spoof อีเมลได้อย่างมีประสิทธิภาพ



รูปที่ 3.15 Payload Spoof อีเมลที่ถูกตรวจจับได้โดย T-Antispoof Algorithm



รูปที่ 3.15 Payload Spoof อีเมลที่ถูกตรวจจับได้โดย T-Antispoof Algorithm (ต่อ)

บทที่ 4
ผลการวิจัยและการวิเคราะห์

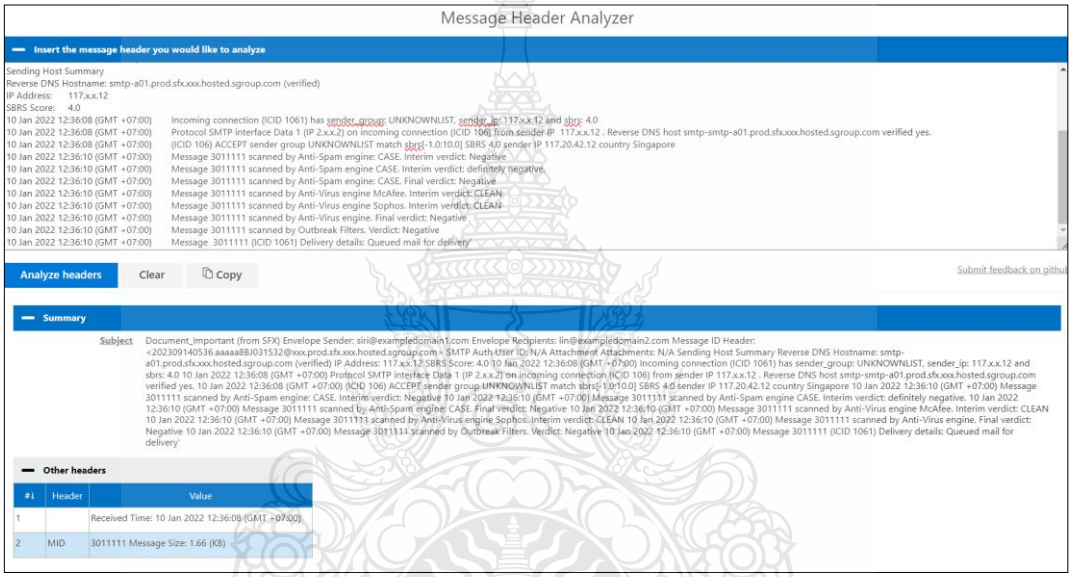
4.1 บทนำ

อุปกรณ์อีเมล Gateway ที่ใช้ในการศึกษาในที่นี้จะใช้เป็น Cisco อีเมล Gateway ภายใต้ระบบการใช้งานอีเมล server แบบ On premise ซึ่งยังเป็นที่นิยมในองค์กรรัฐบาลของหลายประเทศที่ยังไม่มีงบประมาณในการใช้งานอีเมล server แบบ Cloud โดยการคัดแยกอีเมลของ Cisco อีเมล Gateway ในการตั้งค่าแบบมาตรฐานปกติของอุปกรณ์ จะไม่สามารถคัดแยก Spoof อีเมลได้เลย เนื่องด้วยเทคโนโลยีของอุปกรณ์ Cisco อีเมล Gateway หรืออุปกรณ์อีเมล Gateway ของผู้ผลิตรายอื่นๆ ในปัจจุบันยังไม่มีความสามารถในการป้องกัน Spoof อีเมลได้ด้วย Feature ของอุปกรณ์เอง งานวิจัยนี้ได้ทำการศึกษาการรับอีเมลขององค์กรราชการแห่งหนึ่งในประเทศไทยพบว่า ตั้งแต่เดือนมกราคมถึงเดือนมิถุนายน มีอีเมลส่งเข้ามาประมาณ 33 ล้านฉบับ เมื่อตรวจสอบรายงานบนอุปกรณ์ Cisco อีเมล Gateway พบว่าสามารถคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ประมาณ 30 ล้านฉบับ คิดเป็น 93 เปอร์เซ็นต์ และที่เหลืออีก 7 เปอร์เซ็นต์เป็นอีเมลที่ถูกระบุว่าปลอดภัย อุปกรณ์นี้จึงทำการ Forward อีเมลเหล่านี้ไปยังผู้ใช้งานต่างๆ

อย่างไรก็ตามเราได้รับเรื่องร้องเรียนจากผู้ใช้งานว่าได้รับอีเมลที่เป็นภัยคุกคาม โดยอีเมลฉบับนั้นถูกส่งมาจากอีเมลของผู้ใช้งานเอง หรือที่เรียกว่า Spoof อีเมลเนื้อหาในอีเมลได้แจ้งข้อความจากผู้ไม่หวังดีว่าสามารถเข้าควบคุมเครื่องคอมพิวเตอร์ของผู้ใช้งานท่านนี้ได้ทุกอย่างแล้ว รวมถึงยังติดตามพฤติกรรมการใช้งานอินเตอร์เน็ตอีกด้วย และยังได้รับเรื่องร้องเรียนจากผู้ใช้งานรายอื่นว่าได้รับอีเมลที่ส่งจากอีเมลของตัวเองซึ่งเนื้อหาและไฟล์ที่แนบมาดูเหมือนอีเมลปกติที่ผู้ใช้งานรับส่งกัน แต่ทว่าทางผู้ใช้งานไม่ได้ทำการส่งอีเมลฉบับนั้นเข้ามาที่อีเมลตัวเองเลย

4.2 ผลการตรวจสอบช่องโหว่จากการใช้งานไดอะแกรมแบบดั้งเดิม

หากทำการตรวจสอบไปยังอุปกรณ์ Cisco อีเมล Gateway จะพบว่าอีเมลเหล่านั้นส่งมาจาก IP Address ที่เป็นของต่างประเทศ เมื่อทำการตรวจสอบ Header ของอีเมลที่ถูกระบุว่าปลอดภัย ดังรูปที่ 4.1 โดยละเอียดพบว่า มีอีเมลในลักษณะนี้เป็นจำนวนมาก ทำให้เราพบช่องโหว่ของอุปกรณ์นี้ว่าไม่สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้ ดังนั้นเราจึงคิดค้น Script T-Antispoof ขึ้นมาเพื่อช่วยเพิ่มประสิทธิภาพของอุปกรณ์ Cisco อีเมล Gateway นี้ให้สามารถคัดแยกอีเมลที่เป็นภัยคุกคามในรูปแบบ Spoof อีเมลได้



รูปที่ 4.1 การวิเคราะห์ Header ของ Spoof อีเมล

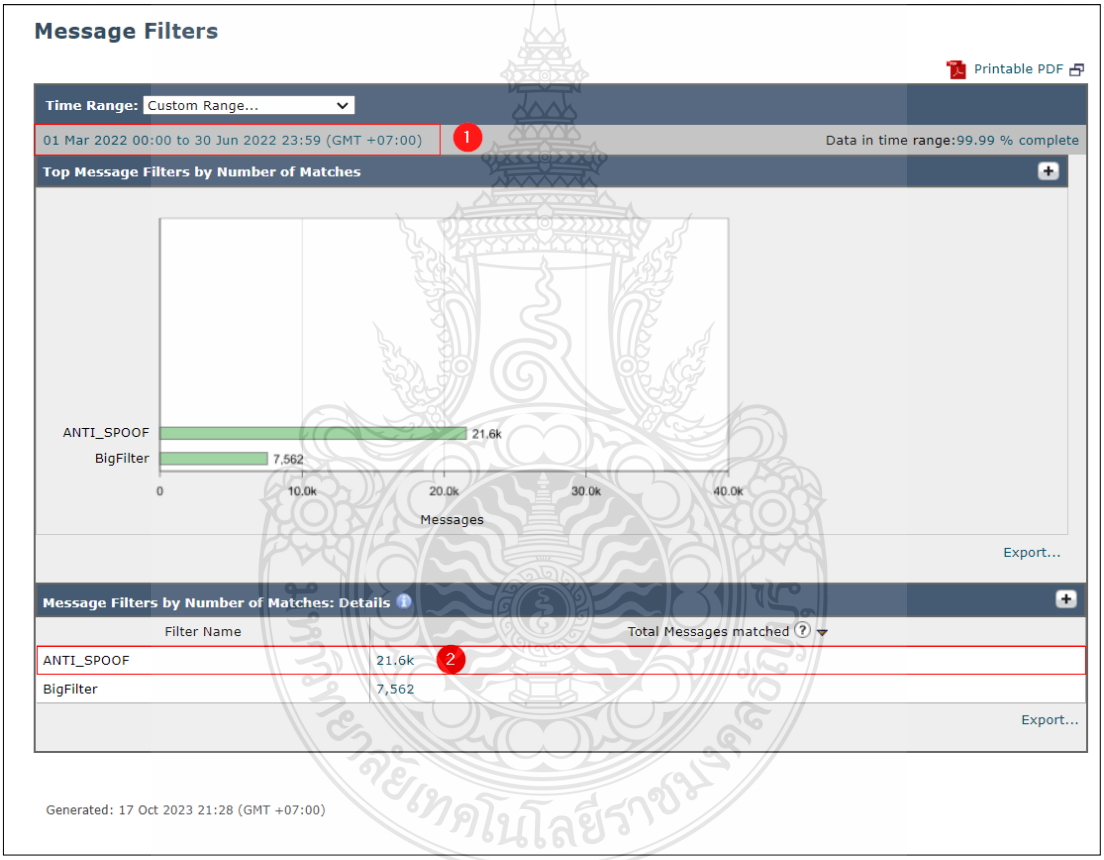
4.3 ผลการตรวจสอบช่องโหว่บนอุปกรณ์ Email Security Gateway จากไดอะแกรมแบบ T-Antispoof Algorithm

เมื่อทำการ Implement Script จากบทที่ 3 บนอุปกรณ์ Cisco อีเมล Gateway นี้แล้ว และทำการติดตามผลเป็นระยะเวลา 120 วัน ซึ่งจะได้ผลรับดังตารางที่ 4.1 โดยมีรายละเอียดมีดังต่อไปนี้

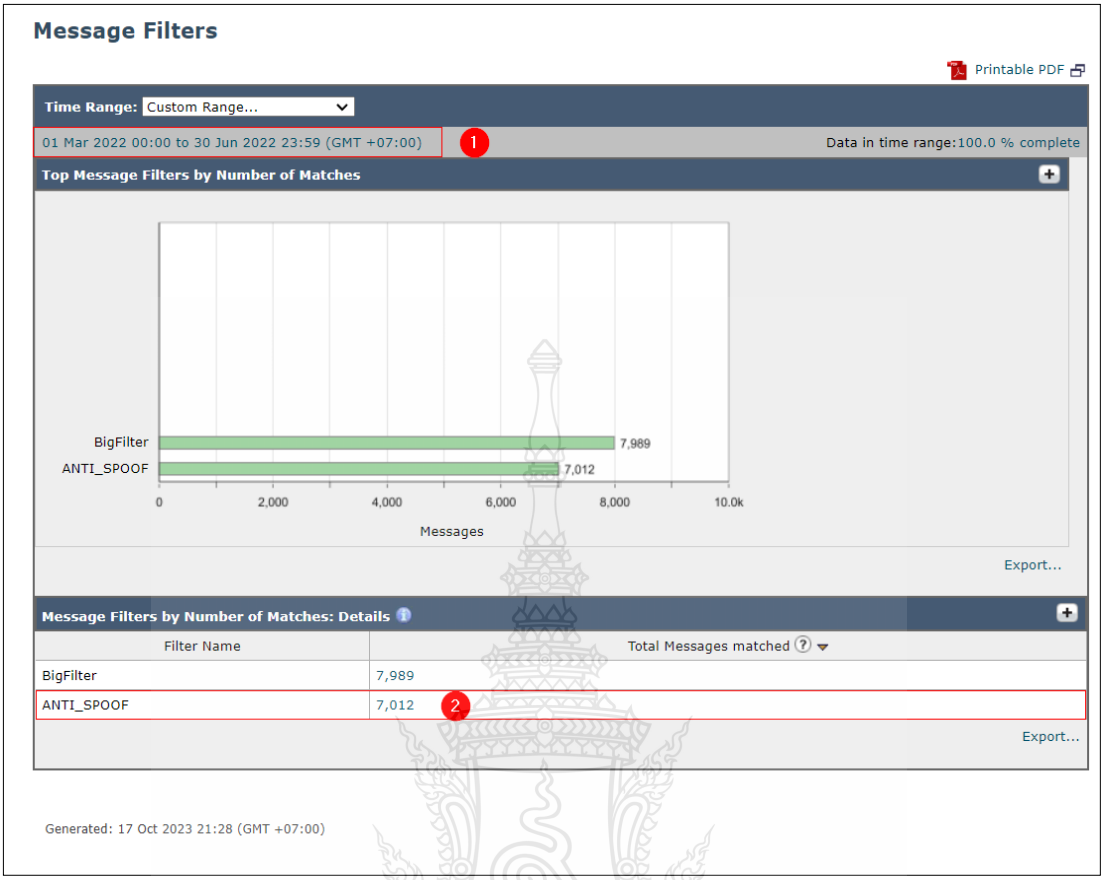
1) เดือนมกราคม มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 3,620,268 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 3,012,785 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 607,483 ฉบับ และยังไม่สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้เลย เนื่องจากยังไม่ได้ทำการติดตั้ง Script T-Antispoof

2) เดือนกุมภาพันธ์ มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 2,854,832 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 2,391,540 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 463,292 ฉบับ และยังไม่สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้เลย เนื่องจากยังไม่ได้ทำการติดตั้ง Script T-Antispoof

3) เดือนมีนาคม มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 4,918,557 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 4,527,650 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 390,907 ฉบับ และสามารถคัดแยกอีเมลที่เป็น Spoof อีเมลออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัยได้ หลังจากทำการติดตั้ง Script T-Antispoof 7,153 ฉบับ



รูปที่ 4.2 จำนวน Spoofing Email ที่คัดแยกได้หลังจากติดตั้ง T-Antispoof Algorithm บนอุปกรณ์ Email security gateway ตัวที่ 1



รูปที่ 4.3 จำนวน Spoofing Email ที่คัดแยกได้หลังจากติดตั้ง T-Antispoof Algorithm บนอุปกรณ์ Email security gateway ตัวที่ 2

4) เดือนเมษายน มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 8,696,700 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 8,391,525 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 305,175 ฉบับ และสามารถคัดแยกอีเมลที่เป็น Spoof อีเมลออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัยได้ หลังจากทำการติดตั้ง Script T-Antispoof 6,329 ฉบับ

5) เดือนพฤษภาคม มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 6,113,675 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 5,770,549 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 343,126 ฉบับ และสามารถคัดแยกอีเมลที่เป็น Spoof อีเมลออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัยได้ หลังจากทำการติดตั้ง Script T-Antispoof 7,281 ฉบับ

6) เดือนมิถุนายน มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 6,902,249 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 6,539,283 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 362,966 ฉบับ และ

สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัยได้ หลังจากทำการติดตั้ง Script T-Antispoof 7,849 ฉบับ

ตารางที่ 4.1 ผลสรุปการออกแบบและติดตั้ง T-Antispoof Algorithm บนอุปกรณ์ Email Security Gateway

เดือน	อีเมลที่ส่งเข้ามายังโดเมนนี้	อีเมลที่ถูกระบุว่าไม่ปลอดภัย	อีเมลที่ถูกระบุว่าปลอดภัย	อีเมลที่ถูกคัดแยกว่าเป็น Spoofing อีเมล
1. มกราคม	3,620,268	3,012,785	607,483	0
2. กุมภาพันธ์	2,854,832	2,391,540	463,292	0
3. มีนาคม	4,918,557	4,527,650	390,907	7,153
4. เมษายน	8,696,700	8,391,525	305,175	6,329
5. พฤษภาคม	6,113,675	5,770,549	343,126	7,281
6. มิถุนายน	6,902,249	6,539,283	362,966	7,849
รวมทั้งสิ้น	33,106,281	30,633,332	2,472,949	28,612

โดยสรุปนับตั้งแต่เดือนมกราคม จนถึงเดือนมิถุนายน เป็นเวลา 240 วัน มีอีเมลที่ถูกส่งเข้ามายังโดเมนนี้ 33,106,281 ฉบับ อุปกรณ์ทำการคัดแยกอีเมลที่ไม่ปลอดภัยออกไปได้ 30,633,332 ฉบับ และระบุว่าเป็นอีเมลที่ปลอดภัย 2,472,949 ฉบับ และสามารถคัดแยกอีเมลที่เป็น Spoof อีเมลออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัยได้ หลังจากทำการติดตั้ง Script T-Antispoof 28,612 ฉบับ จะพบว่าการติดตั้ง Script T-Antispoof นั้นสามารถทำการคัดแยกอีเมลที่เป็นประเภท Spoof อีเมลได้จริง

จากรูปที่ 4.4 จะแสดงให้เห็นว่าตัวเลขของการคัดแยกอีเมลที่เป็น Spoof อีเมลนั้นมีการเพิ่มขึ้นจากก่อนหน้านี้ที่ยังไม่มีการติดตั้ง Script T-Antispoof ในเดือนมกราคม และเดือนกุมภาพันธ์ ซึ่งตัวเลข Spoof อีเมลที่คัดแยกได้จะเป็นศูนย์ฉบับ แต่นับจากเดือนมีนาคมเป็นต้นไปจะเห็นได้ว่าอุปกรณ์ Email Security Gateway นี้ สามารถคัดแยกอีเมลที่เป็นประเภท Spoof อีเมลได้ ซึ่งเป็นผลมาจากการติดตั้ง Script T-Antispoof เพิ่มเข้าไปที่อุปกรณ์นี้ โดยจำนวนของการ Spoof อีเมลที่คัดแยกได้มีดังนี้

1) เดือนมกราคม ยังไม่สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้เลย เนื่องจากยังไม่ได้ทำการติดตั้ง Script T-Antispoof

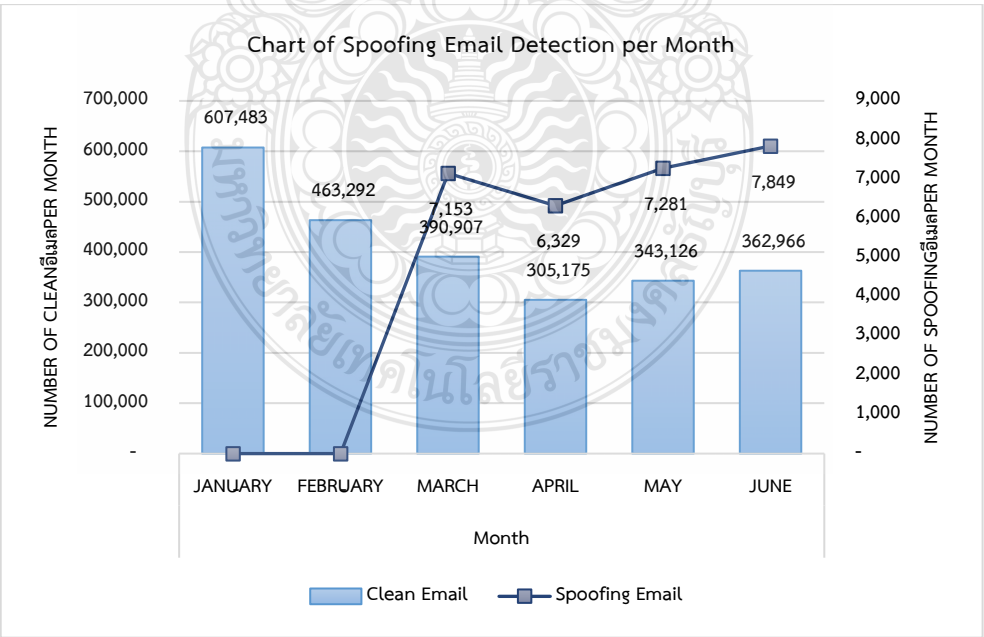
2) เดือนกุมภาพันธ์ ยังไม่สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้เลย เนื่องจากยังไม่ได้ทำการติดตั้ง Script T-Antispoof

3) เดือนมีนาคม หลังจากทำการติดตั้ง Script T-Antispoof สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้จำนวน 7,153 ฉบับ โดยคัดแยกออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัย 390,907 ฉบับ ซึ่งคิดเป็น 1.83 เปอร์เซ็นต์

4) เดือนเมษายน หลังจากทำการติดตั้ง Script T-Antispoof สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้จำนวน 6,329 ฉบับ โดยคัดแยกออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัย 305,175 ฉบับ ซึ่งคิดเป็น 2.07 เปอร์เซ็นต์

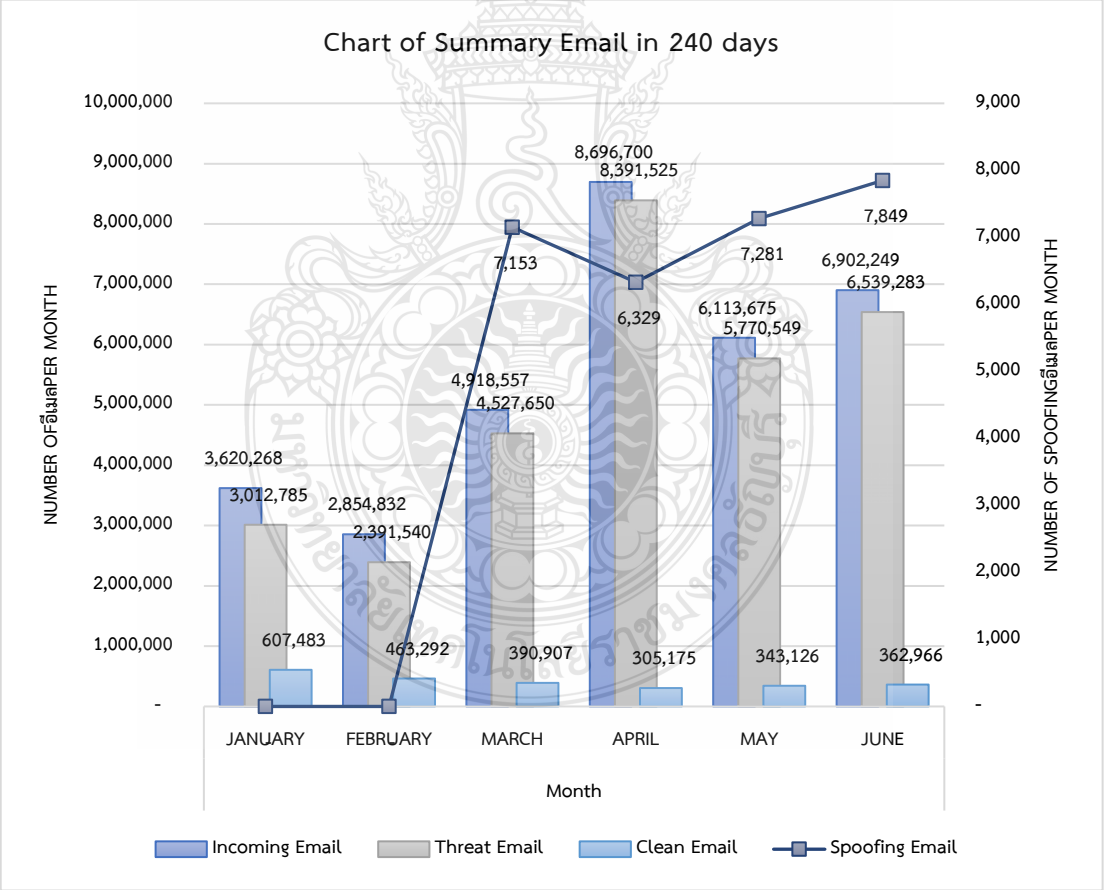
5) เดือนพฤษภาคม หลังจากทำการติดตั้ง Script T-Antispoof สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้จำนวน 7,281 ฉบับ โดยคัดแยกออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัย 343,126 ฉบับ ซึ่งคิดเป็น 2.12 เปอร์เซ็นต์

6) เดือนมิถุนายน หลังจากทำการติดตั้ง Script T-Antispoof สามารถคัดแยกอีเมลที่เป็น Spoof อีเมลได้จำนวน 7,849 ฉบับ โดยคัดแยกออกจากอีเมลที่อุปกรณ์ระบุว่าปลอดภัย 362,966 ฉบับ ซึ่งคิดเป็น 2.16 เปอร์เซ็นต์



รูปที่ 4.4 กราฟแสดงการเพิ่มขึ้นของ Spoof อีเมลที่คัดแยกได้หลังจากติดตั้ง Script T-Antispoof

สรุปได้ว่าเมื่อทำการติดตั้ง Script T-Antispoof แล้ว สามารถเพิ่มประสิทธิภาพของ Email Security Gateway ในการคัดแยกอีเมลที่ไม่ปลอดภัยได้จริง ดังแสดงในรูปที่ 4.5 ซึ่งคือภาพรวมของการคัดแยกอีเมลของอุปกรณ์นี้ในระยะเวลา 240 วัน จะเห็นได้ว่าในช่วง 2 เดือนแรก คือเดือนมกราคม และเดือนกุมภาพันธ์จะเป็นช่วงที่ยังไม่ได้ติดตั้ง Script นี้เข้าไป เนื่องจากอยู่ในระหว่างการเก็บข้อมูลเพื่อนำไปสู่การคิดค้นในแนวทางในการตรวจตัดแยก Spoof อีเมลที่ทางหน่วยงานนี้ถูกโจมตีด้วยอีเมลประเภทนี้เป็นจำนวนมาก เมื่อรวบรวมข้อมูลและนำมาวิเคราะห์พฤติกรรมของการโจมตีด้วย Spoof อีเมลแล้ว จึงนำไปสู่การพัฒนา Script นี้ขึ้นมาเพื่อใช้ในการตรวจคัดแยกอีเมลที่เป็น Spoof อีเมลนี้โดยเฉพาะ ผลที่ได้คือ อุปกรณ์นี้มีประสิทธิภาพเพิ่มขึ้นจริงจากการตรวจคัดแยก Spoof อีเมลที่ไม่สามารถทำได้เลยในตอนแรก โดยประสิทธิภาพเพิ่มขึ้นเป็นจาก 0 ฉบับ เป็น 7,153 ฉบับ ในเดือนแรกที่มีการติดตั้ง Script นี้ และยังสามารถตรวจจับ Spoof อีเมลได้ตลอดในช่วงเดือนต่อๆ มาจะดังแสดงในกราฟภาพรวมในรูปที่ 4.5



รูปที่ 4.5 ภาพรวมของการตรวจคัดแยกอีเมลโดย Email Security Gateway ใน 240 วัน

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

จากการศึกษาและวิเคราะห์รูปแบบการโจมตีทางด้านอีเมลในลักษณะของการทำ Email Spoof Attack เป็นเวลา 240 วันตั้งแต่ วันที่ 1 มกราคม 2022 จนถึง วันที่ 30 มิถุนายน 2022 พบว่ามี Email Spoof Attack เป็นจำนวน 28,612 ฉบับ ในการใช้งาน อุปกรณ์ Email Security Gateway เพียงอย่างเดียวไม่สามารถคัดแยก Email Spoof Attack ได้

งานวิจัยนี้ได้พัฒนา T-Antispoof Algorithm ขึ้นมาเพื่อคัดแยกการโจมตีแบบ Email Spoof Attack ร่วมกับ Email Security Gateway โดยมีประสิทธิภาพในการตรวจสอบช่องโหว่ 99.99% ซึ่งเป็นไปตามวัตถุประสงค์และขอบเขตของงานวิจัยที่ได้ตั้งไว้ ซึ่งสามารภนำ T-Antispoof Algorithm ไปใช้ประโยชน์ได้ดังต่อไปนี้

1. เพื่อเพิ่มประสิทธิภาพในการคัดกรองภัยคุกคามในรูปแบบอีเมล Attack บนอุปกรณ์อีเมล server และ Email Security Gateway

2. เพื่อสร้างองค์ความรู้และความเข้าใจให้กับบุคลากรด้านไอทีขององค์กรทั้งภาครัฐและภาคเอกชนในการทำงานป้องกันการโจมตีทางด้าน Cybersecurity โดยเฉพาะในส่วนของอีเมล Attack ซึ่งเป็นช่องทางหลักที่ผู้โจมตีในทุกระดับเลือกใช้เป็นเครื่องมือในการทำลายและหลอกลวงผู้ใช้งาน

หากไม่มีการใช้งาน T-Antispoof Algorithm บนอุปกรณ์ Email Security Gateway ก่อให้เกิดความเสี่ยงที่จะสร้างความเสียหายให้กับองค์กร จะเห็นได้ว่า Script ที่เราทำการ Implement นั้น สามารถเพิ่มประสิทธิภาพของการคัดแยกอีเมลที่เป็นภัยคุกคามให้กับอุปกรณ์นี้อีกประมาณ 50-60 เปอร์เซ็นต์ โดยคิดจากอีเมลที่เข้าทั้งหมดจำนวน 240 วัน จากเดิมที่ไม่สามารถตรวจจับอีเมลที่เป็นประเภท Spoof อีเมลได้เลย ทำให้เกิดความเสียหายกับองค์กรในวงกว้าง มีผู้ใช้งานหลายรายที่ได้รับอีเมลที่เป็น Spoof อีเมลและบางรายถูกผู้ไม่หวังดีเข้าควบคุมเครื่องคอมพิวเตอร์ได้ทั้งหมด สามารถเข้าถึงข้อมูลในเครื่อง เข้าถึงกล้องถ่ายภาพ และยังรวมไปถึงการติดตามการใช้งานอินเตอร์เน็ตอีกด้วย ทำให้เกิดความไม่ปลอดภัยทางด้านไซเบอร์กับองค์กรนี้ เมื่อทำการ Implement Script นี้เข้าไปแล้วพบว่าสามารถคัดแยก Spoof อีเมลได้เป็นจำนวนมาก เพิ่มความปลอดภัยให้กับผู้ใช้งานในองค์กรมากยิ่งขึ้น แต่ถึงอย่างไรก็ตามผู้ไม่หวังดียังคงพยามคิดหาวิธีการโจมตีทางด้านไซเบอร์ใหม่ๆ เพื่อโจมตีผู้ใช้งานเข้ามาเรื่อย ๆ ดังนั้นผู้ใช้งานก็ต้องตระหนักในการใช้งานทั้งอีเมลและอินเตอร์เน็ตให้มากยิ่งขึ้นด้วย เพราะไม่มีอุปกรณ์หรือวิธีการใดที่จะป้องกันภัยคุกคามทางด้านไซเบอร์ได้ร้อยเปอร์เซ็นต์

5.1 ข้อเสนอแนะและการพัฒนาต่อยอดงานวิจัย

1. ข้อเสนอแนะในการป้องกันตัวเองจากการโจมตีทางด้านความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอีเมลใช้ระบบอีเมลที่มีความมั่นคงปลอดภัย เลือกระบบอีเมลที่มีการยืนยันตัวตนผ่านหลายขั้นตอน (Multi-Factor Authentication, MFA) และใช้ระบบการตรวจจับสแปมและมัลแวร์

2. ข้อความแจ้งเตือน (Alerts) ตั้งค่าข้อความแจ้งเตือนในกรณีที่มีการเข้าถึงอีเมลจากตำแหน่งที่ไม่ปกติ หรือการทำธุรกรรมที่ผิดปกติ

3. การอบรมและการสร้างความตื่นตัวในการรับมือกับภายคุกคาม ให้บุคลากรได้รับการอบรมเกี่ยวกับความปลอดภัยในอีเมล และทราบถึงประเภทของการโจมตีที่อาจเกิดขึ้น เช่น ปลอมอีเมล (Phishing), ประเภทของไฟล์ที่ไม่ควรเปิด หรือลิงค์ที่อาจเป็นอันตราย

4. ตรวจสอบที่อยู่อีเมลและลิงค์ อย่าเปิดไฟล์หรือลิงค์จากที่อยู่อีเมลที่ไม่รู้จักหรือไม่น่าเชื่อถือ และตรวจสอบที่อยู่ URL ให้ละเอียด หลีกเลี่ยงการคลิกลิงค์แบบย่อที่ไม่สามารถตรวจสอบได้

5. อัปเดตแพทช์และซอฟต์แวร์ อัปเดตระบบปฏิบัติการ, ซอฟต์แวร์และแอปพลิเคชันอยู่เสมอ เพื่อป้องกันช่องโหว่ที่อาจถูกใช้ในการโจมตี

6. ใช้ซอฟต์แวร์ Antivirus และ Firewall ติดตั้งและปรับปรุงซอฟต์แวร์ป้องกันไวรัส และใช้ Firewall เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

7. การสำรองข้อมูล สำรองข้อมูลที่สำคัญอยู่เสมอ กรณีที่อีเมลของคุณถูกโจมตีและข้อมูลถูกลบหรือถูกเข้ารหัส

8. รีวิวประจำปี ทบทวนและปรับปรุงนโยบายความปลอดภัยประจำปี และให้ความสำคัญกับการติดตามเหตุการณ์และข้อความที่มีเนื้อหาที่สำคัญในด้านความปลอดภัย

9. การติดตามและรายงาน สร้างระบบการติดตามและรายงานเหตุการณ์เฉพาะที่เกี่ยวข้องกับความปลอดภัยของอีเมล เพื่อสร้างข้อมูลสถิติและเสริมสร้างการตัดสินใจที่มีประสิทธิภาพ

การปฏิบัติตามข้อเสนอแนะดังกล่าวจะเพิ่มโอกาสในการป้องกันตัวเองจากการโจมตีทางด้านความปลอดภัยไซเบอร์ โดยเฉพาะในเรื่องของอีเมลอย่างมีประสิทธิภาพมากขึ้น

สรุป T-Antispoof Algorithm ได้ถูกพัฒนาขึ้นภายในข้อขอบเขตของการวิจัยซึ่งส่วนใหญ่ใช้การบริหารจัดการอุปกรณ์ในส่วนที่เป็น On-premise Infrastructure ซึ่งในอนาคตจากผลการสำรวจขององค์กร Gartner พบว่าบริษัททั้งภาครัฐและเอกชนมีแนวโน้มที่จะใช้งาน Cloud Solution มากขึ้น จึงเป็นไปได้ว่าอุปกรณ์ในส่วนของอีเมล server และ Email Security Gateway จะถูกพัฒนาไปใช้บน Cloud Platform เช่น Google Cloud, Microsoft Cloud (Azure) และ AWS Cloud จากสาเหตุดังกล่าวทำให้ภัยคุกคามทางด้านอีเมล attack ทวีความรุนแรงมากขึ้นภายใต้การใช้งานที่หลากหลาย

รูปแบบมากขึ้น ผู้ศึกษาสามารถนำ T-Antispoof Algorithm ไปพัฒนาต่อยอดให้ครอบคลุมการป้องกันอีเมล Attack ทั้งบน Cloud Environment และ Onpremise Environment

บรรณานุกรม

[1] Feinler, Elizabeth; Vittal, John (2022-07-01). "Email Innovation Timeline" (PDF). Computer History Museum. Retrieved 2023-08-18. pp.12-20

[2] L. Ceci. (2023, Aug. 22). Number of sent and received e-mails per day worldwide from 2017 to 2026 [Online]. Available: https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ [Accessed: 7-August-2023]

[3] S. Shukla, M. Misra, and G. Varshney, “Identification of spoofed emails by applying email forensics and memory forensics,” 10th Int’l Conf. on Comm. and Net. Secu., 2020. Pp.1

[4] D. Mooloo and T. P. Fowdur. 2013. An SSL-based client-oriented anti-spoofing email application. In 2013 Africon. 1–5. https://doi.org/10.1109/AFRCON.2013.6757757

[5] H. Hu and G. Wang, “End-to-end measurements of email spoofing attacks,” in Proc. 27th USENIX Security Symp., 2018, pp. 1095–1112.

[6] จตุชัย แพงจันทร์, “Master in Security 3rd Edition: Endpoint Security: Windows Security,” นนทบุรี: ไอดีซีฯ, สิงหาคม 2558, pp.499-501.

[7] H. Hu, P. Peng and G. Wang, "Towards Understanding the Adoption of Anti-Spoofing Protocols in email Systems," 2018 IEEE Cybersecurity Development (SecDev), Cambridge, MA, USA, 2018, pp. 94-101, doi: 10.1109/SecDev.2018.00020.

[8] S. Kitterman, “Sender policy framework (spf),” ser. RFC7208, 2014, https://tools.ietf.org/html/rfc7208.

[9] D. Crocker, T. Hansen, and M. Kucherawy, “Domainkeys identified mail (dkim) signatures,” ser. RFC6376, 2011.

[10] M. Kucherawy and E. Zwicky, “Domain-based message authentication, reporting, and conformance (dmarc),” ser. RFC7489, 2015, https://tools.ietf.org/html/rfc7489.

บรรณานุกรม (ต่อ)

[11] J. Ramprasath, S. Priyanka, R. Manudev and M. Gokul, "Identification and Mitigation of Phishing email Attacks using Deep Learning," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 466-470, doi: 10.1109/ICACITE57410.2023.10182911.

[12] S. Maroofi, M. Korczyński, A. Hölzel and A. Duda, "Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3184-3196, Sept. 2021, doi: 10.1109/TNSM.2021.3065422.

[13] N. T N, D. Bakari and C. Shukla, "Business E-mail Compromise — Techniques and Countermeasures," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 217-222, doi: 10.1109/ICACITE51222.2021.9404587.

.

ภาคผนวก

ภาคผนวก ก
ผลงานตีพิมพ์และเผยแพร่

1. วรวุฒิ จำปาหอม และคณะ, Design and Implementation of Spoofing Email Detection for Email Security Gateway


CONFERENCE PROCEEDINGS
EMSES 2022
CARBON FREE
15th Eco-Energy and Materials Science and Engineering Symposium
Organized by
Co-organized by
Supported by
Sponsors by
Special issue on Materials and Energy in Negative and Neutral Carbon Society
7 - 10 DECEMBER 2022
DUSIT THANI PATTAYA
Chonburi, THAILAND
MRS-Thailand
NMT
METTLER TOLEDO
ESSOM
ISO 9001
AD
CARBON NEUTRALITY
CO2

Proceedings

15th Eco-Energy and Materials Science and Engineering Symposium

(EMSES 2022)

Conference Topics:

- Materials Science and Nano Technology (MN)
- Energy Technology (ET)
- Environmental Science (ES)
- Energy Society and Sustainability (ESS)
- Electric Vehicle Technology (EV)
- Carbon Capture and Utilization (CCU)
- Nuclear Technology (NT)
- Related Topics in Material and Energy (ME)

Special Session:

- Generation and Application of High-power Radiation Sources (RS)
- Drone (DR)
- Hospitality and Tradition (HT)

Organized by

Rajamangala University of Technology Thanyaburi, Thailand

Kyoto University, Japan

Co-Organized by

Silpakorn University, Thailand

Supported by

The Materials Research Society of Thailand

Thailand Chapter – The American Ceramic Society

Association of Rajamangala Network of Manufacturing and Management Technology

EMSES Steering Committee

Honorary Advisory Chair:
Sommai Pivsa-Art (RMUTT, Thailand)

Honorary Advisory Co-Chair:
Hideaki Ohgaki (Kyoto University, Japan)

General Chair:
Krischonme Bhumkittipich (RMUTT, Thailand)

General Co-Chair:
Sorapong Pavasupree (RMUTT, Thailand)

International Advisory Committee:
Hideaki Ohgaki (Kyoto University, Japan)
Sommai Pivsa-Art (RMUTT, Thailand)
Hiroyuki Hama (Tohoku University, Japan)
Ken Miyata (Yamagata University, Japan)
Sadao Miura (Tohoku University, Japan)
Wisanu Pecharapa (KMITL, Thailand)
Toshiya Muto (Tohoku University, Japan)
Tomoko Ota (Chuo Business Group, Japan)
Jakrapong Kaewkhao (NPRU, Thailand)
Pastraporn Thipayasothorn (KMITL, Thailand)
Trinet Yingsamphancharoen (KMUTNB, Thailand)
Nipon Ketjoy (Naresuan University, Thailand)
Akihiko Goto (Osaka Sangyo University, Japan)
Naoki Sugiyama (Kyoto Institute of Technology, Japan)
Suthum Patumsawad (KMUTNB, Thailand)
Monchai Jitvisate (SUT, Thailand)
Sakhorn Rimjaem (Chiang Mai University, Thailand)
Sanchai Ramphueiphad (RMUTI, Thailand)
Hadarajah Mithulananthan (UQ, Australia)
Supakij Suttiruengwong (Silpakorn University, Thailand)

Technical Program Committee:
Chair:
Sumonman Niamlang (RMUTT, Thailand)

Co-Chairs:
Boonyang Plangklang (RMUTT, Thailand)
Hideaki Ohgaki (Kyoto University, Japan)

Technical Conference Committee:
Suchalinee Mathurosemontri (RMUTT, Thailand)
Nichanan Phansroy (RMUTT, Thailand)
Sirichai Dangeam (RMUTT, Thailand)
Boonyang Plangklang (RMUTT, Thailand)
Monthon Nawong (RMUTT, Thailand)
Sirichai Torsakul (RMUTT, Thailand)
Chatchai Veranitisagul (RMUTT, Thailand)
Sorapong Pavasupree (RMUTT, Thailand)
Anin Memon (RMUTT, Thailand)
Uthen Kamnarn (RMUTL, Thailand)
Monthon Nawong (RMUTT, Thailand)
Nitikorn Junhuathon (RMUTT, Thailand)

Suwat Sakulchat (RMUTSB, Thailand)
Watcharaphon Naktong (RMUTI, Thailand)

Publicity and Website Committee:
Nathabhat Phankong (RMUTT, Thailand)
Prusayon Nintanavongsa (RMUTT, Thailand)
Somchai Biansoongnern (RMUTT, Thailand)

Registration Committee:
Anin Memon (RMUTT, Thailand)
Weraporn Pivsa-Art (RMUTT, Thailand)
Suchalinee Mathurosemontri (RMUTT, Thailand)
Nichanan Phansroy (RMUTT, Thailand)

Financial Chair:
Sirichai Torsakul (RMUTT, Thailand)

Local Arrangement Committee:
Amnoiy Reungwaree (RMUTT, Thailand)
Narongchai O-Chareon (RMUTT, Thailand)
Sanidda Tiewtoy (RMUTT, Thailand)
Porakoch Sirisuwan (RMUTT, Thailand)

General Secretariat:
Nathabhat Phankong (RMUTT, Thailand)
Prusayon Nintanavongsa (RMUTT, Thailand)

List of Reviewers

Hideaki Ohgaki	Kyoto University, Japan
Hiroyuki Hama	Tohoku University, Japan
Hikaru Yoshida	Kumamoto Industrial Research Institute, Japan
Apirat Laobuthee	Kasetsart University, Thailand
Yuttana Kumsuwan	Chiang Mai University, Thailand
Nathabhat Phankong	Rajamangala University of Technology Thanyaburi, Thailand
Krischonme Bhumkittipich	Rajamangala University of Technology Thanyaburi, Thailand
Pimolpun Niamlang	Rajamangala University of Technology Rattanakosin, Thailand
Wissanu Charerntanom	Rajamangala University of Technology Isan, Thailand
Narongchai O-Charoen	Rajamangala University of Technology Thanyaburi, Thailand
Sumonman Niamlang	Rajamangala University of Technology Thanyaburi, Thailand
Sirichai Torsakul	Rajamangala University of Technology Thanyaburi, Thailand
Chatchai Veranitisagul	Rajamangala University of Technology Thanyaburi, Thailand
Sorapong Pavasupree	Rajamangala University of Technology Thanyaburi, Thailand
Anin Memon	Rajamangala University of Technology Thanyaburi, Thailand
Natee Srisawat	Rajamangala University of Technology Thanyaburi, Thailand
Sirichai Dangeam	Rajamangala University of Technology Thanyaburi, Thailand
Saichol Chudjuarjeen	Rajamangala University of Technology Krungthep, Thailand
Chokchai Chuenwattanapraniti	Burapha University, Thailand
Prusayon Nintanavongsa	Rajamangala University of Technology Thanyaburi, Thailand
Itarun Pitimon	Rajamangala University of Technology Thanyaburi, Thailand
Thanasin Bunnam	Rajamangala University of Technology Thanyaburi, Thailand
Sakhorn Rimjaem	Chiang Mai University, Thailand
Siriwan Pakluea	Chiang Mai University, Thailand
Araya Mungchamnankit	Rangsit University, Thailand
Atipong Bootchanont	Rajamangala University of Technology Thanyaburi, Thailand
Rattikarn Khankrua	Suranaree University of Technology, Thailand
Teerin Kongpun	Rajamangala University of Technology Rattanakosin, Thailand
Napaporn Phuangpornpitak	Kasetsart University, Thailand
Uthen Kamnarn	Rajamangala University of Technology Lanna, Thailand
Monthon Nawong	Rajamangala University of Technology Thanyaburi, Thailand
Nitikorn Junhuathon	Rajamangala University of Technology Thanyaburi, Thailand
Suwat Sakulchat	Rajamangala University of Technology Suvarnabhumi, Thailand
Watcharaphon Naktong	Rajamangala University of Technology Isan, Thailand
Nophawan Paradee	Rajamangala University of Technology Thanyaburi, Thailand
Prapita Thanarak	Naresuan University, Thailand
Nithiwatthn Choosakul	Rajamangala University of Technology Thanyaburi, Thailand
Sommai Pivsa-Art	Rajamangala University of Technology Thanyaburi, Thailand
Anyarat Watthanaphanit	Mahidol University, Thailand
Kulnida Taptim	Rajamangala University of Technology Rattanakosin, Thailand
Pramuk Unahalekhaka	Rajamangala University of Technology Suvarnabhumi, Thailand
Sarawut Jaiyen	Rajamangala University of Technology Thanyaburi, Thailand
Nophawan Paradee	Rajamangala University of Technology Thanyaburi, Thailand
Akapong Phunpueok	Rajamangala University of Technology Thanyaburi, Thailand
Chaiyan Chaiya	Rajamangala University of Technology Thanyaburi, Thailand
Teeranan Nongnual	Burapha University, Thailand
Chularat Iamsamai	Chulalongkorn University, Thailand
Manop Yamfang	Rajamangala University of Technology Thanyaburi, Thailand
Porakoch Sirisuwan	Rajamangala University of Technology Thanyaburi, Thailand
Bawornkit Nekhamanurak	Rajamangala University of Technology Rattanakosin, Thailand
Boonyang Plangklang	Rajamangala University of Technology Thanyaburi, Thailand
Rattikarn Khankrua	Silpakorn University, Thailand
Nu-orn Choothong	Rajamangala University of Technology Rattanakosin, Thailand
Nattaporn Khanoonkon	Kasetsart University, Thailand
Voranuch Thongpool	Rajamangala University of Technology Thanyaburi, Thailand
Sillawat Romphochai	Rajamangala University of Technology Thanyaburi, Thailand
Krawee Treeamnuk	Suranaree University of Technology, Thailand
Prachoom Khamput	Rajamangala University of Technology Thanyaburi, Thailand

Jatuphon Tangpagasit	Rajamangala University of Technology Thanyaburi, Thailand
Suchalinee Mathurosemontri	Rajamangala University of Technology Thanyaburi, Thailand
Pansa Liplap	Suranaree University of Technology, Thailand
Pinyo Puangmali	Chiang Mai University, Thailand
Nampueng Pangpaiboon	King Mongkut's University of Technology North Bangkok, Thailand

Conference Program of EMSES 2022

Time				
December 7, 2022				
13:00 – 16:00	Registration			
16:30 – 17:30	EMSES Committee Meeting			
December 8, 2022				
08:00 – 09:00	Registration			
09:00 – 09:30	Opening Ceremony (Napalai Ballroom B&C)			
09:30 – 10:30	Keynote Speaker (KS1): Functionalization-triggered Fractionation of Lignocellulosic Biomass to Afford Cellulose-, Hemicellulose-, and Lignin-based Functional Materials *Professor Dr. Hiroshi Kamitakahara* *Division of Forest and Biomaterials Science,* *Graduate School of Agriculture, Kyoto University, Japan*			
10:30 – 10:45	Coffee Break			
10:45 – 11:45	Keynote Speaker (KS2): Graphene Technology for Next Generation Energy Storage Devices *Dr. Adisorn Tuantranont* *(Acting) Assistant Director,* *National Science and Technology Development Agency (NSTDA), Thailand*			
12:00 – 13:00	Lunch (The Cascade Restaurant)			
Parallel Session				
Room	Dusit 1	Dusit 3	Dusit 4 – 5	Dusit 6 – 7
13:00 – 14:45	**Materials Science and Nano Technology I**	**Materials Science and Nano Technology II**	**Energy Society and Sustainability**	**Related Topics in Material and Energy I**
Paper ID	IN2, MN1, MN2, MN6, MN7, MN15	IN4, MN16, MN17, MN20, MN21, MN22	ESS1, ESS2, ESS3, ESS4, ESS6, ESS7, ESS8	ME1, ME2, ME3, ME4, ME5, ME6, ME7
Chair	Prof. Dr. Wisanu Pecharapa KMITL, Thailand	Assoc. Prof. Dr. Ken Miyata Yamagata University, Japan	Assoc. Prof. Dr. Pastraporn Thipayasothorn KMITL, Thailand	Assoc. Prof. Dr. Trinet Yingsamphancharoen KMUTNB, Thailand
Co-Chair	Assoc. Prof. Dr. Chaiyan Chaiya RMUTT, Thailand	Dr. Nichanan Phansroy RMUTT, Thailand	Asst. Prof. Dr. Bopit Chainok NPRU, Thailand	Asst. Prof. Dr. Prachoom Khamput RMUTT, Thailand
14:45 – 15:00	Coffee Break			
Room	Dusit 1	Dusit 3	Dusit 4 – 5	Dusit 6 – 7
15:00 – 16:30	**Materials Science and Nano Technology III**	**Environmental Science**	**Special Session: Generation and Application of High-power Radiation Sources I**	**Related Topics in Material and Energy II**
Paper ID	IN3, MN23, MN24, MN25, MN26	ES1, ES2, ES3, ES5, ES6	IN1, IN6, RS9, RS5, RS7, RS15	ME8, ME9, ME10, ME11, ME12, ME13
Chair	Assoc. Prof. Dr. Jakrapong Kaewkhao NPRU, Thailand	Asst. Prof. Dr. Nathabhat Phankong RMUTT, Thailand	Prof. Dr. Hideaki Ohgaki Kyoto University, Japan	Asst. Prof. Dr. Prusayon Nintanavongsa RMUTT, Thailand
Co-Chair	Asst. Prof. Dr. Anin Memon RMUTT, Thailand	Dr. Therakanya Sripho RMUTT, Thailand	Dr. Monchai Jitvisate SUT, Thailand	Asst. Prof. Dr. Teerapot Wessapan RMUTT, Thailand
16:30 – 18:00	Poster Session			
Paper ID	MN3, MN4, MN5, MN8, MN9, MN10, MN11, MN12, MN13, MN14, MN18, MN19, ET3, ET8, ET10, ET11, ET12, ET15, ET16, ET17, ET18, ES4, ESS5			
Chair	Prof. Dr. Hideaki Ohgaki (Kyoto University, Japan)			
Co-Chair	Assoc. Prof. Dr. Sorapong Pavasupree (RMUTT, Thailand)			
18:30 – 22:00	Banquet			

December 9, 2022				
Parallel Session				
Room	Dusit 1	Dusit 3	Dusit 4 – 5	Dusit 6 – 7
08:45 – 10:15	**Special Session: Generation and Application of High-power Radiation Sources II**	**Energy Technology I**	**Electric Vehicle Technology**	**Special Session: Drone and Special Session: Hospitality and Tradition I**
Paper ID	RS8, RS10, RS11, RS12, RS14, RS16	ET1, ET2, ET4, ET5, ET6, ET7,	EV1, EV2, EV3, EV4, EV5, EV6	IN8, DR1, DR2, DR3, HT1, HT2
Chair	Assoc. Prof. Dr. Sadao Miura Tohoku University, Japan	Dr. Sanchai Ramphueiphad RMUTI, Thailand	Asst. Prof. Dr. Sirichai Dangeam RMUTT, Thailand	Dr. Tomoko Ota Chuo Business Group, Japan
Co-Chair	Asst. Prof. Dr. Sakhorn Rimjaem Chiang Mai University, Thailand	Assoc. Prof. Dr. Nipon Ketjoy Naresuan University, Thailand	Asst. Prof. Dr. Monthon Nawong RMUTT, Thailand	Dr. Porakoch Sirisuwan RMUTT, Thailand
10:15 – 10:30	Coffee Break			
Room	Dusit 1	Dusit 3	Dusit 4 – 5	Dusit 6 – 7
10:30 – 12:15	**Special Session: Generation and Application of High-power Radiation Sources III**	**Energy Technology II**		**Special Session: Hospitality and Tradition II**
Paper ID	IN5, IN7, RS1, RS3, RS6, RS13, RS2, RS4	ET9, ET13, ET14, ET19, ET20		HT3, HT4, HT5, HT6, HT7, HT8, HT9
Chair	Prof. Dr. Hiroyuki Hama Tohoku University, Japan	Assoc. Prof. Dr. Suthum Patumsawad KMUTNB, Thailand		Asst. Prof. Dr. Narongchai O-Charoen RMUTT, Thailand
Co-Chair	Asst. Prof. Dr. Toshiya Muto Tohoku University, Japan	Asst. Prof. Dr. Winai Chanpeng RMUTT, Thailand		Dr. Nareerut Jariyapunya RMUTT, Thailand
12:15 – 13:15	Lunch (The Cascade Restaurant)			
13:15 – 14:15	Closing Ceremony (Napalai Ballroom B&C)			
14:15 – 14:35	Coffee Break			
December 10, 2022				
09:00 – 16:00	Excursion			

Remark: Please see the Paper ID in the Abstract Book.

Design and Implementation of Spoofing Email Detection for Email Security Gateway

Worawoot Jampahom, Prusayon Nintanavongsa*, and Itarun Pitimon
Department of Computer Engineering, Rajamangala University of Technology Thanyaburi, Pathum Thani, Thailand
Email: worawoot_j@en.rmutt.ac.th, prusayon.n@en.rmutt.ac.th, itarun.p@en.rmutt.ac.th

***Abstract*—Email is undeniable the major mean of communication in the present time, thanks to its low cost of operation and non-confrontational nature. However, email spoofing, a kind of attack on users that make them believed that an email is sent from trustworthy sender, starts growing exponentially. In this work, we propose a method to detect such spoof emails. The computer programming script is developed to verify whether the incoming email is sent by trustworthy sender. We implement the countermeasure for a period of six months and our method can intercept 30,633,332 unsafe emails out of the total 33,106,281 emails, a percentage of 92.53. Moreover, our method is capable of quarantining 10,008 spoofed emails out 2,472,949 safe emails, a percentage of 0.40. Lastly, our method boasts 100% email spoofing detection and all spoof emails destined to the organization are dropped.**

Keywords—email, spoofing, security, gateway.

I. Introduction

The history of email starts in 1960s, there are billions of emails sent daily. Email has not been designed with high security at the first place it was built with a concept that it must be easy to use and deploy in a computer system. That make email has many vulnerabilities in smtp protocol. There is a variety attack pattern on the computer system, but e-mail is still the number one threat vector. By 2021, there are approximately 319 billion of e-mails sent each day [1-3]. Email is still an easy method of attack that damage the network. The public email system is relatively easy to sign up. Hence, it can be used as a channel for attacking. According to the BBC, even tech companies such as Google, Facebook are also hit by email compromise, known as business email compromise.

Email originates in the 80's with the emerging of the Simple Mail Transfer Protocol (SMTP) and then the flourish of internet globally [4-5]. The email conversation between 2 stations is in the form of text message, comprising of 3 major parts: Mail User Agent (MUA) acting as an interface between user and email server, Email server which provides important services such as Mail Transfer Agent (MTA), and Domain Name System (DNS) server. When the email server is setup, it is necessary to assign the hostname, i.e., mail.example.com, to the email server and use it for the MX record on the DNS server by IP binding. Consequently, the email server can be accessed anywhere on the internet. The email exchange occurs as follows. Harry from the company A with the email address harry@example1.com wants to send an email to Jenny from the company B with the email address jenny@example2.com. Once Harry presses "send" button, MUA transfer the message to the email server through SMTP where the validity of the destination address is verified. If the destination address is valid, the location of the hostname of the MX record "example2.com" is queried. Upon the receipt of the location, the MTA in the sender's email server establishes the SMTP session to the receiver's email server which relays the message to Mail Delivery Agent (MDA) and the message is kept in Jenny's mailbox. Finally, Jenny can access her email through either Post Office Protocol (POP) or Internet Message Access Protocol (IMAP), depending on company's policy [6]. The process is illustrated in Fig. 1.

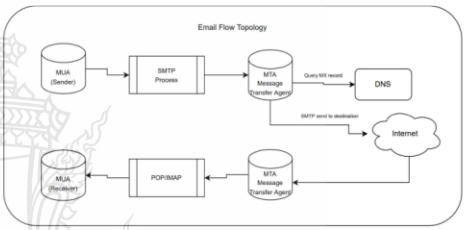


Fig. 1. Email sending process.

The aforementioned process only takes a second to accomplished. With this simple yet fast message exchange, email is the prominent channel for communication and so the malicious attacks from hackers. The damage incurred ranging from personal disturbance to financial loss in the enterprise level.

Email has been implemented and evolved for the past 50 years and currently can be used throughput the internet thanks to Hypertext Transfer Protocol (HTTP),Hypertext Transfer Protocol Secure (HTTPS) and SMTP. Consequently, there exists numerous vulnerabilities as email is designed for ease of use rather than security. The email vulnerability causes considerable damage [7] through various attacks such as virus, spam, fraudulence, spoofing, business compromise, and phishing. Phishing email results in over 2.3 billion dollars in financial damage between 2013-2016 [8] while business email compromise costs over 26 billion dollars between 2013-2019 [9]. Lastly, email spoofing damages over 3.1 billion dollars [10].

When we are examining in detail, we found that the type of email attack that leads users to believe that it is a safe email is a Spoof Email. This type of attack is difficult to detect, and in general an email security gateway does not have the capability to isolate spoof email attacks. Email Spoofing Attack is conducted by making the victim believed

that the attacker is the legitimate email sender and hence the email content. This usually leads to attached file openings or internet link that can contain harmful virus [11]. Email spoofing is a form of social engineering attack that the attacker exploits the trust and outdated security measure which has a high rate of success without tools or skills.

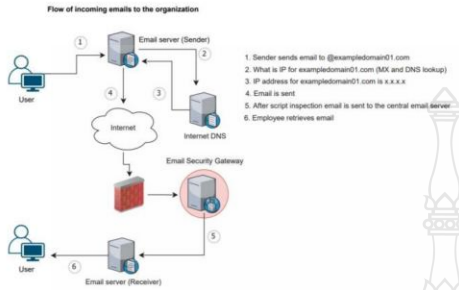


Fig. 2. Flow of incoming emails to the organization.

Based on this problem, as shown in Fig. 2, Security Gateway and go through the email sorting process as follows:

1. Review the Reputation Sender Score. The ratings are based on the Talos Database standards (talosintelligence.com).

2. Verify email headers using SPF, DKIM and DMARCH principles.

3. Verify by using Recipient Access Table and Host Access Table (RAT: The Domains that can send emails will be determined by the organization policy).

Lastly, we implement script designed for detecting spoof email in this scenario, as shown in Fig. 3.

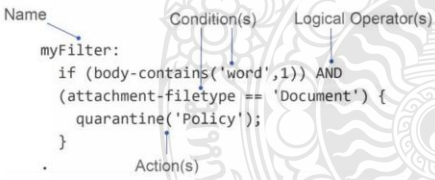


Fig. 3. Pseudocode to detect spoofed email.

Sender Policy Framework (SPF) is created to let the sender declares the IP address for outgoing email from his domain. This IP address is kept in the DNS record. On the other hand, the receiver can verify if the incoming email is originated from the sender's domain by checking the IP address of the incoming email with one registered in the DNS record. For instance, the sender sends an email with IP address 192.168.200.10 which is registered to sender's domain. If the receiver finds that the incoming email has an IP address 192.168.200.10 which coincides with the IP address of the sender's domain, the email is legitimate. Otherwise, the email is considered harmful and should be quarantined.

Domain Keys Identified Mail (DKIM) is an email verification method that allows the receiver to check if an incoming email is actually sent by sender's domain. DKIM works in similar fashion as SPF by declaring sender's Public Key in the DNS record instead of the IP address. In other words, DKIM implements digital signature to the email. Once the receiver verifies that an incoming email has a valid DKIM signature, the receiver can be certain that the email is legitimate and actually sent from the sender.

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an extension of SPF and DKIM by utilizing both results from SPF and DKIM. The sender can publish DMARC instructions in the DNS record for the sender's domain. The receiver can verify the incoming email by using DMARC instructions published by the sender's domain. If the incoming email passes the verification, the email is legitimate. On the contrary, if the incoming email fails the verification, the email could be quarantined or rejected, depending on the instructions provided by the DMARC record.

II. Related Work

Based on research related to SPF and DKIM, it is believed that SPF is implemented approximately 80.7% by organizations while DKIM is implemented only 59.4% by email domain worldwide [8-10]. This implies that there exist numerous email vulnerabilities according to 2 major reasons.

- Email security system is implemented in augmented fashion which makes the system complicated. The user has to be proficient and understand the email security in details.
- IT administrator lacks an in-depth knowledge of email security implementation and maintenance.

III. The Proposed Scheme

Two months later, after implementing Email Security gateway Appliance. We found that the email security gateway be able to detect unsafe email approximately 79% (9,200,000 of 11,700,000) of all emails that sent to this organization and the accuracy is 100%. But soon after the e-mail administrator of this organization received notification from several users that they received an email which sent from a trust domain but found later it was a fraud email. We take a closer look in detail of an original email from a hacker. Found that a hacker already stole a user's passwords, private credential, and a private information from a user. We are concurring that it is a spoof email because the sender is themselves, but the IP Address is not a set of IP Addresses that used in Thailand or any IP address of a user's organization. The emails that were once considered safe to be forwarded to the user is not safe anymore. So, we have noticed a limitation of the Email Security Gateway appliance with the standard settings. And in general, we found that the email security gateway in the market cannot detect the spoof email as well.

IV. Methodology

Email system consists of equipment from both sender's side and receiver's side working reciprocally. The email security features cannot be implemented only on the receiver's end. For example, if the receiver wants to verify the incoming email by implementing SPF, DKIM, and DMARC. However, the email sender has not implemented SPF, DKIM, and DMARC, the receiver cannot verify the email if it is legitimate since the email security features have not been implemented on both sides. At present, business is conducted online globally and hence the incoming email from various sources, both known and unknown. Consequently, it is recommended against implementing SPF, DKIM, and DMARC for all senders, but only to specific groups of senders.

The spoof email can be detected using email security gateway that can filter out harmful emails such as phishing email and spoofing email. In the work, we employ the Cisco email gateway with default settings and observe the results for 2 months. We find that the Cisco email gateway can effectively filter out harmful emails. However, numbers of spoofed emails are delivered to users. This implies that the Cisco email gateway is ineffective against spoofed emails.

We investigate the spoof email in details and find that it has an IP address from oversea and upon closer inspection in the email header, we find many of them are classified as safe emails. This conclude our assumption that the Cisco email gateway is ineffective against spoofed emails. Consequently, we implement the script to detect spoofed email as shown in Fig. 4. This script can drastically improve the efficiency of that the Cisco email gateway against spoofed emails.

```
Script Name: if sendergroup != "RELAYLISTDOMAIN" {
                if (mail-from == "@exampledomain01\\.com$")
                OR ((mail-from == "exampledomain01\\.co\\.th$")
                OR ((mail-from == "exampledomain02\\.com$")
                OR ((header("From") == "@exampledomain01\\.com$")
                OR ((header("From") == "exampledomain01\\.co\\.th$")
                OR (header("From") == "exampledomain02\\.com$")))))) {
                    quarantine("quarantine profile name");
                    log-entry("Antispoof Email Details: MID $MID $RemoteIP $remotehost $EnvelopeFrom");
                }
            }
```

Fig. 4. Script implementation to detect spoofed email.

The script inspects sender's IP address if it originates from the known sources, that is, if the incoming email has an IP address from outside organization, it checks if the incoming email has the same email domain. If all conditions are true then the incoming email is quarantined and logged.

V. Experimental results

We have developed a script to detect these spoofing emails. The conditions will check these emails if the sender have an IP Address that is not specified in the specific list and the domain is the domain of this organization or affiliated organizations then send it to quarantine and write a logging file. We followed up to six months after implementing this script. We found that the standard settings were able to distinguish unsafe emails as a percentage 92.53% (30,633,332 of 33,106,281) of all emails were sent to this organization and the script can distinguish spoof email as a percentage 0.4% (10,008 email of 2,472,949) of safe or clean emails. In terms of correctness, when checking the e-mail that has been quarantine by our script it has a 100% of an accuracy according to the conditions It can be proof that the spoof emails that sent to this organization are drop by our script.

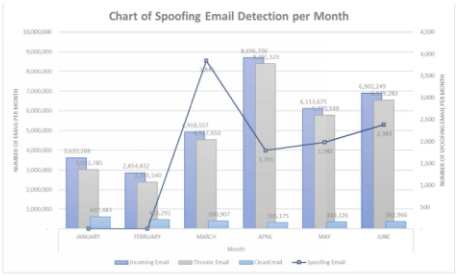


Fig. 5. Spoofing email detection.

The script we implemented was able to increase the efficiency of e-mail filtering of threats to this Email Security Gateway by approximately 10,008 emails from the original 2,472,949 clean email as shown in Fig. 5.

VI. Conclusions

There are many users who receive spoof emails, and some have been completely taken over by fraud people from the internet. hacker can export user's personal data and a private information including an important credential on user's computer it causes risks and damage to this a wide organization so after implementing this Script, we found that all spoof emails can be filtered by our solution. Increase more security for users and secure the organization. However, Attacker is still trying to find a new cyber-attack method to constantly attack any users. Therefore, users need to be more aware of the use of both email and the internet as there is no device or method that offers 100% protection against cyber threats.

References

[1] S. Maroofi, M. Korczynski, and A. Duda, "From defensive registration to subdomain protection: evaluation of email anti-spoofing schemes for high-profile domains," in Proc. Netw. Traffic Meas. Anal. Conf. (TMA), 2020, pp. 1–9.

[2] H. Hu and G. Wang, "End-to-end measurements of email spoofing attacks," in Proc. 27th USENIX Security Symp., 2018, pp. 1095–1112.

[3] H. Hu, P. Peng, and G. Wang, "Towards understanding the adoption of anti-spoofing protocols in email systems," in Proc. IEEE Cybersecurity Develop. (SecDev), Cambridge, MA, USA, 2018, pp. 94–101.

[4] S. Shukla, M. Misra, and G. Varshney, "Identification of spoofed emails by applying email forensics and memory forensics," 10th Int'l Conf. on Comm. and Net. Secu., 2020.

[5] What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security

[6] Email Trouble: Secrets of Spoofing, the Dangers of Social Engineering, and How We Can Help

[7] A survey of phishing attacks: Their types, vectors and technical approaches

[8] https://www.ic3.gov/Media/Y2019/PSA190910

[9] https://www.forbes.com/sites/johnkoetsier/2020/05/11/scammers-send-31-billion-domain-spoofing-emails-a-day-heres-how-to-protect-yourself-and-your-company/?sh=3dbc8d0148cb

[10] Email Spoofing Detection Using Volatile Memory Forensics

[11] Email Trouble: Secrets of Spoofing, the Dangers of Social Engineering, and How We Can Help

ประวัติผู้เขียน

ชื่อ นายวรวุฒิ จำปาหอม

วัน เดือน ปีเกิด 21 กรกฎาคม 2533

ที่อยู่ 119/1053 หมู่ที่ 1 ต.ไทรม้า อ.เมือง จ.นนทบุรี 11000

การศึกษา ปริญญาตรี คณะวิศวกรรมศาสตร์ ภาควิชาคอมพิวเตอร์ มหาวิทยาลัยกรุงเทพ

ประสบการณ์การทำงาน

- Senior Technical Implementation Engineer
  (Oct 2021–Present)
  Company: NTT Ltd. Bangkok, Thailand
- Solutions Architect - Cybersecurity (Jul 2020–Oct 2021)
  Company: NTT Ltd. Bangkok, Thailand
- Presales Engineer – Security (Mar 2019–Jun 2020)
  Company: ACA Pacific Group Co., Ltd. Bangkok, Thailand
- Network Engineer (Apr 2015-May 2018)
  Company: United Information Highway Co., Ltd. Bangkok, Thailand
- Problem Analyst - Infra/Network (Sep 2012-Dec 2013)
  Company: IT One Co Ltd. Bangkok, Thailand

เบอร์โทรศัพท์ 087-166-2999

อีเมล worawoot_j@en.rmutt.ac.th