การตรวจจับบอทเน็ตสแปมเมล์และความตระหนักในภัยลวงเฟซบุ๊คฟิชชิ่ง
Botnet Spam Detection and Facebook Phishing Scam Awareness

เบญจพร ลิ้มธรรมาภรณ์[1]* และ กอบเกียรติ สระอุบล[2]
Benchaphon Limthanmaphon[1]* and Kobkiat Saraubon[2]

บทคัดย่อ

ภัยจากอาชญากรรมคอมพิวเตอร์ที่เข้ามามีบทบาทและส่งผลต่อผู้ใช้งานในสังคมออนไลน์อย่างมาก คือภัยลวงจากบอทเน็ตและฟิชชิ่ง ผู้ใช้จำนวนไม่น้อยที่ตกเป็นเหยื่อ ถูกลวงเอาข้อมูลสำคัญไป เช่น ข้อมูลการล็อกอิน รหัสผ่าน ข้อมูลบัตรเครดิต เป็นต้น บทความนี้นำเสนอแนวทางการตรวจจับฟิชชิ่งและบอทเน็ตสแปมที่สามารถป้องกันการหลองลวงได้ทั้งเครือข่ายสังคมออนไลน์ชื่อดังเช่น Facebook รวมถึงแนวทางการป้องกันสำหรับผู้ดูแลระบบและผู้ใช้งาน

คำสำคัญ: ภัยคุกคามเครือข่ายสังคม ฟิชชิ่ง บอทเน็ต สแปม

Abstract

Phishing scam and botnet spams are examples of cyber crime that substantially affect online users. A considerable number of victims have suffered the intrusion of sensitive information such as their login information, entry password and credit card details. The paper provides guidance on how to monitor and detect malicious activity on the Internet such as spam, botnets, and phishing emails that imitate famous web sites including renowned Facebook. Finally, effective guidelines with regard to social networking threat detection and fraud preventive measures are suggested to IT users and systems administrators.

Keywords: Social Networking Threat, Phishing, Botnet, Spam

1. บทนำ

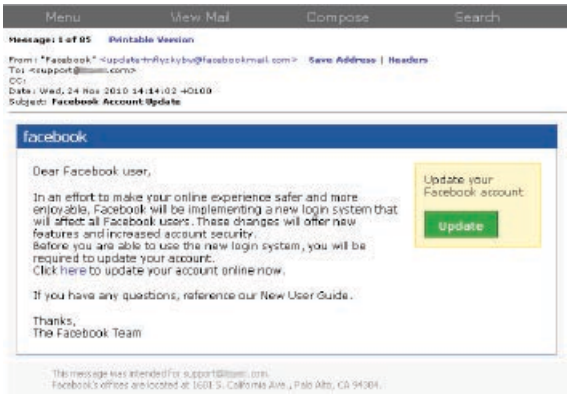
Facebook เป็นเว็บไซต์สังคมออนไลน์ชื่อดังที่รู้จักกันดี ปัจจุบันมีผู้ใช้งานทั่วโลกราวห้าร้อยล้านคน [1] อย่างไรก็ตาม มีผู้ใช้จำนวนไม่น้อยที่ยังไม่ทราบถึงภัยลวงจากบอทเน็ต (Botnet) และฟิชชิ่ง (Phishing) ซึ่งส่งเมล์หลอกลวงเอาข้อมูลสำคัญของเหยื่อไป โดยการส่งเมล์มาแจ้งให้ผู้ใช้งานทำการอัพเดทข้อมูลส่วนตัว หรือให้ดาวน์โหลดไฟล์ที่มีมัลแวร์ (Malware) แฝงอยู่ ซึ่งเมล์ที่ส่งเข้ามานี้จะมีลักษณะเหมือนกับของจริงที่ส่งมาจาก Facebook มาก ดังรูปที่ 1 หากผู้ใช้ที่ยังไม่มีความรู้เรื่องระบบความมั่นคง (Security) ที่ดีพอ ก็อาจถูกลวง

[1] ผู้ช่วยศาสตราจารย์ ภาควิชาวิทยาการคอมพิวเตอร์และสารสนเทศ คณะวิทยาศาสตร์ประยุกต์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

[2] นักศึกษา ภาควิชาวิทยาการคอมพิวเตอร์และสารสนเทศ คณะวิทยาศาสตร์ประยุกต์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

* Corresponding Author, Tel 0-2913-2500 Ext. 4617, E-mail: blt@kmutnb.ac.th

รับเมื่อ 11 กุมภาพันธ์ 2554 ตอบรับเมื่อ 27 พฤษภาคม 2554



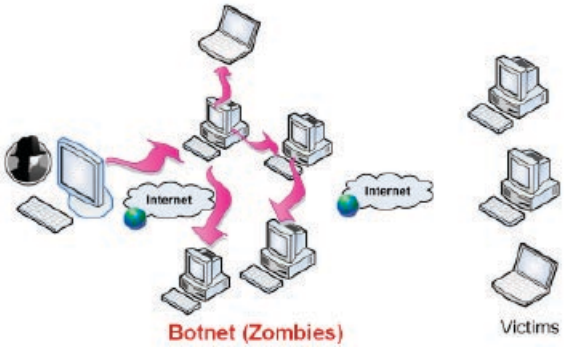
รูปที่ 1 ตัวอย่างอีเมล์ปลอมที่อ้างว่าส่งมาจาก Facebook หลอกให้ผู้ใช้ล็อกอินเข้าไปปรับปรุงข้อมูล

ให้ลงชื่อเข้าสู่ระบบ ผู้ใช้จำนวนมากหลงกลทำการล็อกอิน (Login) เข้าไปแล้ว ข้อมูลชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) จะถูกส่งไปยังผู้ไม่ประสงค์ดี โดยอาจมีการแกล้งเปลี่ยนรหัสผ่านทำให้เจ้าของตัวจริงเข้าใช้งานต่อไปอีกไม่ได้ โดยเฉพาะอย่างยิ่ง หากผู้ใช้ท่านใดใช้รหัสผ่านเหมือนกับตัวอีเมล์ ก็จะทำให้เสียอีเมล์นั้นไปด้วย หรือบางรายอาจมีการเรียกค่าไถ่เพื่อแลกกับรหัสผ่าน เป็นต้น

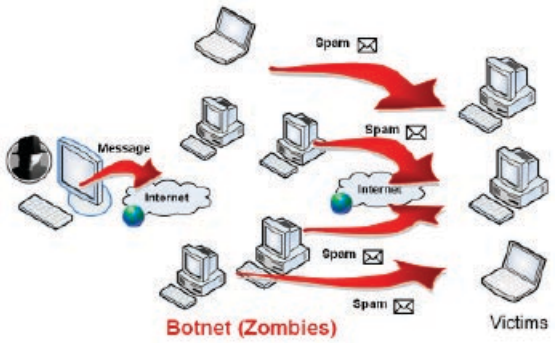
2. บอทเน็ตสแปม

บอทเน็ตคือกลุ่มคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ต กลุ่มคอมพิวเตอร์เหล่านี้ถูกควบคุมโดยโปรแกรมประเภทมัลแวร์ (Malware) เช่น ไวรัส (Virus) หนอน (Worm) โทรจัน (Trojan) เป็นต้น ที่ผู้ไม่หวังดีทำการปล่อยไว้ ซึ่งมักมาจากการที่ผู้ใช้ดาวน์โหลดซอฟต์แวร์หรือเปิดอีเมล์ที่มีโค้ดดังกล่าวแฝงอยู่ ทำให้เครื่องคอมพิวเตอร์ถูกควบคุมและกลายเป็นทาส หรือเรียกอีกอย่างว่าซอมบี้ (Zombies) โดยที่ผู้ร้ายสามารถทำการควบคุมกลุ่มบอทเน็ตจากระยะไกลได้ดังรูปที่ 2

เพื่อการส่งเมล์ให้เหยื่อจำนวนมาก ผู้ไม่ประสงค์ดีจึงใช้วิธีปล่อยสแปม โดยจะส่งคำสั่งควบคุมไปยังบอทเน็ตเพื่อให้กลุ่มคอมพิวเตอร์ที่เป็นทาสซึ่งมีอยู่จำนวนมากมายมหาศาล ทำการส่งอีเมล์ออกไป เรียกว่าบอทเน็ตสแปม



รูปที่ 2 กลุ่มคอมพิวเตอร์ที่ติดมัลแวร์แล้วกลายเป็นบอทเน็ต [2]



รูปที่ 3 ผู้ปล่อยสแปมส่งคำสั่งควบคุมให้เครื่องกลุ่มบอทเน็ต ส่งอีเมล์ออกไป [2]

ดังรูปที่ 3 ซึ่งอีเมล์ที่ถูกส่งโดยบอทเน็ตมักจะมีเนื้อหาคล้ายกัน ดังรูปที่ 5

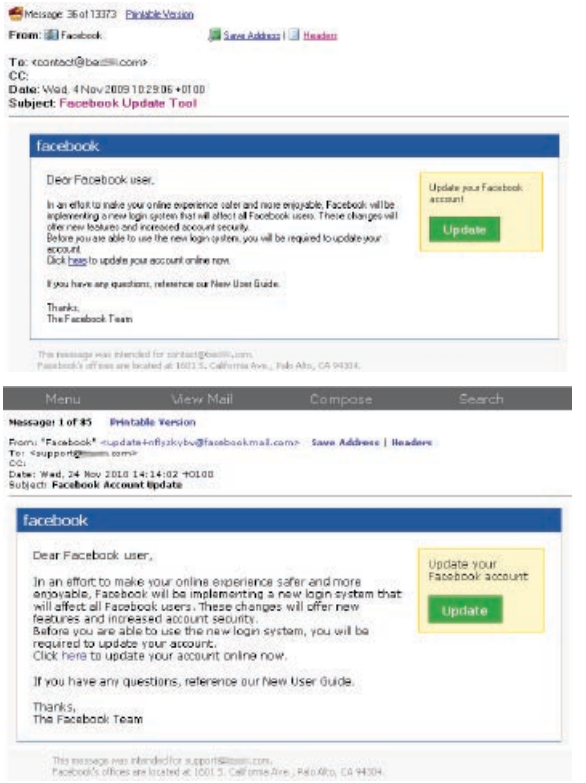
3. ฟิชชิ่ง (Phishing)

ฟิชชิ่งหมายถึงการหลอกลวงทางอินเทอร์เน็ต เพื่อเอาข้อมูลสำคัญ ได้แก่ ชื่อผู้ใช้งาน รหัสผ่าน ข้อมูลบัตรเครดิต ฯลฯ โดยการปลอมหรือเลียนแบบให้เหมือนกับเว็บไซต์ผู้ให้บริการจริงๆ แล้วส่งข้อความทางอีเมล์หรือส่งผ่านโปรแกรมการส่งข้อความทันทีหรืออินสแตนท์เมสเสจจิ้ง (Instant Messaging) หลอกให้เหยื่อหลงกล เช่น แจ้งว่าทางผู้ให้บริการต้องการอัพเดทระบบสมาชิกให้ผู้ใช้เข้ามาล็อกอินเพื่ออัพเดท มิฉะนั้นจะเข้าระบบไม่ได้ ฯลฯ

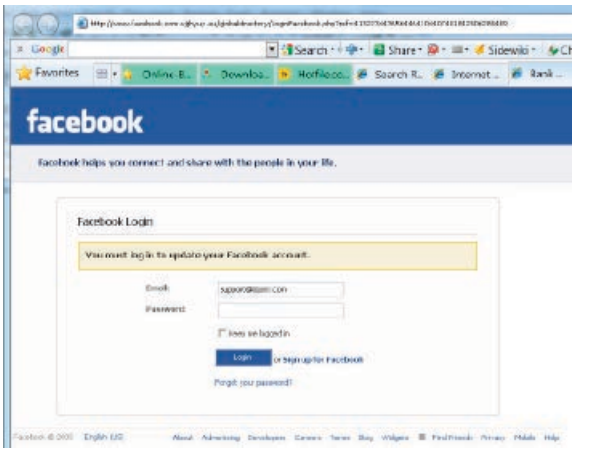
เพื่อให้บรรลุวัตถุประสงค์และเพื่อให้ได้จำนวนเหยื่อมากที่สุด จึงจำเป็นที่จะต้องส่งเมล์จำนวนมากๆ ดังนั้นวิธีที่นิยมใช้คือ บอทเน็ตสแปม ดังที่กล่าวมา

		From	Subject	Size
☐		"Facebook"	New login system	1393b
☐		"Facebook"	Facebook Update Tool	5184b
☐		"Your Facebook"	Facebook Password Reset Confirmatio...	33295b
☐		"Facebook"	New login system	5060b
☐		"Facebook"	new login system	5052b
☐		"The Facebook"	Facebook Password Reset Confirmatio...	33043b
☐		"Facebook"	new login system	5431b
☐		"Facebook"	New login system	5132b
☐		"Facebook"	Facebook Account Update	5098b
☐		"Facebook"	Facebook Update Tool	5158b

รูปที่ 4 ตัวอย่างรายการเมล์ประเภทฟิชชิ่ง ที่ส่งโดยบอทเน็ตที่ปลอมแปลงลวงว่ามาจาก Facebook



รูปที่ 5 เมล์ประเภทฟิชชิ่ง จากบอทเน็ตสแปม 2 ฉบับที่มาจากเมล์เซิร์ฟเวอร์คนละแห่งแต่มีเนื้อหาเหมือนกัน



รูปที่ 6 หน้าล็อกอินปลอม

รูปที่ 7 หลังจากล็อกอินเรียบร้อยแล้ว

รูปที่ 4 เป็นตัวอย่างรายการเมล์ในเมล์บอกซ์ที่มีการส่งจากบอทเน็ตแต่ลวงว่าส่งมาจาก Facebook ซึ่งในข้อความของเมล์จะมีข้อความแสดงดังรูปที่ 5 และจากรูปที่ 5 จะเห็นว่าตัวอีเมล์ที่ส่งมามีเนื้อหาแจ้งว่าทาง Facebook ต้องการปรับปรุงระบบให้มีความปลอดภัยและสะดวกต่อการใช้งาน ดังนั้นให้ผู้ใช้คลิกเข้าไปเพื่ออัพเดทข้อมูล ซึ่งหากดูหน้าจอแล้วจะเห็นว่ารูปแบบค่อนข้างเหมือนกับอีเมล์ที่ส่งมาจาก Facebook จริงๆ หลังจากที่คลิกลิ้งค์ตามที่แจ้งมาในอีเมล์ก็จะเข้าสู่หน้าล็อกอิน ดังรูปที่ 6 ซึ่งดูโดยรวมแล้วก็จะคล้ายคลึงกับหน้าล็อกอินของ Facebook จริงๆ เช่นกัน

ถึงตอนนี้ผู้ใช้ที่ตกเป็นเหยื่อก็ยังไม่ได้สูญเสียข้อมูลอะไรไป ซึ่งถ้าผู้ใช้ลองคลิกอัพเดทและทำการกรอกข้อมูล อีเมล์และรหัสผ่านแล้วคลิกล็อกอิน ก็จะเข้าหน้า My Account ดังรูปที่ 7 ราวกับว่าเข้าสู่ระบบ

ได้แล้ว (ไม่ว่าจะใส่ข้อมูลล็อกอินถูกหรือผิดก็ตาม ก็จะเข้าสู่หน้านี้ได้) ขณะเดียวกันข้อมูลล็อกอิน อีเมล์และรหัสผ่านก็จะถูกส่งไปยังผู้ที่สร้างระบบปลอมนี้ขึ้นมาเพื่อนำไปใช้ปลอมตัวในการเข้าสู่ระบบ (Imposter) ซึ่งสามารถเข้าไปใช้งานระบบหรือหาผลประโยชน์อื่นต่อไปได้

หลังจากล็อกอินเรียบร้อยแล้ว ก็มีเพียงแค่ลิ้งค์ให้ดาวน์โหลด updatetool.exe ซึ่งก็เป็นไฟล์ที่มีมัลแวร์แฝงอยู่ภายใน

4. การตรวจจับสแปมเมล์

มีงานวิจัยจำนวนมากถูกออกแบบมาเพื่อคัดกรองหรือตรวจจับสแปมเมล์ ซึ่งมักจะมีการกำหนดคุณลักษณะที่ใช้คัดกรอง เช่น การกรองโดยใช้คำหลัก หรือการคัดแยกโดยใช้ส่วนหัวของเมล์ จากนั้นก็จะกำหนดฟังก์ชันในการคัดกรองหรือตรวจจับโดยหลักๆ แบ่งออกเป็น 2 ประเภทคือประเภทที่ใช้การเรียนรู้ของเครื่องหรือแมชชีนเลิร์นนิ่ง (Machine Learning) [3]-[6] และประเภทที่ไม่ได้ใช้การเรียนรู้ (Non-machine Learning) [7],[8] งานที่ใช้การเรียนรู้ของเครื่องที่ได้รับความนิยมได้แก่ การสร้างข่ายการเรียนรู้โดยใช้ทฤษฎีความน่าจะเป็นของเบส์ (Bayes Theorem) งานวิจัยของ Kosmopoulos และคณะ [6] นำเสนอการตรวจจับสแปมชนิดข้อความ จึงมีข้อจำกัดอยู่บ้างสำหรับการตรวจจับสแปมเมล์แบบรูปภาพ ซึ่งปัจจุบันแนวโน้มสแปมเมล์ชนิดนี้มีจำนวนเพิ่มสูงขึ้นเรื่อยๆ

สำหรับสแปมเมล์ชนิดรูปภาพได้มีงานวิจัยของ Biggio และคณะ [9] เสนอวิธีการกรองโดยใช้ระบบโอซีอาร์ (Optical Character Recognition) ทำการแยกข้อความออกจากรูปภาพ เพื่อนำมาประมวลผลว่าอยู่ในกลุ่มสแปมหรือไม่ และได้นำเสนอกระบวนการประมวลผลรูปภาพ (Image Processing) มาใช้ในการคัดกรองสแปม [10] แต่วิวัฒนาการของสแปมได้มีการส่งสแปมเมล์รูปภาพโดยปรับเปลี่ยนรูปภาพหรือใส่ลวดลายและพื้นฉากหลัง เพื่อให้ระบบประมวลผลไม่สามารถตรวจจับได้ มีงานวิจัยที่ใช้การเรียนรู้ของเครื่องอีกวิธีคือ การใช้โครงข่ายใยประสาทเทียม เช่น งานวิจัยของ Tak และ Tapaswi [11] เสนอการคัดกรองสแปมเมล์โดยอาศัยการดึงข้อมูลสอบถามจากฐานข้อมูลความรู้ (Knowledge Base) มาผนวกกับการสร้างโครงข่ายใยประสาทประดิษฐ์ เพื่อตรวจจับพฤติกรรมของสแปมเมล์ โดยการวิเคราะห์จากส่วนหัวของเมล์ (Mail Header) พร้อมทั้งใช้การตรวจสอบไขว้ (Cross Validation) เพื่อดูว่าเป็นเมล์ที่ถูกสร้างจากเครื่องอัตโนมัติหรือมาจากมนุษย์จริงๆ

สำหรับการตรวจจับสแปมเมล์ที่ไม่ได้ใช้การเรียนรู้ของเครื่องมีวิธีที่นิยมใช้ได้แก่ การใช้รายการบัญชีดำ (Blacklist) โดยการเก็บไอพีแอดเดรสของเครื่องเซิร์ฟเวอร์ที่ส่งสแปมไว้ในฐานข้อมูล เพื่อทำการสกัดกั้นเมล์ที่ส่งมาจากเครื่องดังกล่าว วิธีนี้มีจุดอ่อนคือขาดประสิทธิภาพในการกรองสแปมจากบอทเน็ต และมีอัตราเกิดความผิดพลาดชนิดเชิงบวก (False Positive) ค่อนข้างสูงเนื่องจากเซิร์ฟเวอร์แบบใช้งานร่วมกัน (Shared Hosting) ที่ใช้งานกันทั่วโลกที่แต่ละเครื่องมีไอพีแอดเดรสชุดเดียว แต่มีจำนวนเว็บไซต์อยู่เป็นจำนวนนับร้อย หากมีการส่งสแปมจากผู้ใช้โดเมนหนึ่งแล้วถูกขึ้นรายการบัญชีดำ ผู้ใช้โดเมนอื่นที่อยู่บนเซิร์ฟเวอร์เดียวกันก็จะถูกขึ้นบัญชีดำไปด้วย ทำให้ส่งเมล์ไม่ถึงปลายทาง ซึ่งกรณีนี้ถือเป็นข้อผิดพลาดที่อาจส่งผลให้การติดต่อธุรกิจเสียหายได้ นอกจากนี้มีการใช้ซิกเนเจอร์ (Signature) ซึ่งเกิดจากการนำข้อความอีเมล์ผ่านฟังก์ชันแฮช (Hash) มาเก็บไว้ในฐานข้อมูลเพื่อทำการเปรียบเทียบในคราวต่อๆ ไป แต่วิธีนี้มีข้อเสียคือ ต้องอาศัยข้อมูลที่เตรียมล่วงหน้าว่า เมล์ใดเป็นสแปมเพื่อทำการบันทึกซิกเนเจอร์เอาไว้สำหรับทำการเปรียบเทียบครั้งต่อๆ ไปได้

งานวิจัยกอบเกียรติ และ Limthanmaphon [2],[12] ไม่ได้ใช้การเรียนรู้ของเครื่องและไม่ได้ใช้การคัดกรองจากรายการบัญชีดำ แต่ใช้กระบวนการตรวจจับสแปมโดยการเปรียบเทียบแหล่งที่อยู่ของเซิร์ฟเวอร์ที่ใช้ส่งอีเมล์กับแหล่งที่อยู่ของเอ็มเอ็กซ์โฮสต์ (MX Host) หรือแหล่งที่อยู่ของเซิร์ฟเวอร์ที่อยู่ของโดเมน ซึ่งงานวิจัยนี้

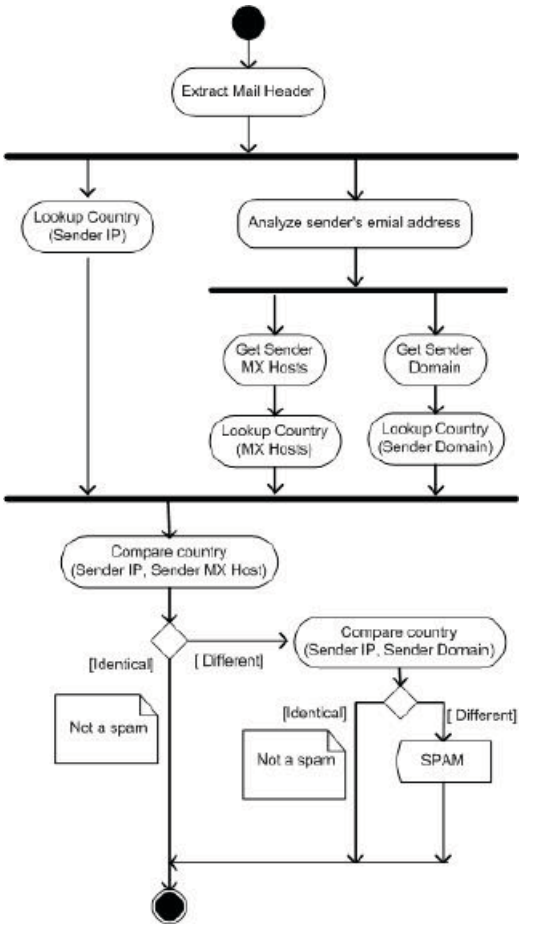
สามารถตรวจจับสแปมเมล์ได้ทั้งเมล์ที่เป็นข้อความและรูปภาพได้อย่างรวดเร็วและมีประสิทธิภาพ ซึ่งสามารถตรวจจับคัดกรองสแปมเมล์ได้ถูกต้องถึงร้อยละ 96.23 โดยค่าความผิดพลาด (False Positive) เป็น 0 รายละเอียดของงานวิจัยนี้ขอกล่าวในหัวข้อถัดไป

5. การตรวจจับสแปมเมล์จากแหล่งที่อยู่

งานวิจัยของกอบเกียรติ และ Limthanmaphon [2],[12] นำเสนอการตรวจจับคัดกรองสแปมเมล์โดยการเปรียบเทียบแหล่งที่อยู่ของเซิร์ฟเวอร์ที่ใช้ส่งอีเมล์ (Sender IP Address) นำมาหาประเทศที่ตั้งของเซิร์ฟเวอร์จากฝั่งผู้ส่ง จากนั้นนำมาเทียบกับประเทศที่อยู่ของอีเมล์ผู้ส่ง ซึ่งเกิดจากการสกัดจากส่วนของอีเมล์แอดเดรสของผู้ส่ง (Sender Email Address) หรือเทียบจากประเทศที่ได้จากการสกัดส่วนของเมล์เซิร์ฟเวอร์ที่ทำหน้าที่รับเมล์บนโดเมนหรือเรียกย่อๆ ว่า MX Host ถ้าได้ประเทศที่อยู่ไม่ตรงกันก็สรุปได้ว่าเป็นสแปมเมล์ ดังรูปที่ 8

พิจารณาจากรูปที่ 9 แสดงส่วนหัวของเมล์ฉบับหนึ่งโดยระบุว่าส่งมาจาก Facebook

การตรวจสอบ เริ่มจากแยกค่าไอพีเซิร์ฟเวอร์ที่ทำการส่งเมล์ (Received: From) เพื่อนำไปค้นหาว่ามาจากประเทศใด โดยในงานนี้ใช้ฐานข้อมูล IP-Location [13] จากตัวอย่างข้างต้นไอพี 88.69.227.159 เป็นไอพีที่อยู่ในประเทศ Germany



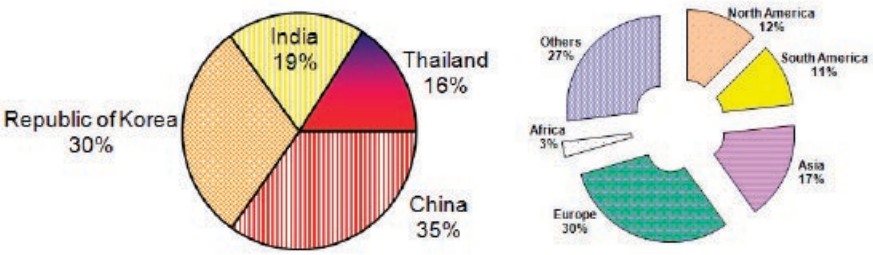
รูปที่ 8 แผนภาพกิจกรรมในการตรวจสอบสแปมจากการเปรียบเทียบแหล่งที่อยู่

```
Received: from dslb-088.pools.arcor-ip.net [88.69.227.159] by ns1.itpt.com with ESMTP
From: “Facebook” <update+nflyzkybw@facebookmail.com>
To: <support@itpt.com>
Subject: Facebook Account Update
Date: Wed, 24 Nov 2010 14:14:02 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary=”----=_NextPart_000_0006_01CA5D50.AD6AE0B0”
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4807.2300
Message-ID: <000d01ca5d50$ad6ae0b0$6400a8c0@stretchierhpc>
```

รูปที่ 9 ตัวอย่างส่วนหัวของเมล์ ที่ระบุว่าส่งมาจาก Facebook

Result	Header
	Received: from dslb-088.pools.arcor-ip.net [88.69.227.159] by ns1.itpt.com with ESMTP (SMTPD32-8.15) id AF0D25D01A0; Wed, 24 Nov 2010 14:14:02 +0700 From: \"Facebook\" <update+nflyzkybw@facebookmail.com> To: <support@itpart.com> Subject: Facebook Account Update Date: Wed, 24 Nov 2010 14:14:02 +0100 MIME-Version: 1.0 Content-Type: multipart/alternative; boundary=\"----=_NextPart_000_0006_01CA5D50.AD6AE0B0\" X-Mailer: Microsoft Office Outlook, Build 11.0.5510 **Sender IP and Country:** 88.69.227.159 DE - Germany **From MX:-** mx01.facebookmail.com | 69.63.179.27 US - United States **From hostdomain :** facebookmail.com | 69.63.179.27 US - United States

รูปที่ 10 การตรวจจับได้ผลลัพธ์ว่าเป็นอีเมล์ปลอม



รูปที่ 11 ผลการตรวจจับอีเมล์สแปม Facebook

ขั้นต่อมา นำข้อมูลอีเมล์แอดเดรสของผู้ส่ง (From: Email) ไปหาข้อมูล MX Host (รายละเอียดการค้นหา MX Host ดูได้จาก [2]) แล้วเปลี่ยนเป็นไอพี ซึ่งจากในตัวอย่างผู้ส่งคือ

update+nflyzkybw@facebookmail.com ได้ค่า MX Host คือ mx01.facebookmail.com US - United States ส่วนไอพีคือ 69.63.179.27 จากนั้นทำการค้นหาว่ามาจากประเทศใด หลักการเช่นเดียวกับขั้นตอนแรก ผลลัพธ์ได้ว่าไอพีอยู่ในประเทศ US - United States ดังรูปที่ 10 ผลการเปรียบเทียบ พบว่าอีเมล์ถูกส่งมาจากประเทศเยอรมนี แต่ที่อยู่ MX Host ของผู้ส่งและโดเมนอยู่ในประเทศอเมริกา ซึ่งอยู่คนละแห่งกัน ดังนั้นผลการตรวจจับจะได้ว่าเมล์ฉบับนี้เป็นสแปม เนื่องจากตรวจพบการปลอมแปลงข้อมูลผู้ส่ง (จากข้อมูลตรง From:)

จากอัลกอริทึมดังกล่าวเมื่อนำมาทดสอบกับอีเมล์ฟิชชิ่ง Facebook สามารถตรวจจับได้ผลถูกต้องกว่าร้อยละ 94 โดยแยกตามโซนทวีป ซึ่งจากผลดังรูปที่ 11 ในโซนทวีปเอเชีย ประเทศไทยติดอันดับ 4 ในการส่งอีเมล์สแปม

6. การป้องกันการลวงจากสแปมเมล์และฟิชชิ่ง

เนื่องจากการปลอมแปลงเนื้อหาและหน้าเว็บ จะค่อนข้างเหมือนกับ Facebook ของจริงมาก ดังนั้นในการใช้งานให้ผู้ใช้สังเกตจาก URL โดย URL ของจริงจะต้องเป็น facebook.com เท่านั้น แต่ของปลอมจะเป็นลักษณะโดเมนย่อย (Sub-domain) ซึ่งจะมีชื่อโดเมนจุดและอื่นๆ ตามมา เช่น รูปที่ 12 ตรง URL www.facebook.com.ujjhyuy.eu โดเมนจริงคือ ujjhyuy.eu ไม่ใช่โดเมนจริงของ Facebook.com

รูปที่ 12 ก. URL ที่แสดงให้เห็นว่าเป็น Facebook ของปลอม

รูปที่ 12 ข. URL Facebook ของจริง

แต่อย่างใด ตัว URL ส่วนที่ทำให้คล้ายของจริงซึ่งก็คือ Facebook.com นั้นเป็นเพียงโดเมนย่อยของ ujjhyuy.eu นั่นหมายถึงว่าขณะที่เปิดหน้าเว็บแบบฟอร์มล็อกอินนี้ ผู้ใช้กำลังอยู่ที่เว็บไซต์ ujjhyuy.eu ไม่ใช่เว็บไซต์ Facebook.com

7. การป้องกันสำหรับผู้ดูแลระบบ

เพื่อลดปริมาณอีเมล์สแปมและฟิชชิ่งเข้ามาในระบบ เว็บมาสเตอร์หรือผู้ใช้ที่เกี่ยวข้องควรดูแลและป้องกันดังนี้

1. ไม่เปิดเผยเบอร์อีเมล์ตามฟอรั่มหรือเว็บบอร์ดเวทีแสดงความเห็นต่างๆ

2. หากคลิก URL หรือลิ้งค์ที่ส่งมากับอีเมล์ให้ดูว่า URL นั้นเป็นโดเมนจริงของเว็บไซต์หรือไม่ หรือเป็นเพียงโดเมนย่อย

3. หากต้องการเปิดเผยเบอร์อีเมล์บุคลากรในหน่วยงาน เพื่อให้ผู้อื่นสามารถติดต่อได้ควรทำเป็นภาพกราฟิกแทนการพิมพ์เป็นข้อความธรรมดา (Text) เพื่อป้องกันตัวกวาดอัตโนมัติที่จะมาเก็บเอาเบอร์อีเมล์ไป หรือใช้วิธีทำแบบฟอร์มเมล์กรอกสอบถามติดต่ออัตโนมัติแทน โดยไม่ต้องระบุเบอร์อีเมล์ที่หน้าเว็บ

4. ไม่ควรตั้งค่าเมล์ในระบบเป็นแคชออล (CatchAll) เพราะจะทำให้อีเมล์ที่ไม่มีการระบุชื่อผู้รับหรือระบุชื่อผู้รับที่ไม่มีอยู่ในระบบ ถูกส่งเข้ามาในระบบตามที่อยู่บนโดเมนเดียวกัน

5. การสมัครใช้บริการฟรีต่างๆ เช่น Facebook, Twitter ควรใช้อีเมล์ฟรี เช่น Hotmail, Yahoo, Gmail หรืออื่นๆ ไม่ควรใช้อีเมล์ขององค์กร

8. สรุป

บทความนี้ได้นำเสนอภัยลวงจากสแปมเมล์ ที่มักลวงหรือแอบอ้างการส่งจากเว็บไซต์สังคมออนไลน์ชื่อดังอย่าง Facebook ถ้าหากผู้ใช้ขาดความระมัดระวังในการใช้งาน ก็อาจถูกลวงให้ส่งข้อมูลสำคัญไปยังผู้ไม่ประสงค์ดีที่ใช้บอทเน็ตสแปมเป็นเครื่องมือในการล่อลวงหรือฟิชชิ่ง ทั้งนี้บทความนี้ได้สรุปแนวทางการตรวจจับสแปมเมล์ และนำเสนอการใช้อัลกอริทึมในการตรวจจับสแปมเมล์จากแหล่งที่อยู่ดังที่กล่าวในหัวข้อที่ 5 สามารถนำมาใช้ตรวจจับสแปมเมล์เพื่อลดการล่อลวงลงไปได้ พร้อมกันนี้ในส่วนท้ายได้เสนอแนะแนวทางการป้องกันสำหรับผู้ใช้งานและผู้ดูแลระบบ ซึ่งสามารถนำไปใช้กับการทำธุรกรรมอิเล็กทรอนิกส์อื่นๆ เช่น ธุรกรรมทางธนาคารและพาณิชย์อิเล็กทรอนิกส์ได้

เอกสารอ้างอิง

[1] Facebook สถิติ, (01/08/11). [Online]. Available: http://www.facebook.com/press/info.php?statistics

[2] กอบเกียรติ สระอุบล, “การกรองสแปมจากบอทเน็ต,” สารนิพนธ์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ, 2552.

[3] Y. F. Chiu, C. M. Chen, B. Jeng, and H. C. Lin, “An Alliance-based Anti-Spam Approach,” *Third International Conference on Natural*

Computation(ICNC2007), IEEE, 2007.

[4] M. Dredze, R. Gevaryahu, and A. Elias-Bachrach, "Learning Fast Classifiers for Image Spam," *Email and Anti-Spam (CEAS 2007)*, CA, USA, August, 2007.

[5] B. Issac, W. J. Jap, and J. H. Sutanto, "Improved Bayesian Anti-Spam Filter, " *ICCET*, vol. 2, pp.326-330, International Conference on Computer Engineering and Technology, 2009.

[6] A. Kosmopoulos, G. Paliouras, and I. Androutsopoulos, "Adaptive Spam Filtering Using Only Naive Bayes Text Classifiers," *Email and Anti-Spam (CEAS 2008)*, CA, USA, August, 2008.

[7] C. Dietrich and C. Rossow, "Empirical research on IP blacklisting," *Email and Anti-Spam (CEAS 2008)*, CA, USA, August, 2008.

[8] J. Jung and E. Sit, "An Empirical Study of Spam Traffic and the Use of DNS Black Lists," in *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, Taormina, Sicily, Italy, October 25-27, 2004.

[9] B. Biggio, G. Fumera, I. Pillai, and F. Roli, "Image Spam Filtering by Content Obscuring Detection," *Email and Anti-Spam (CEAS 2007)*, CA, USA, August, 2007.

[10] B. Biggio, G. Fumera, I. Pillai, and F. Roli, "Improving Image Spam Filtering Using Image Text Features," *Email and Anti-Spam (CEAS 2008)*, CA, USA, August, 2008.

[11] G. K. Tak and S. Tapaswi, "Query Based Approach Towards Spam Attacks using Artificial Neural Network," *International Journal of Artificial Intelligence & Applications (IJAIA)*, vol.1, no.4, October, 2010.

[12] K. Saraubon and B. Limthanmaphon, "Fast Effective Botnet Spam Detection," in *Proceedings of 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT 2009)*, IEEE, Seoul, November 24-26, 2009.

[13] IP Database Contributions. (09/09/10). [Online]. Available: http://www.phpclasses.org