บทที่ 3

วิธีการดำเนินการวิจัย

งานวิจัยนี้นำเสนอ ระบบการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต Detecting and Slowing Down Spam E-mail System (DSDSE) โดยมีรายละเอียดการพิจารณา 2 กรณีร่วมกัน คือ การตรวจสอบบอตเน็ตจากพฤติกรรมการสอบถามข้อมูล Domain Name ผ่านระบบ Domain Name System (DNS) และเทคนิคการตรวจสอบความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์โดยอาศัยค่า Threshold การดำเนินการวิจัยตั้งอยู่บนสมมุติฐาน คือ จดหมายอิเล็กทรอนิกส์สแปมส่วนมากถูกส่งออกมาจากเครื่องที่เป็นบอตเน็ต วัตถุประสงค์ของงานวิจัย เพื่อลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมที่ถูกส่งออกมาจากเครื่องบอตเน็ต ดังนั้นเครื่องที่มีพฤติกรรมในลักษณะที่อาจจะเป็นบอตเน็ต แต่ไม่มีความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์ จะไม่ถูกนำมาพิจารณาเพื่อลดอัตราการส่งจดหมายอิเล็กทรอนิกส์

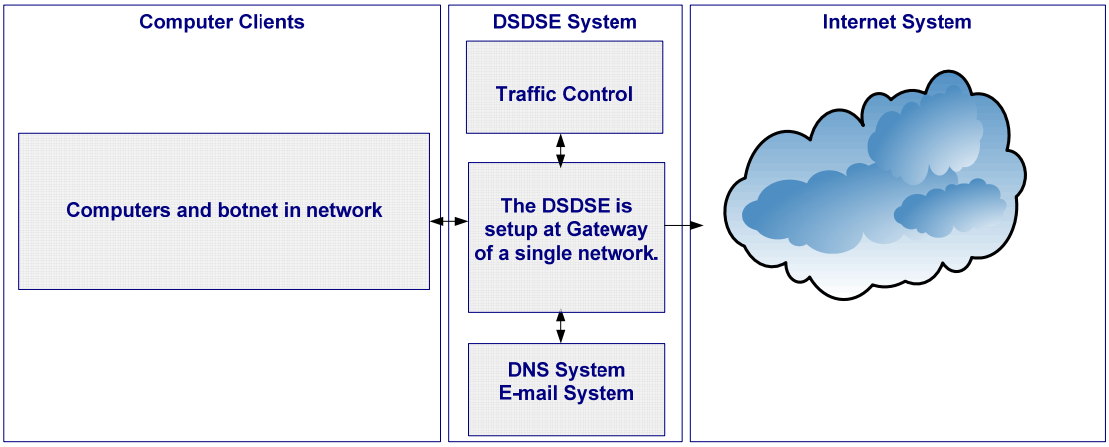
บทที่ 3 ประกอบด้วย การออกแบบระบบ DSDSE การเตรียมการทดลอง การดำเนินการทดลอง ข้อจำกัดของระบบที่ใช้ในการทดลอง มีรายละเอียดวิธีการดำเนินการวิจัย ดังนี้

3.1 การออกแบบระบบ DSDSE

การออกแบบระบบตรวจสอบและลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต (DSDSE) มีวัตถุประสงค์เพื่อตรวจหาเครื่องที่เป็นบอตเน็ตซึ่งอยู่ในระบบเครือข่ายขององค์กรหรือหน่วยงานที่ต้องการตรวจสอบ ระบบ DSDSE จะทำการวิเคราะห์ว่าเครื่องคอมพิวเตอร์เครื่องใดเป็นเครื่องปรกติและเครื่องใดเป็นเครื่องบอตเน็ต โดยพิจารณาจากการร้องขอตรวจสอบข้อมูล Domain Name จากระบบ DNS พร้อมกับตรวจสอบปริมาณการส่งจดหมายอิเล็กทรอนิกส์ที่ผิดปรกติ โดยอาศัยค่า Threshold มาช่วยคัดกรองระหว่างจดหมายอิเล็กทรอนิกส์ธรรมดากับจดหมายอิเล็กทรอนิกส์สแปม เมื่อผลตรวจสอบตรงตามเงื่อนไขที่กำหนด ระบบจะทำการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องคอมพิวเตอร์ดังกล่าว

การทำงานของระบบตรวจสอบและลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต สามารถแสดงภาพรวมดังภาพที่ 3.1

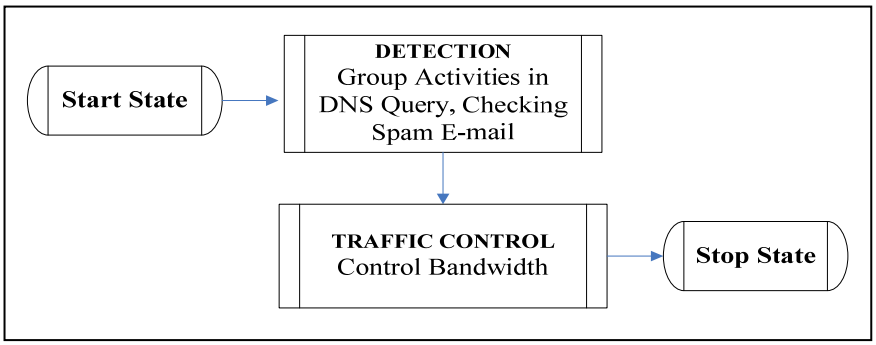
ภาพที่ 3.1 การทำงานของระบบ DSDSE



จากภาพที่ หีย3.1 แสดงภาพรวมการทำงานของระบบ DSDSE ซึ่งมีการติดต่อสื่อสารด้วยกัน 3 ส่วน ได้แก่ กลุ่มเครื่องคอมพิวเตอร์ลูกข่าย ระบบ DSDSE ที่ถูกติดตั้งไว้ที่เกตเวย์ และระบบอินเตอร์เน็ต โดยกลุ่มคอมพิวเตอร์ลูกข่ายจะประกอบด้วยเครื่องคอมพิวเตอร์ปรกติและเครื่องคอมพิวเตอร์ที่เป็นบอตเน็ต จะส่งข้อมูลให้ระบบ DSDSE ทำการวิเคราะห์ ก่อนที่จะส่งข้อมูลจดหมายอิเล็กทรอนิกส์ออกสู่ระบบอินเตอร์เน็ต

หน้าที่ของระบบ DSDSE มีหน้าที่หลัก 3 ประการ คือ การตรวจสอบหาเครื่องบอตเน็ต การวิเคราะห์จดหมายอิเล็กทรอนิกส์ เพื่อที่จะระบุให้ได้ว่าเป็นจดหมายอิเล็กทรอนิกส์สแปมหรือไม่ และการควบคุมอัตราการส่งออกจดหมายอิเล็กทรอนิกส์สแปมที่ถูกส่งออกมาจากเครื่องบอตเน็ตเข้าสู่ระบบอินเตอร์เน็ต

ภาพที่ 3.2 โครงสร้างระบบ DSDSE

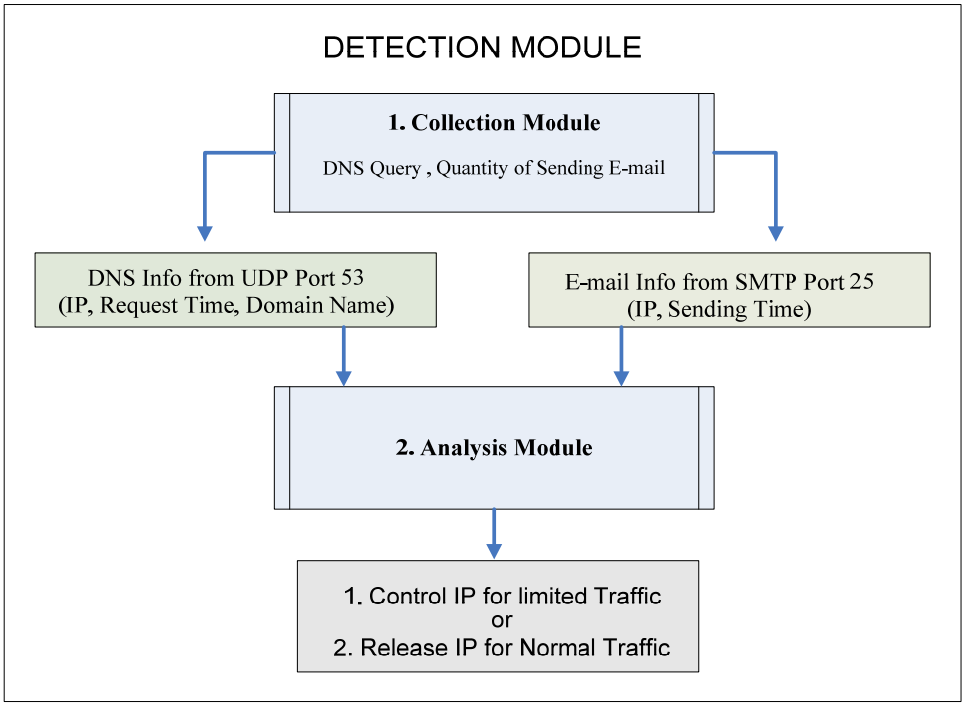


จากภาพที่ 3.2 โครงสร้างระบบ DSDSE ประกอบด้วย 2 ระบบย่อย คือ Detection Module และ Traffic Control Module

3.1.1 ระบบ Detection

ระบบ Detection ประกอบด้วยการทำงาน 2 ส่วนย่อย คือ ส่วนเก็บข้อมูล (Collection Module) และส่วนวิเคราะห์ข้อมูล (Analysis Module) ผลลัพธ์ที่ได้จากส่วน Detection จะได้หมายเลข IP ของเครื่องที่มีโอกาสจะเป็นบอตเน็ต แล้วส่งต่อให้ระบบ Traffic Control เพื่อควบคุมอัตราการส่งจดหมายอิเล็กทรอนิกส์จากเครื่องดังกล่าว

ภาพที่ 3.3 การทำงานของระบบ Detection Module ในระบบ DSDSE



จากภาพที่ 3.3 สามารถแสดงส่วนงานที่สำคัญ 2 ส่วนคือ ส่วนเก็บข้อมูล (Collection Module) และส่วนวิเคราะห์ข้อมูล (Analysis Module) มีรายละเอียดดังนี้

1) ส่วนเก็บรวบรวมข้อมูล (Collection Module)

ส่วนเก็บรวบรวมข้อมูลจะทำการดักจับข้อมูลหรือแพ็กเก็จที่ถูกส่งออกมาจากเครื่องลูกข่ายและทำการบันทึกข้อมูลลงฐานข้อมูล โดยมีข้อมูลที่ถูกบันทึกแบ่งได้ 2 กลุ่ม ดังนี้

ข้อมูลกลุ่มที่ 1 คือ ข้อมูลการร้องขอหมายเลข IP Address ของ Domain Name ที่ต้องการทราบ จาก DNS Server โดยสามารถดักจับข้อมูลที่ผ่านเข้ามาที่ Gateway ได้จาก UDP Port หมายเลข 53 ข้อมูลที่ทำการจัดเก็บประกอบด้วย หมายเลข IP Address ของเครื่องลูกข่ายที่ทำการร้องขอ เวลาที่ทำการร้องขอ และชื่อโดเมนที่ต้องการขอหมายเลข IP Address ข้อมูลทั้งหมดจะถูกเก็บบันทึกลงฐานข้อมูลในตารางชื่อ DNS ประกอบไปด้วยฟิลด์ SourceIP, QueryTime, และ DomainName ตามลำดับ

ข้อมูลกลุ่มที่ 2 คือ ข้อมูลการส่งจดหมายอิเล็กทรอนิกส์จากเครื่องลูกข่าย โดยสามารถดักจับได้จาก TCP Port หมายเลข 25 (SMTP) ข้อมูลที่ทำการจัดเก็บประกอบด้วยหมายเลข IP Address ของเครื่องลูกข่ายที่ทำการส่งจดหมายอิเล็กทรอนิกส์และเวลาที่ทำการส่งจดหมายอิเล็กทรอนิกส์ ข้อมูลทั้งหมดจะถูกบันทึกลงฐานข้อมูลในตารางชื่อ SMTP ประกอบไปด้วยฟิลด์ SendIP และ SendTimeStamp ตามลำดับ

2) ส่วนวิเคราะห์ข้อมูล (Analysis Module)

เมื่อได้รับข้อมูลจากส่วนรวบรวมข้อมูลแล้ว ระบบจะทำการตรวจสอบบอตเน็ตจากพฤติกรรมการสอบถามข้อมูล Domain Name ผ่านระบบ Domain Name System (DNS) และเทคนิคการตรวจสอบความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์ โดยเริ่มจากข้อมูลจากส่วน Collection Modue มาทำการวิเคราะห์ข้อมูลการร้องขอการตรวจสอบ Domain Name จากระบบ DNS โดยใช้วิธีหาค่า Semilarity จากแนวความคิดของ Choi เพื่อหากลุ่มของเครื่องที่เป็นบอตเน็ต

การวิเคราะห์จดหมายอิเล็กทรอนิกส์สแปมจะใช้วิธีการหาค่า Threshold แล้วนำมาเปรียบเทียบเพื่อระบุว่าเป็นจดหมายอิเล็กทรอนิกส์สแปมหรือไม่ มีขั้นตอนในการคำนวณค่า Threshold ดังนี้

a. กำหนดค่า Threshold สำหรับเริ่มต้นระบบ โดยพิจารณาการส่งจดหมายอิเล็กทรอนิกส์โดยเครื่องปรกติเป็นเวลา 1 สัปดาห์ โดยปรกติมีอัตราการส่งข้อมูลจดหมายอิเล็กทรอนิกส์ปรกติดอยู่ที่ 5 ฉบับต่อ 1 ชั่วโมง รวมเป็น 120 ฉบับต่อ 1 วัน

สูตรในการหาค่า Threshold ของจดหมายอิเล็กทรอนิกส์

THRESHOLD = MAX (จำนวนฉบับที่ส่งสูงสุด 7 วัน, จำนวนจดหมายอิเล็กทรอนิกส์ที่ส่งปรกติใน 1 วัน) + 1

(หรือ Thereshld = MAX + 1)

b. ทำการเปรียบเทียบหาค่าสูงสุด MAX ของการส่งข้อมูลใน 7 วันที่ผ่านมา โดยใช้สูตร MAX (ปริมาณการส่งสูงสุด ในรอบ 7 วัน, 120) หมายเลข 120 สามารถปรับค่าได้ตามความเหมาะสม

c. การกำหนดค่า Threshold โดยนำค่า MAX บวก 1 จะเป็นค่า Threshold โดยค่านี้จะแตกต่างกันในแต่ละเครื่อง ซึ่งค่า Threshold เครื่องใดก็จะใช้กับเครื่องคอมพิวเตอร์เครื่องนั้นเครื่องเดียว จะไม่ใช้กับการตรวจสอบทุกๆเครื่องในเครือข่าย

d. นำค่า Threshold ที่ได้เปรียบเทียบกับการส่งข้อมูลทั้งวันของวันที่ 8 เพื่อพิจารณาว่าเป็นจดหมายอิเล็กทรอนิกส์สแปมหรือไม่ *ถ้าค่าการส่งทั้งวันของวันที่ 8 สูงกว่าหรือเท่ากับค่า Threshold จะถือว่าเป็นการส่งจดหมายอิเล็กทรอนิกส์สแปม*

e. สำหรับเครื่องที่ถูกระบุว่าส่งข้อมูลจดหมายอิเล็กทรอนิกส์สแปมจะถูกลด Bandwidth ในการส่งจดหมายอิเล็กทรอนิกส์สแปม และเครื่องดังกล่าวจะถูกเก็บบันทึกประวัติว่าวันที่ 8 มีการส่งจดหมายอิเล็กทรอนิกส์สแปม พร้อมกับแจ้งให้ผู้ดูแลระบบทราบว่าเกิดปัญหากับเครื่องดังกล่าวแล้ว

f. สำหรับเครื่องที่เมื่อเปรียบเทียบข้อมูลวันที่ 8 แล้วไม่พบว่าเป็นการส่งจดหมายอิเล็กทรอนิกส์สแปม ระบบจะทำการเก็บค่าข้อมูลการส่งของวันที่ 8 เพื่อนำไปคำนวณค่า Threshold ใหม่ต่อไปโดยการคำนวณค่า Threshold ใหม่นี้จะไม่รวบวันที่เครื่องดังกล่าวพบการส่งจดหมายอิเล็กทรอนิกส์สแปม

g. กรณีที่เครื่องของผู้ใช้งานมีความจำเป็นที่ต้องการส่งจดหมายอิเล็กทรอนิกส์จำนวนมากๆ ผู้ดูและระบบ DSDSE จำเป็นต้องกำหนดหมายเลข IP Address ของเครื่องดังกล่าวเพื่อยกเว้นการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์แบบปรกติ แต่มีจำนวนมากๆ จากเครื่องของผู้ใช้

เมื่อได้ IP Address ทั้งในส่วนการร้องขอตรวจสอบ Domain Name และ IP ที่มีการส่งจดหมายอิเล็กทรอนิกส์ที่ผิดปรกติเมื่อเปรียบเทียบกับค่า Threshold จะสรุปได้ว่าเครื่องคอมพิวเตอร์เครื่องนั้นมีพฤติกรรมที่เป็นบอตเน็ต และส่งจดหมายอิเล็กทรอนิกส์สแปม หมายเลข IP Address ดังกล่าวจะถูกส่งเข้าสู่ส่วนควบคุม Bandwidth โดยส่วน Traffic Control เพื่อทำการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมต่อไป

3.1.2 ระบบ Traffic Control

ระบบ Traffic Control มีหน้าที่ในการควบคุม Bandwidth และการยกเลิกการควบคุม Bandwidth ของเครื่องคอมพิวเตอร์ที่ส่งจดหมายอิเล็กทรอนิกส์สแปม ผ่าน SMTP Port หมายเลข 25 ในการพิจารณา Bandwidth ที่เหมาะสมเพื่อควบคุมอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปม ผู้วิจัยนำเสนอรูปแบบการควบคุม Bandwidth 3 วิธีดังนี้

วิธีที่ 1 ใช้วิธีกำหนด Bandwidth ด้วยค่าคงที่ มีรายละเอียดดังนี้

เมื่อระบบ Detection ได้วิเคราะห์และระบุได้ว่าเป็นเครื่องบอตเน็ตส่งจดหมายอิเล็กทรอนิกส์สแปม ระบบจะส่งข้อมูลหมายเลข IP Address ที่ต้องการทำการควบคุมอัตราความเร็ว ให้กับระบบ Traffic Control ระบบ Traffic Control จะทำการควบคุมอัตราความเร็วในการส่งจดหมายอิเล็กทรอนิกส์ด้วยค่าคงที่เท่ากันตลอดเวลา ไม่ว่าปัญหาจะมาจาก IP Address ใด โดยค่าดังกล่าวจะถูกกำหนดไว้ล่วงหน้าโดยผู้ดูแลระบบ เช่น ผู้ดูแลระบบกำหนดค่าความเร็วไว้ที่ 1KB/s (กิโลไบต์ต่อวินาที) ดังนั้นเมื่อระบบพบว่า IP Address ใดที่มีปัญหา ระบบจะจำกัดอัตราในการส่งจดหมายอิเล็กทรอนิกส์ซึ่งถูกกำหนดไว้ที่ 1KB/s (ค่านี้จะกำหนดเท่ากันในทุก IP Address)

วิธีที่ 2 ใช้วิธีกำหนดค่า Bandwidth จากประวัติการใช้งานของแต่ละ IP Address ย้อนหลัง 1 สัปดาห์ ในวันและช่วงเวลาเดียวกัน มีรายละเอียดดังนี้

เมื่อระบบ Detection ได้ส่งข้อมูลหมายเลข IP Address ที่ต้องการทำการควบคุมอัตราความเร็วในการส่งจดหมายอิเล็กทรอนิกส์สแปม ให้กับระบบ Traffic Control ระบบ Traffic Control จะทำการควบคุมอัตราความเร็ว โดยพิจารณาจากประวัติการส่งจดหมายอิเล็กทรอนิกส์ของเครื่องคอมพิวเตอร์ IP Address นั้น ในวันและช่วงเวลาเดียวกันของสัปดาห์ที่ผ่านมาพิจารณาข้อมูลการส่งจดหมายอิเล็กทรอนิกส์ โดยแบ่งเป็นช่วงเวลา คือ ช่วง½ ชั่วโมงก่อนและหลัง ½ ชั่วโมง รวมเป็นเวลา 1 ชั่วโมง ในวันดังกล่าวว่า มีจำนวนข้อมูลที่ส่งออกไปเป็นขนาดเท่าไร แล้วนำมาคำนวณเป็นอัตราความเร็วในการส่งข้อมูล เช่นปัจจุบันเป็นวันที่ 8 เวลา 12.00 น. ประวัติการใช้งานที่จะถูกนำมาใช้คำนวณหาความเร็วจะนำมาจากวันที่ 1 เวลา11.30 ถึง12.30 น. ในช่วงเวลาดังกล่าวมีการส่งจดหมายอิเล็กทรอนิกส์ออกไป 100 ฉบับ ฉบับละ 36 KB รวมแล้วใน 1 ชม.มีการส่งข้อมูล 3.6 MB ต่อ 1 ชั่วโมง (3,600 วินาที) ซึ่งเมื่อนำมาคิดเป็นขนาดข้อมูลต่อวินาทีจะได้ 1 KB ต่อวินาที ค่าดังกล่าวจะนำมาใช้ในการจำกัดความเร็วในการส่งข้อมูลของเครื่องคอมพิวเตอร์ที่มีปัญหา (ผู้วิจัยใช้วิธีแบบที่ 2 ในการทดลองครั้งนี้)

วิธีที่ 3 โดยวิธีจัดสรร Bandwidth กลางสำหรับเครื่องที่เป็นบอตเน็ตทั้งระบบ

เมื่อมีเครื่องที่เป็นเครื่องบอตเน็ตเกิดขึ้นในระบบ จะสรร Bandwidth กลางโดยนำค่า Bandwidth ที่ตั้งไว้ หาร จำนวนเครื่องที่เป็นบอตเน็ต ผลลัพธ์ที่ได้จะเป็น Bandwidth ที่ถูกกำหนดให้แต่ละเครื่องที่เป็นบอตเน็ตใช้ในส่งข้อมูลจดหมายอิเล็กทรอนิกส์สแปม วิธีที่ 3 นี้ อาจจะเกิดผลกระทบที่เกิดกับผู้ใช้งานเครื่องที่เป็นบอตเน็ต กรณีที่มีบอตเน็ตจำนวนมากในระบบ ทำให้บางครั้งอาจจะไม่สามารถส่งจดหมายอิเล็กทรอนิกส์ได้เลยเนื่องจากจำนวนบอตเน็ตมากเกินไป

การยกเลิกการควบคุม Bandwidth เมื่อระบบทำการควบคุม Bandwidth ได้ระยะหนึ่ง ถ้าระบบวิเคราะห์พบว่า IP Address ที่ถูกควบคุมอยู่มีการวิเคราะห์ใหม่แล้วพบว่าไม่มีความผิดปรกติ ระบบ Detection จะสั่งไปที่ระบบ Traffic Control เพื่อยกเลิกการควบคุม Bandwidth ของเครื่องคอมพิวเตอร์เครื่องนั้น

3.1.3 อัลกอริธึมของระบบ DSDSE

ภาพที่ 3.4 อัลกอริทึมระบบ DSDSE

```
Do Interval
Begin
   IP_LIST[] <- Get_IPs()  (1)
   IP_DNS[] <- Get_IPs_Invalid_DNS_Query (dns_windows_size, dns_threshold) (2)
   IP_MAIL[] <- Get_IPs_Invalid_Mail_Quantity
                  (mail_windows_size, mail_threshold, no_of_day) (3)
   N <- NumberOf(IP_LIST[])
   For i=1 to N
   Begin
      IP <- IP_LIST[i]
      If IP Is MemberOf(IP_DNS) And IP Is MemberOf(IP_MAIL) (4)
           Limit_IP(IP)
      Else
           UnLimit_IP(IP)
    End
End
```

จากภาพที่ 3.4 มีรายละเอียดของอัลกอริธึมของระบบ DSDSE ดังนี้

1) เริ่มต้นด้วยการค้นหาเครื่องทั้งหมดในระบบ โดยฟังก์ชัน (Get_IPs())

2) ทำการค้นหา IP Address ที่เป็นบอตผ่านฟังก์ชัน (Get_IP_Invalid_DNS_-Query()) โดยการใช้วิธีพิจารณาค่า Similarity ของการสอบถาม Domain Name จากระบบ DNS

3) ทำการค้นหา IP Address ที่ส่งจดหมายอิเล็กทรอนิกส์สแปม โดยพิจารณาค่า Threshold ผ่าน (Get_IPs_Invalid_Mail_Quantity)

4) ในขั้นตอนสุดท้ายนำ IP Address มาตรวจสอบอีกครั้งโดยมีเงื่อนไขดังนี้ IP $\in$ IP_DNS[] และ IP $\in$ IP_MAIL[] ถ้าหากเงื่อนไขเป็นจริงระบบจะส่งหมายเลข IP Address ให้ระบบ Traffic Control เพื่อควบคุม Bandwidth สำหรับ IP Address นั้น โดยใช้ฟังก์ชัน IP (Limit_IP())

การยกเลิกการควบคุม Bandwidth จะพิจารณาจากเงื่อนไขที่เป็นเท็จ ระบบจะสั่งให้ระบบ Traffic Control ยกเลิกการควบคุม Bandwidth (UnLimit_IP()) ให้กับ IP Address ที่ไม่พบปัญหา

3.2 การเตรียมการทดลอง

การเตรียมการทดลองสำหรับทดสอบระบบ DSDSE ประกอบด้วยข้อมูล 3 ส่วน

3.2.1 การเตรียมการทดลองในส่วนการร้องขอข้อมูล Domain Name จากระบบ DNS

สำหรับการเตรียมการทดลองในส่วนนี้ จำเป็นต้องพิจารณาข้อมูลการร้องขอตรวจสอบชื่อ Domain Name จากระบบ DNS ของแต่ละเครื่อง ในการเตรียนมการทดลองได้รับข้อมูลรายชื่อ Domain Name จากบริษัทเอกชนแห่งหนึ่งที่ทำธุรกิจเกี่ยวกับการประกันภัย โดยมีจำนวน Domain Name ทั้งหมดประมาณ 700 รายชื่อ Domain Name ที่ใช้ในการทดลองครั้งนี้ แต่เนื่องจากการทดสอบในเบื้องต้น ไม่พบรายชื่อ Domain Name ใดที่ผิดปรกติ ดังนั้นผู้วิจัยจึงได้สร้างรายชื่อ Domain Name ชื่อ IRC.bot.com เพื่อกำหนดค่าเบื้องต้นไว้เป็น Domain Name ที่ผิดปรกติใส่รวมเข้ากับรายชื่อ Domain Name ทั้งหมด เพื่อใช้เป็นข้อมูลในการเปรียบเทียบ

3.2.2 การเตรียมการทดลองในส่วนของการส่งจดหมายอิเล็กทรอนิกส์

การเตรียมการทดลองในส่วนของจดหมายอิเล็กทรอนิกส์ มีการเตรียมข้อมูลสำหรับการทดลอง โดยใช้วิธีการจำลองการส่งจดหมายอิเล็กทรอนิกส์ทั้งแบบจดหมายปรกติ และ

จดหมายอิเล็กทรอนิกส์สแปม โดยกำหนดค่าความน่าจะเป็นในการส่งจดหมายอิเล็กทรอนิกส์สแปมในแบบต่างๆ เริ่มจากการกำหนดปริมาณบอตเน็ตที่ใช้ในการส่งจดหมายอิเล็กทรอนิกส์เริ่มต้นที่ จำนวนบอตเน็ต 10 20 30 40 50 60 70 80 90 100 เปอร์เซ็นต์ ซึ่งบอตเน็ตเหล่านี้มีความน่าจะเป็นในการส่งจดหมายอิเล็กทรอนิกส์สแปม เริ่มจาก 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 และ 1 ในแต่ละเปอร์เซ็นต์ของบอตเน็ตจะมีความน่าจะเป็นในการส่งจดหมายอิเล็กทรอนิกส์ครบทั้ง 10 กรณี

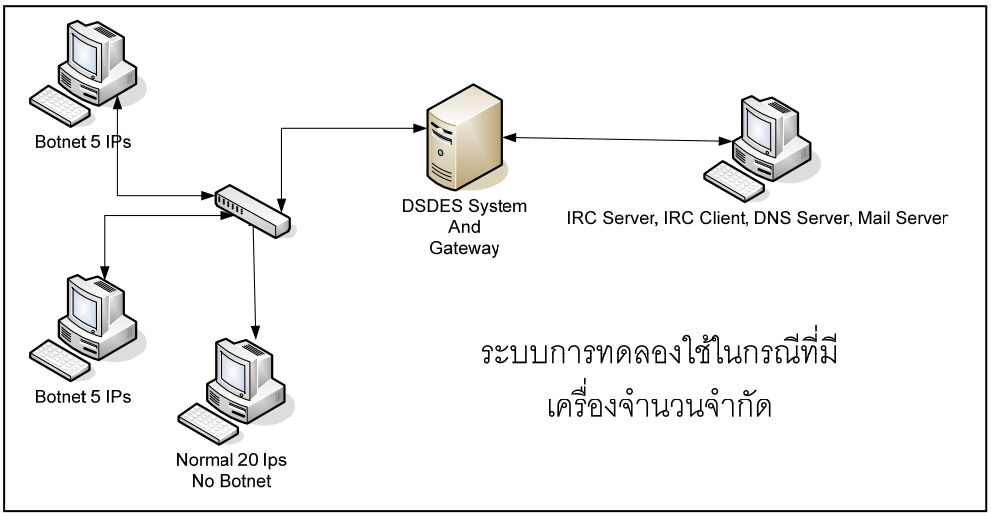
3.2.3 การเตรียมการทดลองในส่วนการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปม

การเตรียมการการทดลองในส่วนนี้ ได้ทดลองกำหนดเครื่องจำนวน 30 เครื่องโดยทั้ง 20 เครื่องมีการส่งจดหมายอิเล็กทรอนิกส์ปรกติ และอีก 10 เครื่องส่งจดหมายอิเล็กทรอนิกส์สแปม โดยบอตเน็ตที่นำมาใช้ในการส่งจดหมายอิเล็กทรอนิกส์สแปมคือ SDbot ซึ่งมีการติดต่อเพื่อรับคำสั่งในการส่งจดหมายอิเล็กทรอนิกส์สแปม ทุกๆ 3 นาที

3.2.4 รายละเอียดฮาร์ดแวร์และซอฟแวร์ที่ใช้ในการเตรียมทดลอง

การติดตั้งระบบฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) สำหรับการทดลองประกอบด้วย เครื่องคอมพิวเตอร์จำนวน 5 เครื่อง แบ่งเป็นเครื่องแม่ข่าย (Server) จำนวน 2 เครื่อง และเครื่องลูกข่าย (Client) จำนวน 3 เครื่อง แสดงดังภาพที่ 3.5

ภาพที่ 3.5 แสดงการวางระบบเครือข่ายที่ใช้สำหรับทำการทดลอง



จากภาพที่ 3.5 มีรายละเอียดดังนี้

1) เครื่องแม่ข่าย (Server) จำนวน 1 เครื่อง ทำหน้าที่เป็น Gateway ซึ่งติดตั้งระบบ DSDSE, SQL Database 2000, Windows 2000 Server, โปรแกรมควบคุมขนาด Bandwidth (Softperfect Bandwidth Manager), Internet Gateway เป็นโปรแกรมที่ทำให้เครื่องสามารถแชร์อินเตอร์เน็ตได้ (Internet Connectiong Sharing ที่มาพร้อมกับ Windows 2000), โปรแกรมตรวจวัดปริมาณข้อมูลเข้าและออกจากเครื่อง Server (Speed Test Network Analyzer) สามารถนำ Bandwidth ปัจจุบันที่มีการใช้งาน นำมาแสดงเป็นกราฟได้

2) เครื่องแม่ข่าย (Server) จำนวน 1 เครื่อง ติดตั้ง Windows 2000 Sever ลงโปรแกรม IRCServer โปรแกรม DNS Server Service ของ Windows 2000 Server SMTP/POP3 Mail Server ใช้ในการรับส่งจดหมายอิเล็กทรอนิกส์ (ชื่อ hMailServer) IRC Client สำหรับใช้ในการติดต่อกับเครื่องลูกข่ายที่เป็นบอตเน็ต ดังนั้นเครื่องแม่ข่ายที่ทำหน้าที่ส่งจดหมายอิเล็กทรอนิกส์จะมีเพียง 1 เครื่องเท่านั้น

3) เครื่องลูกข่าย (Client) จำนวน 3 เครื่อง ติดตั้ง Windows XP และใช้วิธีกำหนดหมายเลข IP Address ไว้จำนวน 30 IP Address เพื่อจำลองเป็นคอมพิวเตอร์ 30 เครื่อง โดยแบ่งเป็น IP Address ที่ทำงานส่งจดหมายอิเล็กทรอนิกส์ตามปรกติ จำนวน 20 IP Address, และ IP Address ที่เป็นบอตเน็ตและส่งจดหมายอิเล็กทรอนิกส์สแปม อีกจำนวน 10 IP Address

3.3 การดำเนินการทดลอง

3.3.1 การทดลองการร้องขอข้อมูล Domain Name จากระบบ DNS

การทดลองในส่วนนี้ จะอาศัยหลักการวิเคราะห์ของ Choi โดยอาศัยการหาค่า Threshold เพื่อใช้ในการเปรียบเทียบ และการคำนวณหาค่า Similarity ของแต่ละ Domain Name ที่เครื่องคอมพิวเตอร์ในเครือข่ายร้องขอเพื่อที่จะทำการติดต่อด้วย ถ้าค่า Similarity ที่ได้ของแต่ละ Domain Name นั้นเกินกว่าค่า Threshold ที่คำนวณได้ หมายถึง Domain Name นั้นเป็น Domain Name ที่บอตเน็ตพยายามติดต่อสื่อสารด้วย มีขั้นตอนการทดลองดังนี้

1) นำข้อมูลการร้องขอการตรวจสอบชื่อ Domain Name จริงที่ได้มา เพื่อคำนวณหาค่า Threshold ที่เหมาะสม

2) จำลองพฤติกรรมการร้องขอตรวจสอบ Domain Name ชื่อ irc.bot.com ซึ่งเป็น Domain Name ที่บอตเน็ตต้องการติดต่อด้วย

3) เริ่มการทำงานในส่วนของการวิเคราะห์ข้อมูล (Analysis) โปรแกรมที่ใช้คือ detection.exe ส่วนนี้จะเป็นส่วนที่ทำการวิเคราะห์ข้อมูลการตรวจสอบชื่อ Domain Name จากระบบ DNS โดยอาศัยการคำนวณหาค่า Threshold และการคำนวณค่า Semilarity

4) Domain Name ใดที่มีค่า Similarity เกินกว่าค่า Threshold ที่ตั้งไว้หมายถึง Domain Name นั้นมีกลุ่มเครื่องที่พยายามติดต่อด้วยจำนวนหลายเครื่องในเวลาเดียวกัน และเป็นกลุ่มเครื่องที่เป็นบอตเน็ต

3.3.2 การทดลองการส่งจดหมายอิเล็กทรอนิกส์

การทดลองในเรื่องการส่งจดหมายอิเล็กทรอนิกส์ มีการทดลองดังนี้

1) จำลองการส่งจดหมายอิเล็กทรอนิกส์ของเครื่องคอมพิวเตอร์จำนวน 100 เครื่อง

2) จำลองการส่งจดหมายอิเล็กทรอนิกส์สแปมจากอัตราบอตเน็ต 10 20 30 40 50 60 70 80 90 และ 100 เปอร์เซ็นต์ (บอตเน็ต 10 เปอร์เซ็นต์ หมายถึง เครื่องคอมพิวเตอร์ 100 เครื่องมีเครื่องคอมพิวเตอร์ที่เป็นบอตเน็ตจำนวน 10 เครื่อง)

3) ความน่าจะเป็นในการส่งจดหมายอิเล็กทรอนิกส์สแปมโดยเริ่มที่ 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 และ 1 ความน่าจะเป็นทั้ง 10 ค่านี้จะเป็นตัวกำหนดปริมาณการส่งจดหมายอิเล็กทรอนิกส์สแปมในทุกๆเปอร์เซ็นต์ของบอตเน็ต

4) เริ่มการส่งจดหมายอิเล็กทรอนิกส์แบบปรกติเป็นจำนวน 7 วัน

5) วันที่ 8 เริ่มการส่งจดหมายอิเล็กทรอนิกส์สแปมตามเปอร์เซ็นต์ของบอตเน็ตที่กำหนดไว้และความน่าจะเป็นของการส่งจดหมายอิเล็กทรอนิกส์สแปมทั้ง 10 ค่า

6) คำนวณหาค่า MAX และค่า Threshold

7) เปรียบเทียบข้อมูลวันที่ 8 กับค่า Threshold ที่ตั้งไว้ถ้ามากกว่าค่า Threshold จะถือว่าเครื่องคอมพิวเตอร์เครื่องนั้นส่งจดหมายอิเล็กทรอนิกส์สแปม

3.3.3 การทดลองการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต

ในส่วนนี้จะเป็นส่วนที่ทำการทดลองโดยอาศัยข้อมูลจากข้อ 3.3.1 และ 3.3.2 ประกอบการทดลอง มีขั้นตอนดังนี้

1) เก็บข้อมูล (Collection) การสอบถามรายชื่อ Domain Name จากระบบ DNS โดยเก็บข้อมูล IP Address ของเครื่องที่ร้องขอ เวลาที่ทำการร้องขอ และ Domain Name ที่

ต้องการร้องขอ (SourceIP, QueryTime, DomainName) บันทึกลงระบบฐานข้อมูลในตาราง DNS และใช้โปรแกรม WindumpG.exe (Windum GUI) เก็บข้อมูลความถี่การสอบถามระบบ DNS

2) เก็บประวัติการส่งจดหมายอิเล็กทรอนิกส์ โดยใช้โปรแกรม EmailS.exe (Email Statistic) เพื่อเก็บข้อมูลการส่งจดหมายอิเล็กทรอนิกส์ โดยข้อมูลที่เก็บ คือ หมายเลขเครื่องที่ทำการส่งจดหมายอิเล็กทรอนิกส์ ข้อมูลขนาดจดหมายอิเล็กทรอนิกส์ที่ส่งออก เวลาที่ทำการส่งจดหมายอิเล็กทรอนิกส์ ข้อมูลดังกล่าวนำมาเป็นประวัติการใช้งาน และใช้ในการพิจารณาการลดขนาด Bandwidth ต่อไป

3) เปิดระบบ IRC Server และติดตั้งระบบ Domain Name ของ Server ให้เป็น irc.bot.com จากนั้นจึงเปิดโปรแกรม IRC Client และทำการเชื่อมต่อไปที่ IRC Server เพื่อสร้างห้องสำหรับการสนทนาให้ระหว่างบอตเน็ตและผู้คุมบอตเน็ต

4) เปิดระบบการรับส่งจดหมายอิเล็กทรอนิกส์ เปิดระบบ SMTP server สำหรับการส่งจดหมายอิเล็กทรอนิกส์ โดยกำหนด Domain Name ของ SMTP/POP3 Sever ชื่อ mail.bot.com เพื่อให้บอตเน็ตใช้ส่งจดหมายอิเล็กทรอนิกส์และเปิดระบบรับจดหมายอิเล็กทรอนิกส์ POP3 ชื่อ mail.bot.com โดยทั้ง 2 ส่วนติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ 1

5) เปิดการใช้งาน DSDSE บนเครื่องคอมพิวเตอร์แม่ข่ายที่ 2 ซึ่งทำหน้าที่เป็น Gateway เริ่มเปิดระบบ Detection ประกอบไปด้วย 2 ส่วนคือ ส่วนเก็บข้อมูล Collection Data และส่วนการวิเคราะห์ Analysis และระบบ Traffic Control เพื่อเก็บข้อมูลจากเครื่องลูกข่าย และทำการวิเคราะห์ข้อมูล

6) เริ่มเก็บข้อมูล (Collection) การส่งจดหมายอิเล็กทรอนิกส์ที่ส่งออกมาจากเครื่องลูกข่าย ใช้โปรแกรม WindumpG.exe (Windum GUI) โดยเก็บข้อมูล IP Address ของเครื่องที่ทำการส่งจดหมายอิเล็กทรอนิกส์ และเวลาที่ทำการส่ง (SendIP และ SendTimeStamp)

7) เปิดโปรแกรม Softperfect bandwidth manager สำหรับควบคุม bandwidth โดยเปิดเป็น Service ตลอดเวลาซึ่งจะสามารถทำการลดอัตรา Bandwidth ได้ทันที

8) ส่วนของผู้ควบคุมบอตจะทำการเปิดห้องสนทนา IRC ที่ IRC Client เพื่อรอให้บอตเน็ตติดต่อเข้ามาโดยมีรูปแบบคำสั่งคือ .login password เพื่อเริ่มการติดต่อกับบอตเน็ต จากนั้นจึงเริ่มพิมพ์คำสั่งอื่น ๆ เพื่อสั่งให้บอตเน็ตทำงานตามคำสั่ง

9) เครื่องลูกข่ายที่ติดตั้งโปรแกรมบอตเน็ตไว้ ทำการเรียกโปรแกรมบอตเน็ตให้ทำงาน เมื่อบอตเน็ททำงานจะทำการเชื่อมต่อไปยัง IRC Server ที่มีการตั้งค่าไว้ ในการทดลองได้

ตั้งค่าไว้ที่ irc.bot.com โดยการสอบถามหา irc.bot.com จากระบบ DNS เพื่อหาทางเชื่อมต่อไปที่ IRC Server และทุก ๆ ครั้งเมื่อมีการตัดการเชื่อมต่อกับ IRC Server และต้องการเชื่อมต่อเข้าไปใหม่จะทำการสอบถามชื่อ Domain Name กับระบบระบบ DNS ใหม่อีกครั้ง เมื่อเชื่อมต่อกับ IRC Server แล้ว จากนั้นจึงเข้าไปยังห้องสนทนาที่กำหนดไว้ในโปรแกรม เพื่อทำการรอรับคำสั่งจากผู้ควบคุมบอตเน็ต เมื่อเชื่อมต่อเป็นเวลาครบ 3 นาทีแล้ว บอตเน็ตจะตัดการเชื่อมต่อแล้วทำการเชื่อมต่อเข้าไปใหม่ ทุกๆครั้งที่บอตเน็ตทำการเชื่อมต่อใหม่บอตเน็ตจะทำการเปลี่ยนชื่อตัวเองใหม่ทุกๆ ครั้งแล้วเข้ามาใหม่อีกครั้ง ผู้ควบคุมต้องทำการล็อกอินใหม่ทุกครั้งที่ต้องการจะสั่งงานบอตเน็ต

10) ระบบเริ่มสั่งให้บอตเน็ตทดลองส่งจดหมายอิเล็กทรอนิกส์จำนวน 2,000 ฉบับต่อหนึ่งเครื่องรวมทั้งหมด 10 เครื่อง และมีปริมาณจดหมายอิเล็กทรอนิกส์ทั้งหมด 20,000 ฉบับ

11) การทำงานของส่วนการวิเคราะห์ จะทำการวิเคราะห์ข้อมูลใน 1 วัน โดยการวิเคราะห์ค่าการร้องขอ Domain Name 10 ชั่วโมงย้อนหลัง และการส่งจดหมายอิเล็กทรอนิกส์พิจารณาย้อนหลัง 1 วัน

12) พิจารณาว่าเครื่องใดเป็นเครื่องบอตเน็ตจากพฤติกรรมการสอบถามข้อมูล Domain Name ผ่านระบบ DNS และความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์ โดยอาศัยค่า Similarity และค่า Threshold

13) ส่งหมายเลข IP Address ของเครื่องที่มีปัญหา ให้ระบบ Traffic Control เพื่อควบคุมอัตราการส่งข้อมูลจดหมายอิเล็กทรอนิกส์จาก IP Address เครื่องนั้น

14) ทดลองการลดอัตราการส่งข้อมูลโดยการควบคุม Bandwidth 3 วิธี

15) ดูปริมาณ Bandwidth ทั้งก่อนและหลังการทำงานของระบบ DSDSE

16) เปรียบเทียบกระบวนการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์ Bandwidth ทั้ง 3 วิธี โดยกราฟ

3.4 ข้อมูลเพิ่มเติมที่ใช้ในการทดลอง

3.4.1 ข้อมูลเกี่ยวกับจดหมายอิเล็กทรอนิกส์

จากข้อมูลการสำรวจการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องที่เป็นบอตเน็ตของ Securework Research.com และ Marshal.com แสดงให้เห็นว่าบอตเน็ตในปัจจุบันที่มีอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมสูงที่สุดคือ Srizbi โดยมีอัตราการส่ง 6,000 ล้านฉบับต่อวัน

(Stewart J, 2008) ดังนั้น เพื่อเป็นการประมาณการอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปม และนำมาวิเคราะห์ในงานวิจัยนี้ มีการคิดคำนวณดังนี้

Srizbi ส่งจดหมายทั้งหมดต่อวัน 6,000 ล้านฉบับ

เกิดจากบอตเน็ตประมาณ 315,000 บอตเน็ต

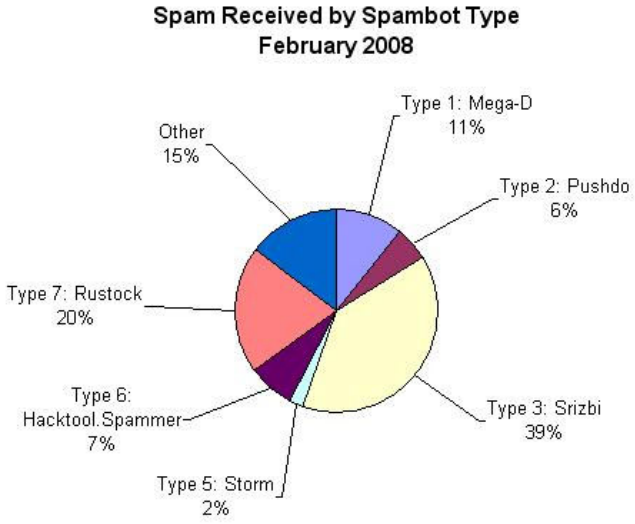
คิดค่าเฉลี่ยต่อบอตเน็ต 6,000(ล้าน)/315,000 = 19,048 ฉบับต่อวัน

ระบบที่ทำการทดลอง 1 บอตเน็ต ประกอบด้วยเครื่องที่เป็นบอต จำนวน 10 เครื่อง

ดังนั้น 1 บอต จะส่งจดหมายต่อวัน 19,048/10 = 1904.8 ฉบับต่อวัน

คิดเป็นแต่ละชั่วโมง (24 ชั่วโมง) จะได้ 1,904.8/24 = 79.37 ฉบับต่อชั่วโมง หรือ 80 ฉบับต่อชั่วโมง

ภาพที่ 3.6 อัตราส่วนการส่งจดหมายอิเล็กทรอนิกส์จากบอตเน็ตแต่ละประเภท



ที่มา : Marshal, 2008

3.4.2 ข้อมูลบอตเน็ตที่นำมาทดลอง

บอตเน็ตที่นำมาใช้ชื่อ SDbot มีพฤติกรรมการทำงานดังนี้

1) กำหนดให้ระบบมีบอตเน็ตอย่างน้อย 10 เครื่องที่ทำการส่งจดหมายอิเล็กทรอนิกส์สแปม

2) บอตเน็ตทำการติดต่อเพื่อสอบถาม Domain Name กับระบบ DNS ทุกๆ 3 นาที เพื่อติดต่อกับผู้ควบคุมบอตและรอรับคำสั่งให้ทำงานตามที่ผู้ควบคุมบอตต้องการ เช่น การส่งจดหมายอิเล็กทรอนิกส์สแปม เป็นต้น

3) ในการทดลองเกี่ยวกับจดหมายอิเล็กทรอนิกส์สแปม บอตเน็ตจะติดต่อเพื่อขอให้ผู้ควบคุมบอตสั่งให้ส่งจดหมายอิเล็กทรอนิกส์ โดยอาศัยความน่าจะเป็นที่บอตเน็ตจะทำการส่งจดหมายอิเล็กทรอนิกส์ 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 และ 1

4) ในการทดลองเพื่อทดสอบการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจะกำหนดให้บอตเน็ตส่งจดหมายต่อชั่วโมงเป็นจำนวน 2,000 ฉบับ มีบอตเน็ต 10 เครื่องรวมการส่งจดหมายต่อชั่วโมงเป็นจำนวน 20,000 ฉบับ และไม่นับรวมการส่งแบบ CC และ BC

5) SDbot มีการทำงานตลอดเวลา 24 ชั่วโมง

3.4.3 **รายละเอียดการสั่งงาน** SDbot

การสั่งให้ SDbot ส่งจดหมายอิเล็กทรอนิกส์สแปม สามารถทำได้โดยผ่านคำสั่ง .execute เนื่องจากบอตเน็ตไม่ใช่โปรแกรมที่ทำหน้าที่ส่งจดหมายอิเล็กทรอนิกส์ ดังนั้นบอตเน็ตจะไม่สามารถส่งจดหมายอิเล็กทรอนิกส์ได้ด้วยตัวเอง จำเป็นต้องอาศัยการเรียกใช้งานโปรแกรมอื่นๆ ให้ส่งจดหมายแทน โดยออกคำสั่งในลักษณะที่เป็นค่า Parameter หรือว่าเป็นโปรแกรมที่เขียนขึ้นมาเฉพาะสำหรับให้บอตเน็ตส่งจดหมายอิเล็กทรอนิกส์ ขึ้นอยู่กับความต้องการของผู้ควบคุมบอตเน็ต ในการส่งจดหมายอิเล็กทรอนิกส์โดย SDbot มีตัวอย่างขั้นตอนการส่ง ดังนี้

1) อัพโหลดโปรแกรมสำหรับส่งจดหมายอิเล็กทรอนิกส์ที่ต้องการใช้ ไฟล์ข้อมูลรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ที่ต้องการส่ง และไฟล์เนื้อหาของจดหมายอิเล็กทรอนิกส์ ไปยังเครื่องแม่ข่าย (HTTP Server) ที่ใดก็ได้

2) บอตเน็ตจะเข้ามาที่ช่องทางการสื่อสาร (Channel) ของระบบ IRC คำสั่งแรกที่ผู้ควบคุมบอตเน็ตสั่งคือ .login [passsword] เพื่อเริ่มการติดต่อกับเครื่องบอตเน็ต

3) ใช้คำสั่ง .download เพื่อให้บอตเน็ตรับข้อมูลโปรแกรมส่งจดหมายอิเล็กทรอนิกส์ ไฟล์ข้อมูลรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ และไฟล์เนื้อหาของจดหมายอิเล็กทรอนิกส์ จากเครื่องแม่ข่ายไปยังเครื่องที่เป็นบอตเน็ต

4) หลังจากที่ติดตั้งโปรแกรม และข้อมูลที่จำเป็นในการส่งจดหมายอิเล็กทรอนิกส์เรียบร้อยแล้ว ผู้ควบคุมบอตเน็ตจะใช้คำสั่ง .execute เพื่อเรียกโปรแกรมส่งจดหมายอิเล็กทรอนิกส์ให้เริ่มส่งจดหมายเป็นการเสร็จสิ้นขั้นตอนการส่งจดหมายอิเล็กทรอนิกส์สแปม

หมายเหตุ ปริมาณจดหมายอิเล็กทรอนิกส์ที่ถูกส่งออกมา พฤติกรรมการส่ง รวมถึงความถี่ในการส่ง ขึ้นอยู่กับความสามารถของโปรแกรมที่ผู้ควบคุมบอตเน็ตเลือกใช้ บางโปรแกรม

สามารถควบคุมระยะเวลาที่ใช้ในการส่งจดหมายอิเล็กทรอนิกส์ ระยะเวลาที่เว้นระหว่างจดหมายอิเล็กทรอนิกส์แต่ละฉบับ

3.4.4 **คำสั่งในการสั่งให้บอตเน็ตทำงาน**

ในการทดลองเพื่อทดสอบการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจะใช้โปรแกรมชื่อ Bot Mailer (sendmail.exe) ซึ่งเป็นโปรแกรมที่พัฒนาขึ้นเพื่อให้มีพฤติกรรมการส่งจดหมายอิเล็กทรอนิกส์ได้หลากหลาย ปรับเปลี่ยนได้ความต้องการ โดยโปรแกรมดังกล่าวมีรูปแบบการสั่งงานในลักษณะของชุดคำสั่ง (Command Line) ดังนี้

Sendmail.exe [-mode] [smtp_user]:[smtp_password]@[smtp_server] [sender_name]:[sender_email] [subject] [data] [email_list]

mode : เป็นการกำหนดลักษณะการส่ง e-mail ว่าจะส่งในรูปแบบใด

-s เป็นการส่งจดหมายอิเล็กทรอนิกส์เพียง 1 ฉบับ ไปถึงผู้รับ 1 คน

-l เป็นการส่งจดหมายอิเล็กทรอนิกส์ ไปถึงผู้รับปลายทางทุกรายชื่อที่มีอยู่ในรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์

-d เป็นการส่งจดหมายอิเล็กทรอนิกส์ ไปถึงผู้รับปลายทางทุกรายชื่อที่มีอยู่ในรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ และมีการหน่วงเวลาระว่างฉบับ

-r เป็นการส่งจดหมายอิเล็กทรอนิกส์ ไปถึงผู้รับปลายทางทุกรายชื่อที่มีอยู่ในรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ และมีการสุ่มเวลาหน่วงเวลาระว่างฉบับ

-t เป็นการส่งจดหมายอิเล็กทรอนิกส์ ไปถึงผู้รับปลายทางทุกรายชื่อที่มีอยู่ในรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ อย่างต่อเนื่องเป็นช่วงระยะเวลาที่กำหนด

smtp_user : user name สำหรับ login เพื่อใช้งาน smtp server

smtp_password : password สำหรับ login เพื่อใช้งาน smtp server

smtp_server : ชื่อ SMTP Server

sender_name : ชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (ไม่จำเป็นต้องใช้ชื่อจริง)

sender_email : ชื่อที่อยู่ผู้รับจดหมายอิเล็กทรอนิกส์ ของผู้ส่ง (ไม่จำเป็นต้องใช้ชื่อจริง)

subject : หัวข้อของจดหมายอิเล็กทรอนิกส์

data : ไฟล์เนื้อหาของจดหมายอิเล็กทรอนิกส์ที่ต้องการส่ง โปรแกรมนี้รองรับ text file

email_list : ข้อมูลรายชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ ที่โปรแกรมต้องการส่งส่งให้

ตัวอย่างการส่งคำสั่ง

sendmail –l admin:asdf@mail.bot.com WebMaster:webmaster@bot.com Help data.txt addslist.txt