บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของงานวิจัย

ในปัจจุบันระบบอินเตอร์เน็ต (Internet System) เข้ามามีบทบาทในการใช้งานในชีวิตประจำวันของคนทั่วไปมากขึ้น มีการนำระบบการเชื่อมต่อแบบอินเตอร์เน็ตความเร็วสูง (Broadband Internet) เข้ามาใช้งานทั้งในระดับองค์กร หน่วยงานธุรกิจ และภายในบ้านพักอาศัย รวมถึงการนำระบบอินเตอร์เน็ตเข้ามาใช้ในเรื่องการติดต่อสื่อสาร ซึ่งช่วยให้ผู้ใช้งานได้รับความสะดวกรวดเร็วและสามารถช่วยลดค่าใช้จ่ายในด้านการสื่อสารลงได้อย่างมาก ระบบสื่อสารผ่านอินเตอร์เน็ตที่นิยมมากในปัจจุบัน คือ การติดต่อสื่อสารผ่านระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail) หรือ อีเมล์ (E-mail) จดหมายอิเล็กทรอนิกส์สามารถนำมาใช้ในหลายลักษณะงาน เช่น การติดต่อเพื่อแลกเปลี่ยนข้อมูล การติดต่อทำธุรกรรมระหว่างองค์กร การรายงานผลต่างๆ เป็นต้น ด้วยเหตุนี้เอง บริษัทหรือกลุ่มคนบางกลุ่มจึงนำเอาข้อดีและประโยชน์ของการใช้งานจดหมายอิเล็กทรอนิกส์ นำมาใช้เป็นช่องทางในการแสวงหาผลประโยชน์ทางธุรกิจ โดยใช้วิธีการส่งจดหมายอิเล็กทรอนิกส์จำนวนมากๆ เพื่อประชาสัมพันธ์เกี่ยวกับสินค้า การบริการรวมถึงผลิตภัณฑ์ที่ต้องการนำเสนอ นำมาซึ่งปัญหามากมายกับผู้ที่รับจดหมายอิเล็กทรอนิกส์นั้น

ในปี ค.ศ. 1969 การเริ่มต้นของโครงการ ARPANET ถือเป็นจุดเริ่มต้นของการพัฒนาระบบอินเตอร์เน็ตในปัจจุบัน จุดเริ่มต้นของการส่งจดหมายอิเล็กทรอนิกส์สแปม (Spam E-mail) เริ่มแรกเกิดขึ้นเมื่อ วันที่ 3 พฤษภาคม ค.ศ.1978 โดยนาย Gary Thuerk ได้ทำการส่งจดหมายอิเล็กทรอนิกส์จำนวน 1 ฉบับ เพื่อโฆษณาสินค้าให้กับผู้ใช้งานอินเตอร์เน็ตจำนวน 600 คน ผ่านทางเครือข่ายของรัฐบาลและมหาวิทยาลัยต่างๆ (ARPANET) จุดประสงค์เพื่อทำการเผยแพร่และประชาสัมพันธ์โครงการบ้านในรัฐ Los Angeles and San Mateo (Streitfeld, 2003) หลังจากนั้นภายในปีเดียวกันก็มีการส่งจดหมายอิเล็กทรอนิกส์ในลักษณะเดียวกันอย่างแพร่หลายซึ่งสร้างความสูญเสียในเชิงธุรกิจถึง 10 ล้านดอลล่าร์สหรัฐ ในปี ค.ศ. 2003 ในปัจจุบันนี้จำนวนของจดหมายอิเล็กทรอนิกส์สแปมมีปริมาณเพิ่มขึ้นเป็น 3,100 ล้านฉบับต่อวันและเพิ่มขึ้นเป็น 9,700 ล้านฉบับต่อวันในปี ค.ศ. 2007 (Leggatt, 2007)

การสื่อสารผ่านจดหมายอิเล็กทรอนิกส์โดยปรกติแล้ว ผู้รับ (Recipient) ส่วนใหญ่มีการติดต่อสื่อสารกัน หรือ รู้จักคุ้นเคยในระดับหนึ่งกับผู้ส่ง (Sender) แต่ในบางครั้งผู้รับก็อาจได้รับการติดต่อจากบุคคลหรือหน่วยงานที่ตนเองไม่รู้จัก มักจะมีปริมาณของจดหมายอิเล็กทรอนิกส์ในลักษณะดังกล่าวถูกส่งเข้าในตู้จดหมาย (Inbox) ของตนเองมากผิดปรกติ นอกจากจะสร้างความรำคาญให้กับผู้รับแล้ว ผลที่ตามมาอาจสร้างความเสียหายอื่นๆ ให้กับผู้รับได้ในกรณีที่ผู้ส่งมีวัตถุประสงค์ที่ไม่ดี (Malicious Purpose) แอบแฝงมากับจดหมายอิเล็กทรอนิกส์ฉบับนั้น จดหมายอิเล็กทรอนิกส์ในลักษณะดังกล่าวเรียกว่า จดหมายอิเล็กทรอนิกส์ขยะ (Junk E-mail) หรือ จดหมายอิเล็กทรอนิกส์สแปม (Spam E-mail)

จดหมายอิเล็กทรอนิกส์สแปม หมายถึง จดหมายอิเล็กทรอนิกส์ปริมาณมาก ที่ถูกส่งออกมาให้ผู้รับโดยที่ผู้รับไม่ได้ร้องขอและไม่ต้องการ (Unsolicited E-mail) โดยส่วนมากจะทำให้เกิดความไม่พึงพอใจกับผู้รับจดหมายฉบับนั้น (Hershkop, 2006:24)

ลักษณะของจดหมายอิเล็กทรอนิกส์สแปมที่พบมากที่สุด คือ จดหมายอิเล็กทรอนิกส์สแปมในเชิงธุรกิจ (Unsolicited Commercial E-mail (UCE)) จดหมายลักษณะดังกล่าวมีการส่งมาจากทั้งภายในและภายนอกประเทศ นอกจากสร้างความรำคาญให้กับผู้รับและเสียเวลาในการจัดการกับจดหมายอิเล็กทรอนิกส์สแปมจำนวนมากที่ถูกส่งมาจากคนที่ตนเองไม่รู้จักแล้วยังอาจจะทำให้จำนวนพื้นที่เก็บข้อมูลจดหมาย (Mail Box) ในเครื่องแม่ข่าย (E-mail Server) มีโอกาสเต็มจนไม่สามารถรับข้อมูลที่สำคัญและข้อมูลที่เกี่ยวข้องกับงานได้ รวมถึงส่งผลกระทบกับภาพรวมการทำงานของระบบเครือข่ายที่ทำงานได้ช้าลงเนื่องจากต้องรองรับปริมาณข้อมูลที่ไม่เป็นประโยชน์ที่ส่งผ่านไปมาในเครือข่าย

ปัญหาที่เกิดจากการได้รับจดหมายอิเล็กทรอนิกส์สแปม ได้เพิ่มระดับความรุนแรงมากขึ้นเรื่อยๆ นอกจากจะสร้างความรำคาญใจให้กับผู้ใช้แล้วยังสร้างความเสี่ยงที่ร้ายแรงให้กับระบบธุรกิจ ถึงแม้ว่าระบบการบริหารจัดการระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานต่างๆ จะมีระบบป้องกันที่สามารถจัดการกับปริมาณจดหมายอิเล็กทรอนิกส์สแปมจำนวนมาก (Anti-Spam E-mail) แต่ปัญหาดังกล่าวยังคงมีอยู่ เนื่องจากผู้พัฒนาจดหมายอิเล็กทรอนิกส์สแปม (Spammer) ได้พัฒนารูปแบบวิธีการใหม่ๆ เพื่อที่จะรอดพ้นจากการตรวจสอบของระบบป้องกันจดหมายอิเล็กทรอนิกส์สแปม (Spam Filter) ในอดีตระบบป้องกันจดหมายอิเล็กทรอนิกส์สแปม ใช้วิธีการกรองจดหมายอิเล็กทรอนิกส์สแปมออกจากจดหมายอิเล็กทรอนิกส์ทั่วๆไป โดยอาศัยหลักการพิจารณารายละเอียดข้อความภายใน (Content-Based) และคำศัพท์บางคำที่เข้าข่ายว่าเป็นจดหมายอิเล็กทรอนิกส์สแปม ผลลัพธ์ที่ได้คือ จดหมายอิเล็กทรอนิกส์สแปมสามารถถูกกำจัดหรือ

กรองออกไปได้ในระดับหนึ่ง ด้วยเหตุนี้ผู้พัฒนาจดหมายอิเล็กทรอนิกส์สแปมจึงได้พัฒนารูปแบบในการส่งที่แตกต่างออกไป เช่น การส่งจดหมายอิเล็กทรอนิกส์สแปมพร้อมกับการแนบไฟล์ (Attachment) การส่งโปรแกรมที่มีวัตถุประสงค์ไม่ดีต่อผู้รับ (Malicious Purpose) การส่งไฟล์รูปภาพ ไฟล์ PDF รวมถึงไฟล์โปรแกรมตารางการคำนวณ (Microsoft Office Excel) เป็นต้น วัตถุประสงค์เพื่อเพิ่มระดับความสนใจในการเปิดดูข้อมูลมากยิ่งขึ้น ปัญหาที่พบคือ ข้อมูลดังกล่าวมักจะไม่ถูกกรองออกจากระบบป้องกันจดหมายอิเล็กทรอนิกส์สแปมทั่วไป (Sophos white paper, 2007) เมื่อผู้รับเกิดความสนใจและเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์สแปมฉบับนั้น กลับพบแต่ข้อมูลที่ไม่เป็นประโยชน์และบางทีก็เป็นเพียงข้อความธรรมดาที่ไม่มีความผิดปรกติใดๆ แต่ภายในระบบการทำงานของคอมพิวเตอร์ได้รับผลกระทบหลังจากเปิดไฟล์แนบดังกล่าวแล้ว โดยมีกระบวนการบางอย่างที่ทำหน้าที่ตามที่ผู้พัฒนาจดหมายอิเล็กทรอนิกส์สแปมต้องการให้กระทำ เช่น การลักลอบแอบส่งข้อมูลที่เป็นความลับของบริษัทไปให้บริษัทอื่นที่เป็นคู่แข่ง ขโมยข้อมูลเลขที่บัตรเครดิต ลักลอบดูข้อมูลเกี่ยวกับการเงิน หรือเครื่องของผู้รับอาจตกเป็นเครื่องมือในการแพร่กระจายจดหมายอิเล็กทรอนิกส์สแปม โดยกลายเป็นสมาชิกของบอตเน็ต (Botnet) โดยที่ผู้ใช้งานอาจจะไม่สามารถทราบได้เลยว่าเครื่องตัวเองเป็นผู้ส่งจดหมายอิเล็กทรอนิกส์สแปม รวมถึงการติดโทรจัน (Trojan) หนอนอินเตอร์เน็ต (Internet Worm) และไวรัสคอมพิวเตอร์ (Computer Virus) ไปยังเครื่องอื่นๆ ในองค์กรได้ เหตุการณ์ดังกล่าวผู้ใช้งานทั่วไปไม่สามารถรับทราบได้เลยถ้าระบบที่ใช้ไม่มีระบบควบคุมและการป้องกันที่ดีพอ

ผู้พัฒนาจดหมายอิเล็กทรอนิกส์สแปมทราบเสมอว่าการส่งจดหมายอิเล็กทรอนิกส์สแปมเป็นงานที่เสี่ยงเพราะในปัจจุบันได้มีกฎหมายเพื่อควบคุมเรื่องดังกล่าวและเป็นความผิดในด้านกฎหมายอาญา ผู้พัฒนาจะเลิกส่งจดหมายอิเล็กทรอนิกส์สแปมก็ต่อเมื่อถูกตรวจสอบและจับกุมเข้าห้องขังแล้วเท่านั้น

จากปัญหาที่กล่าวมา สามารถสรุปเป็นประเด็นในการพิจารณาได้ดังนี้ ประวัติของจดหมายอิเล็กทรอนิกส์สแปม ผลกระทบที่เกิดจากจดหมายอิเล็กทรอนิกส์สแปม รูปแบบและวิวัฒนาการของการส่งจดหมายอิเล็กทรอนิกส์สแปม และรูปแบบในการป้องกันในปัจจุบัน

1.2 วัตถุประสงค์ของงานวิจัย

1.2.1 ศึกษารูปแบบการทำงานของบอตเน็ตที่ส่งจดหมายอิเล็กทรอนิกส์สแปม

1.2.2 ศึกษารูปแบบจดหมายอิเล็กทรอนิกส์ และจดหมายอิเล็กทรอนิกส์สแปมที่ถูกส่งออกมาจากเครื่องปรกติและเครื่องบอตเน็ต

1.2.3 ออกแบบและพัฒนาระบบตรวจสอบบอตเน็ต และระบบลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต

1.3 สมมุติฐานของงานวิจัย

1.3.1 พฤติกรรมการสอบถามข้อมูล Domain Name เดียวกันของกลุ่มเครื่องคอมพิวเตอร์ผ่านระบบ DNS และความผิดปรกติในการส่งจดหมายอิเล็กทรอนิกส์ สามารถระบุได้ว่าเป็นพฤติกรรมของบอตเน็ตที่ส่งจดหมายอิเล็กทรอนิกส์สแปม

1.3.2 การลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมของเครื่องที่ถูกระบุว่าเป็นบอตเน็ตและมีพฤติกรรมส่งจดหมายอิเล็กทรอนิกส์สแปม สามารถช่วยให้มีการใช้ Banwidth ได้มีประโยชน์มากขึ้น

1.4 ขอบเขตงานวิจัย

1.4.1 ศึกษารูปแบบพฤติกรรมการทำงานของบอตเน็ต ลักษณะการติดต่อสื่อสารระหว่างบอตเน็ตและผู้ควบคุมบอตเน็ต โดยการเก็บประวัติการตรวจสอบ Domain Name จากระบบ DNS ของเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายจำนวน 1 เครือข่าย

1.4.2 จำลองการส่งจดหมายอิเล็กทรอนิกส์จากเครื่องคอมพิวเตอร์ปรกติและเครื่องคอมพิวเตอร์ที่ถูกระบุว่าเป็นบอตเน็ต ภายใต้เงื่อนไขการจำลองการส่งจดหมายอิเล็กทรอนิกส์ผ่านเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์จำนวน 1 เครื่อง

1.4.3 ทดสอบการควบคุม Bandwidth เพื่อลดอัตราการส่งจดหมายอิเล็กทรอนิกส์จากเครื่องที่ถูกระบุว่าเป็นบอตเน็ต

1.5 นิยามตัวแปร

1.5.1 จดหมายอิเล็กทรอนิกส์ (Electronic Mail, E-Mail)

เป็นระบบการสื่อสารผ่านระบบอินเตอร์เน็ต ซึ่งมีปริมาณการใช้งานรองจากเวิลด์ไวด์เว็บ (World Wide Web) รูปแบบการทำงานของจดหมายอิเล็กทรอนิกส์ พัฒนามาจากรูปแบบการส่งจดหมายธรรมดา (Post Mail) แต่ข้อได้เปรียบของจดหมายอิเล็กทรอนิกส์ คือ ความรวดเร็วในการรับ-ส่ง ซึ่งเร็วกว่าการส่งจดหมายแบบเดิมและยังเสียค่าใช้จ่ายที่ถูกกว่า ข้อมูลสามารถส่งผ่านระบบจดหมายอิเล็กทรอนิกส์ เป็นได้ทั้งข้อความธรรมดา รูปภาพ ไฟล์ข้อมูล เสียง หรือ วิดีโอ (ส่งทั้งภาพและเสียง)

1.5.2 จดหมายอิเล็กทรอนิกส์สแปม (Spam E-mail)

จดหมายอิเล็กทรอนิกส์สแปม หมายถึง การส่งจดหมายอิเล็กทรอนิกส์ไปให้ผู้รับหลายคน (Recipients) และมีปริมาณมาก (Bulk E-mail) เพื่อวัตถุประสงค์ในการโฆษณาหรือผลประโยชน์ทางธุรกิจ เรียกอีกอย่างหนึ่งว่า จดหมายขยะ (Junk E-mail)

1.5.3 บอต บอตเน็ต และเครื่องซอมบี้ (Bot, Botnet and Zombie PCs)

บอต (Bot) เป็นหุ่นยนต์ทางซอฟท์แวร์ ถูกสร้างเพื่อวัตถุประสงค์ให้เครื่องคอมพิวเตอร์สามารถทำงานตามคำสั่งที่ต้องการได้แบบอัตโนมัติ บอตเน็ต (Botnet) หมายถึง กลุ่มเครื่องคอมพิวเตอร์ที่เป็น Bot (กมล เขมมะรังษี, กิติศักดิ์ จิรวรรณกุล, 2548) ลักษณะของเครื่องคอมพิวเตอร์ที่เป็นบอตเน็ต จะมีคุณสมบัติเฉพาะคือ กระบวนการรับคำสั่งและการควบคุม (Command and Control) จากผู้ควบคุมบอตเน็ต (Botnet Master) ซึ่งเป็นพฤติกรรมเฉพาะและแตกต่างจากมัลแวร์ (Malware) ชนิดอื่นๆ เช่น หนอนอินเตอร์เน็ต (Internet Worms) และไวรัสคอมพิวเตอร์ (Computer Virus) เพื่อรอรับคำสั่งให้ทำงานตามที่ผู้ควบคุมบอต (Baylor, Brown, 2003) (Chris A) และ (Lanelli, Hackworth, 2007)

หมายเหตุ สำหรับงานวิจัยนี้ ผู้วิจัยใช้คำว่า บอตเน็ต แทนคำว่า บอต และ เครื่องซอมบี้

1.5.4 ผู้ควบคุมบอต (Botnet Master)

หมายถึง บุคคลผู้ที่พัฒนาบอต ทำหน้าที่คอยควบคุมและสั่งการเครื่องบอต และกลุ่มเครื่องบอตเน็ต ซึ่งบอตและบอตเน็ตจะมีหน้าทีรอรับคำสั่งและการติดต่อจากผู้ควบคุมบอตเสมอ

1.5.5 Bandwidth

หมายถึง การวัดค่าความเร็วในการส่งข้อมูล ส่วนมากมักวัดความเร็วของการส่งข้อมูลเป็น บิตต่อวินาที (bps) หรือจะมองว่า Bandwidth คือ ความกว้างของเส้นทางในการรับส่ง

ข้อมูลซึ่งถ้ามี Bandwidth ที่กว้างจะทำให้รับการส่งข้อมูลได้เร็วมากขึ้น ถ้าความกว้างน้อยก็จะส่งข้อมูลได้ช้าลง

1.5.6 Detecting and Slowing Down Spam E-mail System (DSDSE)

ระบบ DSDSE เป็นระบบที่พัฒนาขึ้น เพื่อใช้ในการตรวจสอบเครื่องคอมพิวเตอร์ที่เป็นบอตเน็ต และลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต ระบบ DSDSE จะถูกติดตั้งไว้ที่เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเกตเวย์ (Gateway) และแบ่งหน้าที่การทำงาน 2 ระบบย่อยคือ ส่วนตรวจสอบ (Detection) และส่วนควบคุมการส่งข้อมูล (Traffic Control) ระบบ DSDSE จะทำหน้าที่ตรวจสอบความผิดปรกติของข้อมูลความถี่ในการสอบถามชื่อ Domain Name จากระบบ DNS และข้อมูลความถี่ของการส่งจดหมายอิเล็กทรอนิกส์ เมื่อเครื่องคอมพิวเตอร์เครื่องใดตรวจสอบโดยระบบ DSDSE แล้วมีเงื่อนไขทั้ง 2 กรณี ระบบจะควบคุมการส่งออกจดหมายอิเล็กทรอนิกส์ ซึ่งเรียกส่วนนี้ว่า Traffic Control โดยวิธีการควบคุมอัตราความเร็วของ Bandwidth ผลลัพธ์ที่ได้ทำให้การส่งออกจดหมายอิเล็กทรอนิกส์สแปมส่งออกได้ช้าลง

1.5.7 Domain Name System (DNS)

DNS คือ Domain Name System เป็นระบบที่ให้บริการ แปลงชื่อ Domain Name เป็นหมายเลข IP Address เนื่องจากตัวเลข IP Address ไม่สะดวกในการที่จดจำ ด้วยเหตุนี้จึงมีการคิดระบบตั้งชื่อแบบที่เป็นตัวอักษร ให้มีความหมายเพื่อการจดจำได้ง่ายขึ้น เช่น www.tu.ac.th เป็นต้น ระบบ DNS ทำหน้าที่คล้ายสมุดโทรศัพท์ เมื่อต้องการสื่อสารกับคอมพิวเตอร์เครื่องอื่นๆ เครื่องคอมพิวเตอร์เครื่องนั้นจะทำการสอบถามหมายเลข IP Address ของเครื่องที่ต้องการติดต่อด้วยกับระบบ DNS โดยระบบ DNS จะทำการค้นหาหมายเลขดังกล่าวในฐานข้อมูลแล้วแจ้งกลับให้โฮสต์ดังกล่าวทราบว่า Domain Name นั้นมี IP Address เป็นอะไร

1.5.8 Similarity

ความคล้ายคลึงกัน หรือมีพฤติกรรมแบบเดียวกัน ในงานวิจัยนี้นำมาใช้กับการหากลุ่มของเครื่องคอมพิวเตอร์ที่ร้องขอให้ตรวจสอบ Domain Name เดียวกันจากระบบ DNS

1.5.9 การวิเคราะห์ค่าความถูกต้อง 4 ประเภท

True Positive (TP)	หมายถึง	จำนวนเครื่องที่ส่งจดหมายอิเล็กทรอนิกส์สแปมและระบบสามารถระบุถูกว่าส่งจริง
False Positive (FP)	หมายถึง	จำนวนเครื่องปรกติที่ส่งจดหมายอิเล็กทรอนิกส์ปรกติแต่ระบบระบุผิดว่าเป็นเครื่องบอตเน็ตส่งจดหมายอิเล็กทรอนิกส์สแปม
False Negative (FN)	หมายถึง	จำนวนเครื่องที่ส่งจดหมายอิเล็กทรอนิกส์สแปม แต่ระบบระบุผิดว่าไม่ส่งจดหมายอิเล็กทรอนิกส์สแปม

True Negative (TN) หมายถึง จำนวนเครื่องที่ไม่ส่งจดหมายอิเล็กทรอนิกส์สแปมและระบบระบุถูกว่าไม่ส่งจดหมายอิเล็กทรอนิกส์สแปม

1.6 ประโยชน์ที่ได้รับจากงานวิจัย

1.6.1 ระบบที่พัฒนาขึ้น สามารถช่วยตรวจหาเครื่องบอตเน็ตในระบบเครือข่ายได้

1.6.2 สามารถควบคุมอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมโดยใช้วิธีการลดขนาด Bandwidth ของเครื่องบอตเน็ตที่กำลังส่งจดหมายอิเล็กทรอนิกส์สแปมได้

1.6.3 สามารถนำ Bandwidth ที่ถูกนำไปใช้ในการส่งจดหมายอิเล็กทรอนิกส์สแปมกลับคืนมาใช้ในงานด้านอื่นๆ ได้เต็มประสิทธิภาพมากขึ้น

1.7 รายละเอียดของวิทยานิพนธ์

รายละเอียดของวิทยานิพนธ์ฉบับนี้ ประกอบไปด้วยส่วนต่างๆ ดังนี้

บทที่ 1 บทนำ ประกอบไปด้วย ความเป็นมาและความสำคัญของงานวิจัย วัตถุประสงค์ของงานวิจัย สมมุติฐานของงานวิจัย ขอบเขตของงานวิจัย นิยามตัวแปร ประโยชน์ที่ได้รับจากงานวิจัย และรายละเอียดของวิทยานิพนธ์

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง ประกอบไปด้วย ทฤษฎีการทำงานของระบบจดหมายอิเล็กทรอนิกส์ ทฤษฎีการทำงานของบอตเน็ต และงานวิจัยที่เกี่ยวข้องกับจดหมายอิเล็กทรอนิกส์สแปมและบอตเน็ต กรอบแนวความคิดงานวิจัย

บทที่ 3 วิธีการดำเนินการวิจัย ประกอบไปด้วย ขอบเขตการวิจัย รายละเอียดฮาร์ดแวร์และซอฟต์แวร์ การออกแบบระบบ DSDSE การเตรียมการทดลอง การดำเนินการทดลอง ข้อจำกัดของระบบที่ใช้ในการทดลอง

บทที่ 4 ผลการของการวิจัย ประกอบไปด้วย ผลการทดลอง

บทที่ 5 สรุปผลการศึกษา ประกอบไปด้วย สรุปผลการทดสอบสมมุติฐาน และข้อเสนอแนะแนวทางการพัฒนาต่อ