ICT 2559/17

Blue Botnet

โดย

1. นายประกาศิต	วงษ์แวง	รหัสนักศึกษา 573020425-9
2. นายอัครพล	สุนทรศารทูล	รหัสนักศึกษา 573020449-5
3. นายชิดชัย	สารวงษ์	รหัสนักศึกษา 573021137-9
4. นางสาวมลิวัลย์	สวนหนองแวง	รหัสนักศึกษา 573021158-1
5. นางสาวศิริพร	สังข์ปิติกุล	รหัสนักศึกษา 573021167-0
6. นางสาวสุภาวดี	สุทธิรักษ์	รหัสนักศึกษา 573021173-5

อาจารย์ที่ปรึกษา: รศ.ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322 376 Information and Communication Technology Security
ภาคเรียนที่ 1 ปีการศึกษา 2559
สาขาเทคโนโลยีสารสนเทศและการสื่อสาร
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
มหาวิทยาลัยขอนแก่น
(เดือนพฤศจิกายน พ.ศ.2559)

คำนำ

ในปัจจุบันมนุษย์ได้พัฒนาเทคโนโลยีให้ทันสมัยและสะดวกรวดเร็วมากยิ่งขึ้น ไม่ว่าจะเป็นเทคโนโลยีด้านอุตสาหกรรม เทคโนโลยีทางการแพทย์และเทคโนโลยีด้านคอมพิวเตอร์ ซึ่งเทคโนโลยีที่สามารถเข้าถึงผู้คนได้อย่าง

แพร่หลายคือด้านคอมพิวเตอร์ แต่ปัญหาที่มาพร้อมกับเทคโนโลยีด้านคอมพิวเตอร์คือ ปัจจุบันมีภัยคุกคามต่อผู้ใช้ในระบบอินเตอร์เน็ตหลายรูปแบบและแพร่หลายเป็นจำนวนมากซึ่งเกิดขึ้นได้อย่างรวดเร็ว จึงมีการพัฒนารูปแบบการโจมตีในระบบเครือข่ายอินเตอร์เน็ตเพื่อสร้างความเสียหายให้แก่ระบบ จะมีการโจมตีในระบบเครือข่ายเป็นจำนวนมาก โดยที่แฮกเกอร์สามารถควบคุมเครื่องได้จากระยะไกลเพื่อใช้ในการกอบกิจกรรมที่ขัดต่อกฎหมายและล้วงข้อมูลที่สำคัญของผู้ใช้งานจึงมีการศึกษาวิธีการเพิ่มความระมัดระวังในการอุดช่องโหว่ของระบบปฏิบัติการในการป้องกันบอทเน็ต

คณะผู้จัดทำ

1. หลักการและเหตุผล

ปัจจุบันมีภัยคุกคามต่อผู้ใช้ในระบบอินเตอร์เน็ตหลายรูปแบบและแพร่หลายเป็นจำนวนมากซึ่งเกิดขึ้นได้อย่างรวดเร็ว จึงมีการพัฒนารูปแบบการโจมตีในระบบเครือข่ายอินเตอร์เน็ตเพื่อสร้างความเสียหายให้แก่ระบบและใช้เป็นเครื่องมือในการประกอบอาชญากรรมทางคอมพิวเตอร์ โดยจะมีความรุนแรงแตกต่างกันไปตามชนิดของการโจมตี

ซึ่งการใช้งานคอมพิวเตอร์ของผู้ใช้งานส่วนใหญ่ ไม่ว่าจะเป็นระดับทั่วไปหรือระดับองค์กรต่างๆ จะมีการโจมตีในระบบเครือข่ายเป็นจำนวนมาก โดยที่แฮกเกอร์สามารถควบคุมเครื่องได้จากระยะไกลเพื่อใช้ในการกอบกิจกรรมที่ขัดต่อกฎหมายและล้วงข้อมูลที่สำคัญของผู้ใช้งาน ซึ่งเครื่องที่ถูกควบคุมเหล่านี้จะถูกเรียกว่า“botnet”,”zombies” หรือ “drones”

จากข้อมูลข้างต้น ทำให้ทราบถึงความสามารถของผู้ใช้งานคอมพิวเตอร์ทั่วไปที่ยังขาดความเข้าใจถึงการป้องกันความปลอดภัยแก่เครื่องคอมพิวเตอร์ของตนเอง จึงมีการศึกษาวิธีการเพิ่มความระมัดระวังในการอุดช่องโหว่ของ

ระบบปฏิบัติการในการป้องกันบอทเน็ต ผู้จัดทำจึงได้อธิบายหลักการทำงานของบอตเน็ต ผลกระทบของภัยคุกคาม และวิธีการป้องกันหรือวิธีแก้ไข ซึ่งในที่นี้จะใช้โปรแกรม blue botnet ในการศึกษาแนวทางในการโจมตีและป้องกัน

2. วัตถุประสงค์

2.1 เพื่อทดสอบหรือตรวจสอบระบบความปลอดภัยของคอมพิวเตอร์

2.2 เพื่อศึกษาการใช้โปรแกรม blue botnet

3. ประโยชน์ที่คาดว่าจะได้รับ

3.1 ได้รู้ถึงกระบวนการของ botnet

3.2 ได้รู้ถึงความสามารถของระบบความปลอดภัยของคอมพิวเตอร์

3.3 ได้เรียนรู้วิธีการในการโปรแกรม เพื่อสามารถไปพัฒนาในระบบความปลอดภัยของตนเองได้

4. ทฤษฎีที่เกี่ยวข้อง

4.1.1 บอตเน็ต (BOTNET) หรือ roBOT NETwork

คือภัยคุกคามต่อผู้ใช้งานอินเทอร์เน็ตรูปแบบใหม่ ซึ่งแฮ็กเกอร์เขียนโปรแกรมบอตเน็ตโดยใช้เทคนิคการโจมตีเครือข่ายอินเทอร์เน็ตด้วยโปรแกรมประสงค์ร้าย (Malware) ที่ซับซ้อนและมีรูปแบบที่หลากหลายกว่าไวรัสคอมพิวเตอร์หรือหนอนอินเทอร์เน็ตทั่วไป บอตเน็ตที่ถูกสร้างขึ้นนี้อาจเป็นเครื่องมือที่ใช้ส่งสแปมเมล์ (Spam Mail) และ Phishing ซึ่งเป็นวิธีการสร้างความเสียหายให้กับระบบเครือข่ายอินเทอร์เน็ตได้ นอกจากนี้พบว่ามีการนำบอตเน็ตไปใช้เป็นเครื่องมือประกอบอาชญากรรมทางคอมพิวเตอร์อื่น ๆ อีกด้วย เช่น การขู่กรรโชกทรัพย์ ซึ่งจะกล่าวให้ทราบต่อไป เป็นต้นจากข้อมูลรายงานระยะหลังพบว่าภัยคุกคามจากไวรัสคอมพิวเตอร์และหนอนอินเทอร์เน็ตมีระดับความรุนแรงลดลงเมื่อเทียบกับปัญหาที่เกิดจากบอตเน็ต ล่าสุดในต้นปี พ.ศ. 2548 กลุ่มนักวิจัยชาวรัสเซียใน Kaspersky Lab ได้ประมาณการว่า อาจจะมีเครื่องคอมพิวเตอร์ถูกบุกรุกและลักลอบใช้ เพื่อทำให้กลายเป็นส่วนหนึ่งของบอตเน็ตเพิ่มขึ้นถึง 50,000 เครื่องต่อเดือน ซึ่งแสดงให้เห็นว่าอัตราการขยายตัวของบอตเน็ตอยู่ในระดับค่อนข้างสูง ผู้ใช้คอมพิวเตอร์ทั่วไปควรที่จะตระหนักถึงภัยดังกล่าวโดยเฉพาะอย่างยิ่งปัญหาของบอทเน็ตอาจทวีความรุนแรงมากขึ้นในประเทศไทยเมื่อจำนวนผู้ใช้เครือข่ายอินเทอร์เน็ตออนไลน์ประเภท บรอดแบนด์อย่างระบบ ADSL มีมากขึ้นในช่วงปีที่ผ่านมา การ

ขยายตัวของบริการ บรอดแบนด์ทำให้เครื่องคอมพิวเตอร์ที่ออนไลน์อยู่ ตลอดเวลาบนอินเทอร์เน็ตมีจำนวนมากยิ่งขึ้น หากผู้ใช้ทั่วไปขาดความเข้าใจถึงการป้องกันความปลอดภัยแก่เครื่องคอมพิวเตอร์ของตนเอง โดยที่ไม่เพิ่มความระมัดระวังด้วยการอุดช่องโหว่ของระบบปฏิบัติการ ติดตั้งไฟร์วอลล์และระบบความปลอดภัยของข้อมูลอื่น ๆ ก็อาจจะทำให้ตกเป็นเครื่องมือของแฮ็กเกอร์ผู้สร้างบอตเน็ตได้โดยง่าย ในบทความนี้เราจะอธิบายถึงหลักการทำงานของบอตเน็ต ผลกระทบของภัยคุกคามดังกล่าว รวมไปถึงแนวทางป้องกันและแก้ไขให้ทราบ

4.1.1.1 การทำงานของบอตเน็ต

ลักษณะที่สำคัญของบอตเน็ตก็คือจะมีศูนย์กลางควบคุมและสั่งการโดยแฮ็กเกอร์อยู่ที่ใดที่หนึ่งบนอินเทอร์เน็ต กลไกการทำงานของบอตเน็ตถูกออกแบบให้มีการแพร่กระจายตัวเพื่อหาเครื่องใหม่ให้เข้ามาอยู่ในกลุ่ม และมีความสามารถในการแก้ไขโปรแกรมของบอตที่ฝังตัวอยู่บนเครื่องคอมพิวเตอร์ผีดิบเพื่อเปลี่ยนแปลง รูปแบบการบุกรุก ลักลอบใช้งานและสั่งการผ่านศูนย์ควบคุม ซึ่งองค์ประกอบหลักของบอตเน็ตได้แก่เครื่องคอมพิวเตอร์สั่งการ ระยะไกลของแฮ็กเกอร์

เครื่องเซิร์ฟเวอร์ของห้องสนทนา IRC ที่เป็นจุดนัดพบระหว่างกลุ่มของบอตและแฮ็กเกอร์เพื่อรอรับคำสั่ง กลุ่มของ DNS เซิร์ฟเวอร์ซึ่งเป็นทางผ่านเพื่อทำให้บอตสามารถหาเครื่องเซิร์ฟเวอร์ของห้องสนทนา IRC เจอได้ นอกจากนี้ยังมีกลุ่มของเครื่องคอมพิวเตอร์ต่าง ๆ บนเครือข่ายอินเทอร์เน็ตที่เป็นเป้าหมายของบอตเน็ตและกลุ่มที่ได้กลายเป็นส่วนหนึ่งของบอตเน็ตไปแล้วกระบวนการทำงานของบอตเน็ตมีขั้นตอนดังรูปที่ 1 เริ่มจากแฮ็กเกอร์ที่เป็นเจ้าของบอตเน็ตจะสร้างบอตเน็ตด้วยการติดตั้งเซิร์ฟเวอร์ห้องสนทนา IRC เตรียมไว้ ณ ที่ใดที่หนึ่งบนเครือข่ายอินเทอร์เน็ต โดยอาจเป็นเซิร์ฟเวอร์ที่ถูกต้องตามกฎหมายหรือเป็นเครื่องที่ถูกบุกรุกเพื่อนำมาใช้เป็นเซิร์ฟเวอร์ห้องสนทนา IRC ก็ตามหลังจากนั้นแฮ็กเกอร์ก็จะทำการลงทะเบียนชื่อโดเมนและหมายเลข IP ของเซิร์ฟเวอร์ห้องสนทนา IRC ไว้กับบริการ DNS บนอินเทอร์เน็ต

เพื่อให้บอตสามารถค้นหาเซิร์ฟเวอร์ของห้องสนทนาอื่นๆที่แฮ็กเกอร์ผู้นั้นได้ติดตั้งบอตไว้ก่อนแล้วเมื่อโครงสร้างหลักข้างต้นพร้อมแล้ว แฮ็กเกอร์ก็จะเริ่มทำการโจมตีเครื่องคอมพิวเตอร์เครื่องอื่น ๆ บนอินเตอร์เน็ตเพื่อค้นหาเหยื่อสำหรับติดตั้งบอตและทำให้เครื่องคอมพิวเตอร์เหล่านั้นกลายเป็นเครื่องคอมพิวเตอร์ผีดิบ โปรแกรมโจมตีของบอตส่วนใหญ่ที่นิยมมักจะอยู่ในรูปแบบของหนอนอินเทอร์เน็ตหรือโปรแกรมโจมตีคอมพิวเตอร์ที่ฝังตัวอยู่ในโปรแกรมประยุกต์ต่าง ๆ เช่นการโจมตีโดยอาศัยข้อมูลทางเว็บไซต์ที่แฮ็กเกอร์อาจจะทำการฝังโปรแกรมประสงค์ร้ายต่าง ๆ ไว้บนเว็บเซิร์ฟเวอร์ก่อนอยู่แล้ว หรือการซ่อนโปรแกรมประสงค์ร้ายผ่านทางการแชร์ไฟล์ในแบบ peer-to-peer เพื่อที่จะลักลอบเข้าไปติดตั้งโปรแกรมโทรจันสำหรับบอตเน็ตในเครื่องคอมพิวเตอร์ของเหยื่อผู้เคราะห์ร้าย เป็นต้น

เมื่อบอตสามารถทำงานบนเครื่องคอมพิวเตอร์ผีดิบได้แล้ว บอตก็จะทำการติดต่อกับ DNS เซิร์ฟเวอร์โดยอัตโนมัติเพื่อค้นหาเซิร์ฟเวอร์ห้องสนทนา IRC ที่แฮ็กเกอร์ติดตั้งรอไว้ เมื่อพบเซิร์ฟเวอร์แล้วบอตก็จะทำการล็อกอินเข้าไปเพื่อรอรับคำสั่งจากแฮ็กเกอร์ เมื่อถึงเวลาที่ต้องการและมีจำนวนบอตมากเพียงพอแฮ็กเกอร์ก็จะล็อกอินผ่านเครื่องควบคุมบอตเน็ตหลัก (zombie master machine) เข้าสู่ระบบ IRC เซิร์ฟเวอร์นั้นเพื่อทำการออกคำสั่งต่างๆ เช่นให้ทำการโจมตีแบบ DDoS (Distributed Denial of Service) ไปยังเครื่องคอมพิวเตอร์เป้าหมายต่างๆ บนระบบเครือข่ายอินเทอร์เน็ต หรือทำการส่งสแปมแมล์สร้างความรำคาญให้กับผู้ใช้อินเทอร์เน็ตทั่วไปได้

นอกจากนี้แฮ็กเกอร์ยังสามารถที่จะสั่งการให้เกิดการแพร่กระจายและจู่โจมด้วยไวรัสคอมพิวเตอร์โดยอาศัยเครื่องคอมพิวเตอร์ผีดิบได้อีกด้วย ซึ่งจะส่งผลให้มีการติดตั้งบอตเพิ่มขึ้นบนเครื่องคอมพิวเตอร์อื่น ๆ อีกนับพันเครื่องในระบบเครือข่ายอินเทอร์เน็ตต่อไป นอกจากนี้เทคนิคที่เครื่องคอมพิวเตอร์ผีดิบนิยมใช้โจมตีเครื่อง

คอมพิวเตอร์อื่นๆ ก็คือการโจมตีโดยอาศัยโปรโตคอลปกติทั่วไป เช่นโปรโตคอลของเว็บ เป็นต้น ประกอบกับเทคนิคการปลอมแปลงหมายเลข IP ของผู้ส่งหรือที่เรียกว่าเทคนิค IP Spoofing ส่งผลให้การค้นหาต้นกำเนิดของบอตเน็ตที่แท้จริงนั้นทำได้ยากมากยิ่งขึ้น

ดังนั้นจึงไม่น่าแปลกใจเลยว่าในปัจจุบันจำนวนเครื่องคอมพิวเตอร์ผีดิบที่ถูกควบคุมโดยเครื่องควบคุมบอตเน็ตหลักนั้นมีจำนวนมากและมีแนวโน้มว่าจะเพิ่มสูงขึ้นเรื่อย ๆ อีกด้วยนอกจากนี้การโจมตีของเครื่องคอมพิวเตอร์ผีดิบมีความซับซ้อนมากยิ่งขึ้น มีการโจมตีแบบผสมผสานกล่าวคือในการโจมตีครั้งหนึ่งอาจจะใช้ทั้งไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต และม้าโทรจัน ประกอบกันตัวอย่างวิธีการโจมตีที่พบเห็นล่าสุดมีการแบ่งเป็นขั้นตอนดังนี้ เริ่มด้วยการใช้ไวรัสคอมพิวเตอร์โจมตีพร้อมทั้งติดตั้งม้าโทรจันซึ่งจะทำการเปิดประตูลับ (Backdoor) บนเครื่องคอมพิวเตอร์ของเหยื่อ

หลังจากนั้นก็ทำการปลดการควบคุมการใช้งานของเครื่องเหล่านั้นพร้อมทั้งหยุดการทำงานของโปรแกรมป้องกันไวรัสต่าง ๆ และตามด้วยการโจมตีที่รุนแรงยิ่งขึ้นต่อไป เนื่องจากบอตนั้นถูกสั่งการจากศูนย์ควบคุมบอตหลักที่ถูกติดตั้งบนเซิร์ฟเวอร์ของห้องสนทนา IRC จึงไม่ใช่เรื่องยากที่แฮกเกอร์จะสามารถเปลี่ยนแปลงการทำงานของบอต รวมทั้งสามารถอัพเดตตัวเองได้ ล่าสุดเมื่อไม่นานมานี้บอตเน็ตเริ่มมีการประยุกต์ใช้เทคนิคที่สามารถแก้ไขข้อมูลในระดับเคอร์เนล(Kernel) และในระดับแอพพลิเคชัน (Application) ของระบบปฏิบัติการที่เรียกว่าเทคนิค Root Kits เพื่อทำการซ่อนการทำงานของโปรแกรมของบอตเน็ต บอตเน็ตประเภทนี้ได้แก่บอตเน็ตสายพันธุ์ “Rbot” เป็นต้น ดังนั้นจะเห็นว่าบอตเน็ตชนิดใหม่ที่ถูกพัฒนาและถูกปล่อยออกมาอาละวาดในโลกอินเทอร์เน็ตในปัจจุบันนั้นมีความสามารถและรูปแบบที่มีความรุนแรงสูงขึ้นจนทำให้การป้องกันก็ทำได้ยากยิ่งขึ้นด้วย

4.1.1.2 วิธีการป้องกันและแก้ไข

- ห้ามรันไฟล์ที่แนบมากับอี-เมล์ซึ่งมาจากบุคคลที่ไม่รู้จักหรือไม่มั่นใจว่าผู้ส่งเป็น ใครและไม่ทราบว่าไฟล์ ดังกล่าวนั้นเป็นไฟล์อะไร ตลอดจนไฟล์ที่ถูกส่งด้วย โปรแกรมสนทนา (Chat) ต่างๆ เช่น IRC, ICQ หรือ Pirch เป็นต้น

- ติดตั้งโปรแกรมซ่อมแซมช่องโหว่ (patch) ของทุกซอฟต์แวร์อยู่เสมอ โดยเฉพาะโปรแกรม Internet Explorer และระบบปฏิบัติการ ให้เป็นเวอร์ชันใหม่ที่สุด

- ติดตั้งโปรแกรมป้องกันไวรัส และต้องทำการปรับปรุงฐานข้อมูลไวรัสให้ทันสมัย อยู่เสมอ

- ติดตั้งโปรแกรมกำจัดสปายแวร์ ปรับปรุงฐานข้อมูล และสแกนหาสปายแวร์อยู่ เสมอ

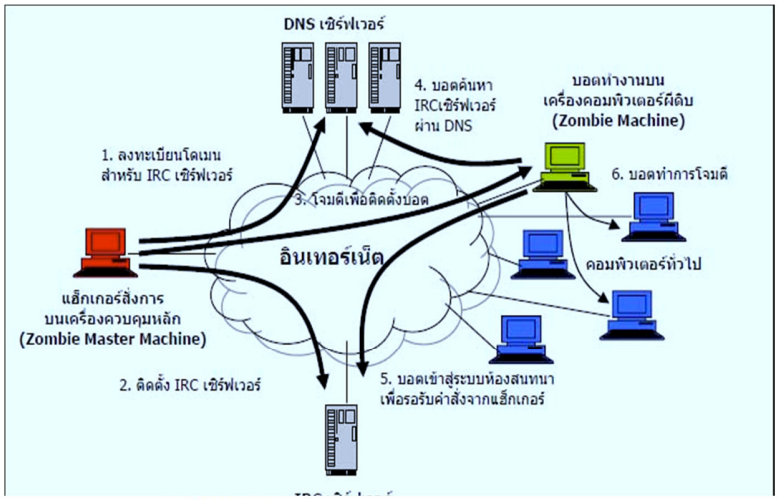
- ตั้งค่า security zone ของ Internet Explorer ให้เป็น high

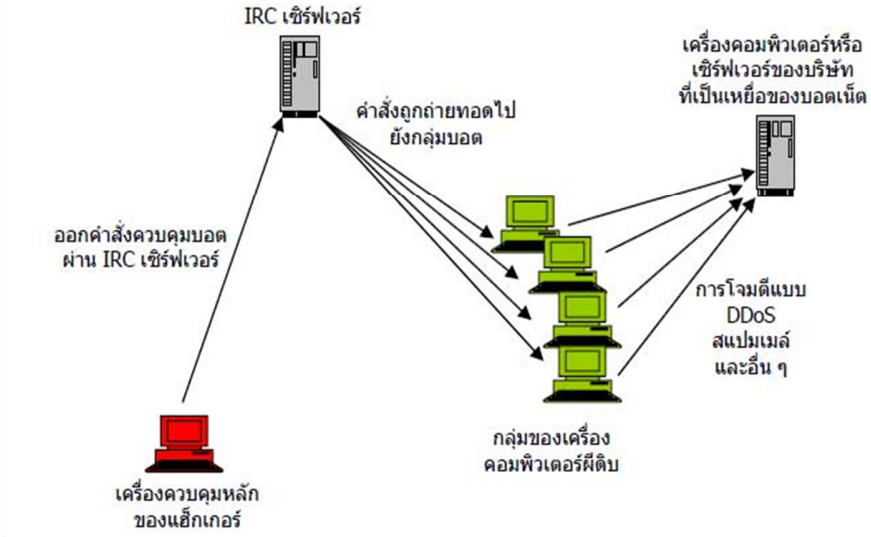
- ติดตั้งและใช้งานโปรแกรมกรองสแปมเมล์ ทั้งในเครื่องไคลเอ็นต์และที่เมล์ เซิร์ฟเวอร์

- หากพบว่ามีการติดตั้งเซิร์ฟเวอร์ที่ให้บริการ IRC โดยมีจำนวนเครื่องที่เข้าสู่ระบบดังกล่าวสูงแต่ไม่มีการส่ง ข้อมูลคุยตามปกติระหว่างกัน เซิร์ฟเวอรดังกล่าวก็อาจกลายเป็นช่องทางในการควบคุมบอตเน็ตได้ ต้องดำเนินการหยุดการทำงานของเซิร์ฟเวอร์ดังกล่าวทันที

- หากพบสิ่งผิดปกติในเครื่องคอมพิวเตอร์หรือระบบเครือข่าย และสงสัยว่าอาจจะเป็นบอตเน็ตต้องรีบแจ้งให้เจ้าหน้าที่ที่เกี่ยวข้องรับทราบทันที เพื่อดำเนินการแก้ไขโดยเร่งด่วน ซึ่งจุดอ่อนของบอตเน็ตก็คือ

หาก มีการปิดกั้น DNS เซิร์ฟเวอร์ และ IRC เซิร์ฟเวอร์ไม่ให้เป็นทางผ่านเพื่อส่งต่อการควบคุมจากหัวหน้า ก็จะสามารถหยุดการทำงานของบอตได้แล้วส่วนหนึ่ง





ภาพที่ 1 และภาพที่2 แสดงขั้นตอนการทำงานของบอตเน็ต

5. วิธีการดำเนินการ

5.1 เสนอหัวข้อโครงงาน

5.1.1 ศึกษาหัวข้อโครงงานที่สนใจ

5.1.3 กำหนดหัวข้อโครงงาน

5.1.4 เสนอหัวข้อโครงงานกับอาจารย์ที่ปรึกษา

5.2 ศึกษาบทความและค้นคว้าข้อมูล

5.2.1 ศึกษาค้นคว้าโปรแกรม Blue Botnet

5.2.2 ศึกษาวิธีการแก้ปัญหา Botnet

5.3 นำเสนอเค้าโครง

5.3.1 นำเสนอเค้าโครงกับอาจารย์ที่ปรึกษาประจำรายวิชา

5.4. ศึกษาเทคนิคและเครื่องมือที่ใช้

5.4.1 ศึกษาวิธีใช้โปรแกรม Blue Botnet

5.5 วิเคราะห์และออกแบบ

5.5.1ไฟล์ไวรัสสามารถปิด fire wall อัตโนมัติ

5.5.2 ไฟล์ไวรัสสามารถตัดการใช้งานอินเทอร์เน็ต

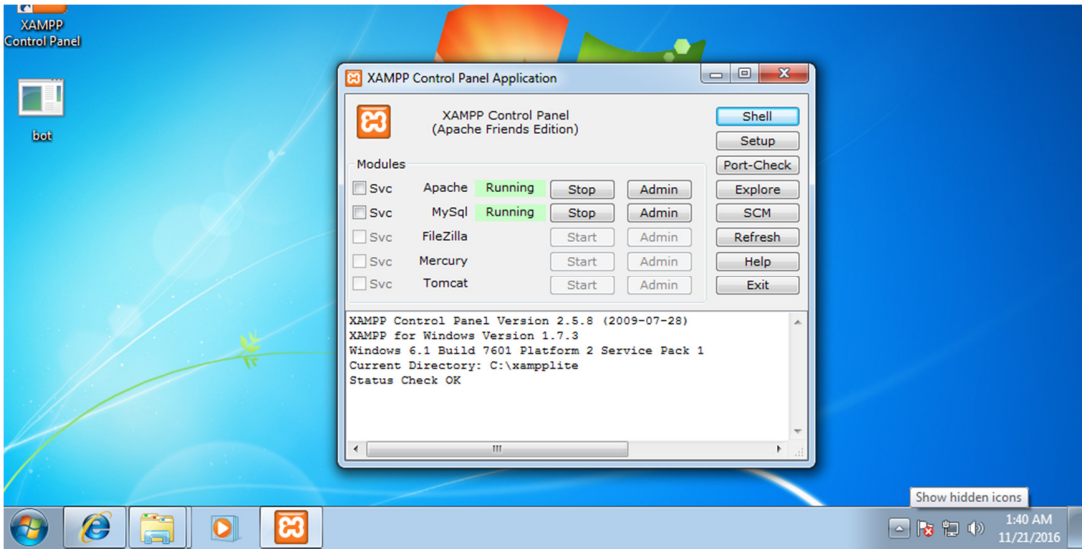
5.6 ทดสอบระบบ

5.7.1นำไฟล์ไวรัสที่สร้างขึ้นไปใส่ไว้ในเครื่องเป้าหมายแล้วดูผลลัพธ์

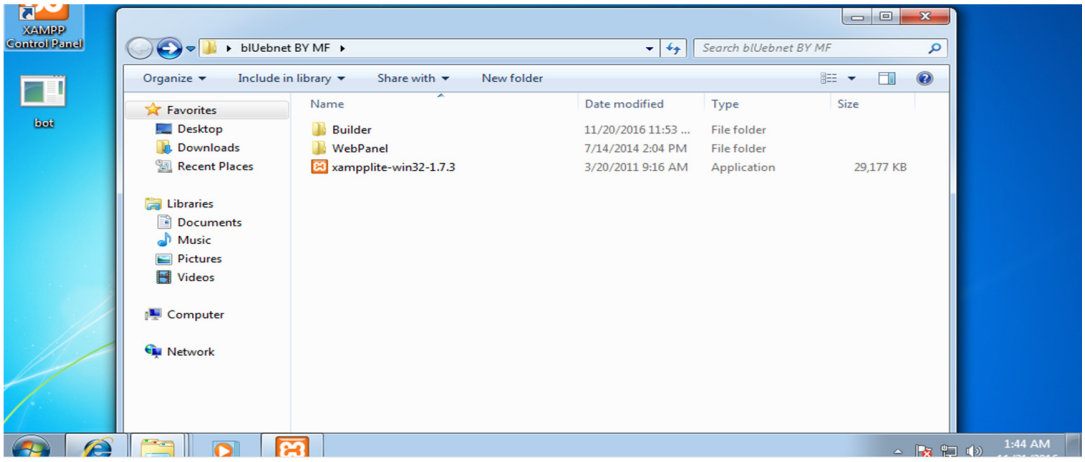
5.7. นำเสนอโครงงาน

คู่มือการใช้งาน โปรแกรม Blue Botnet

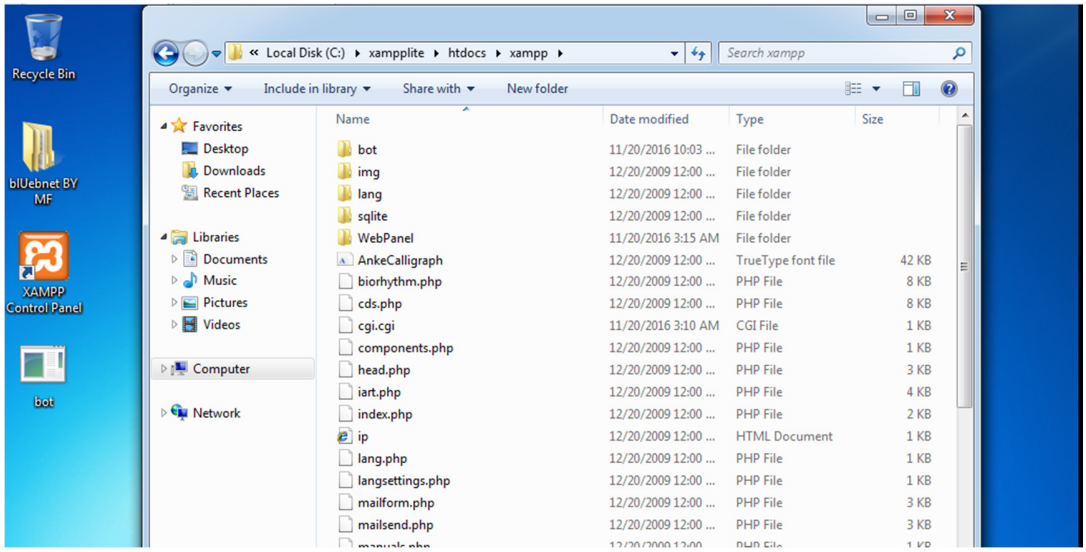
ฝั่งเครื่องที่โจมตี



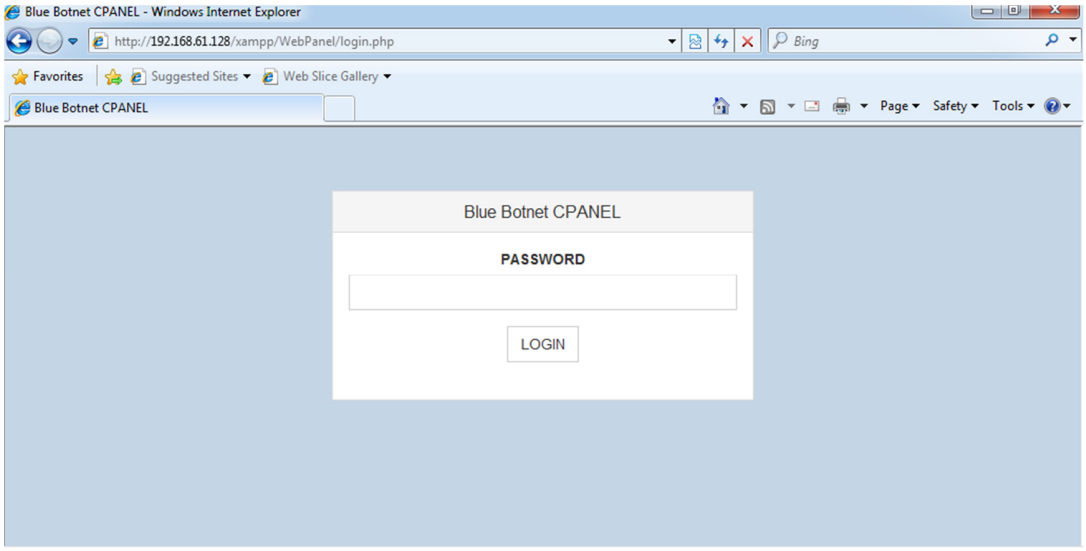
ขั้นตอนที่ 1 ติดตั้งตัวจำลอง web server และกด start Apache เช่น XAMPP



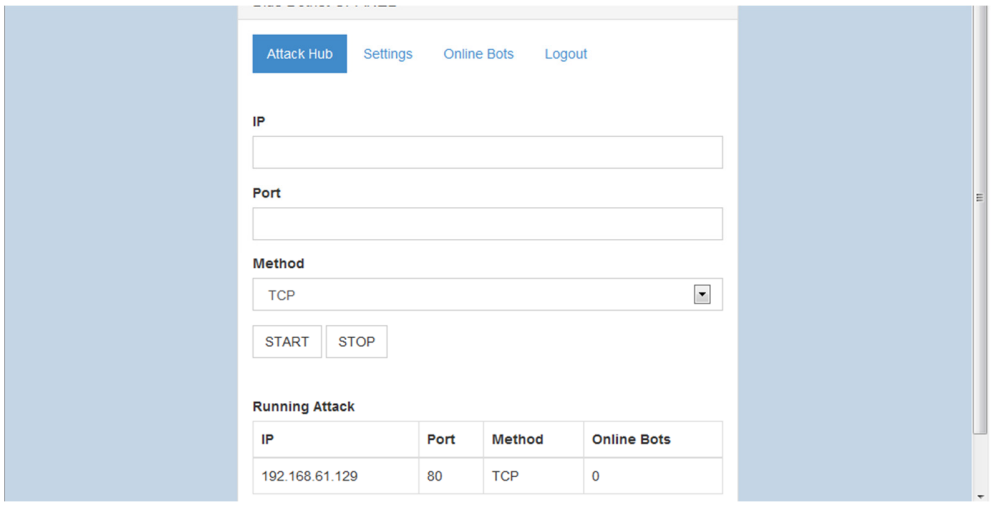
ขั้นตอนที่ 2 Copy Folder WebPanel



ขั้นตอนที่ 3 วาง folder ที่ได้ copyมาไว้ ที่เก็บไฟล์ของตัวจำลอง web server ในที่นี้คือ C:\xampplite\htdocs\xampp\Webpanel



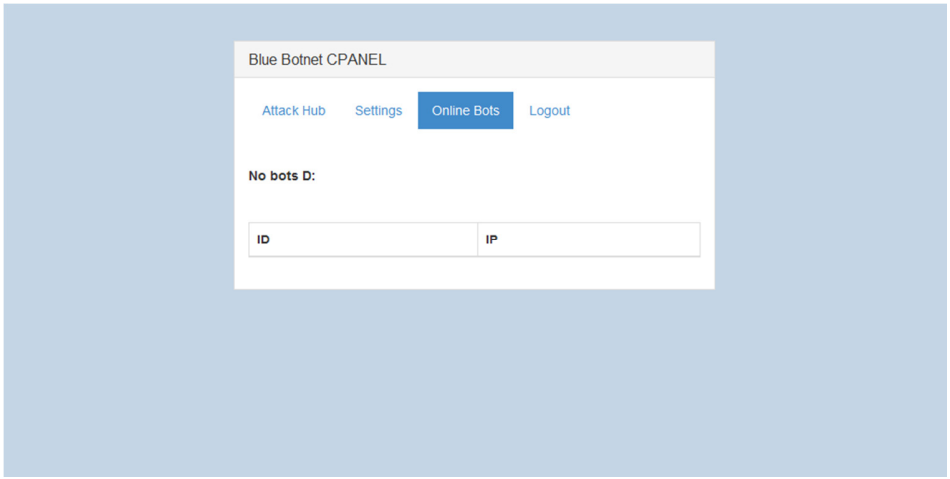
ขั้นตอนที่ 4 ทำการเข้า browser เพื่อเปิดหน้าเว็ปตามตัวจำลอง web server ที่ได้ลงไว้ซึ่งจะแสดงหน้าเว็ปขึ้น จากนั้นทำการใส่รหัสผ่านของ Blue botnet



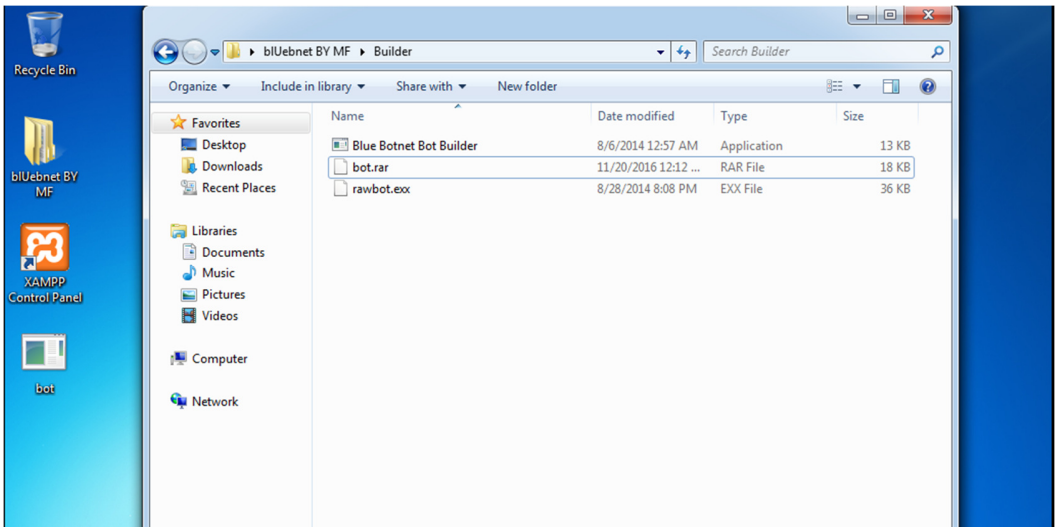
ขั้นตอนที่ 5 เมื่อ login มาแล้วจะแสดงหน้าเมนูของเว็ปดังนี้

Attack Hub เมื่อคลิกจะแสดงหน้าต่างสำหรับใส่ข้อมูลของเครื่องที่จะโจมตี

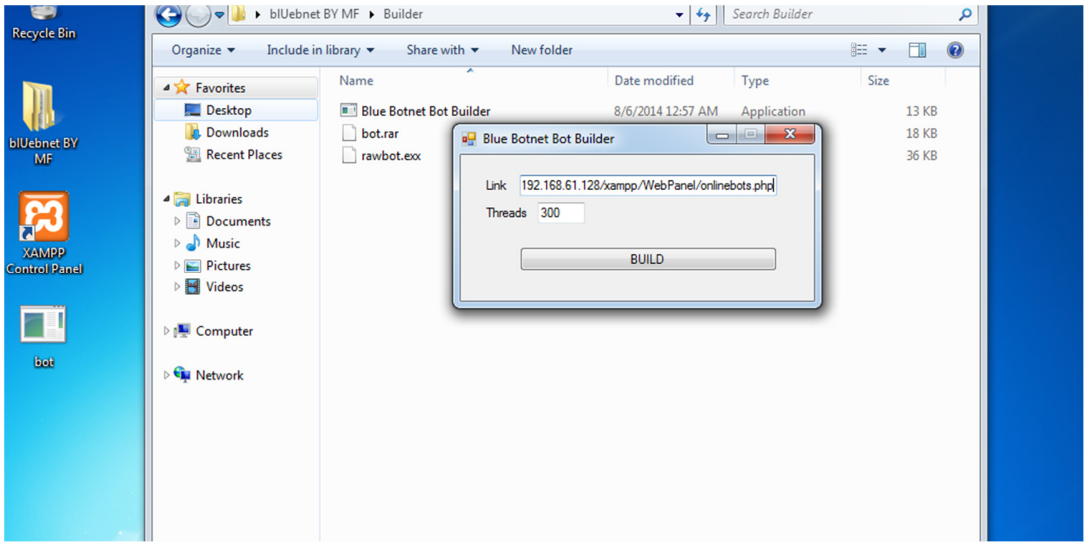
- Ip ใส่เลข ip ของเครื่องที่ติด bot
- Port ใส่ port ของเครื่อง
- Method เลือกMethod ที่จะโจมตีเช่น TCP
- Start/Stop เริ่มและหยุดในการโจมตี botnet
- Running Attack แสดงเครื่องที่กำลังถูกโจมตีในขณะนั้น



แสดงเลข ip ของเครื่องที่ได้ติด bot ทั้งหมด

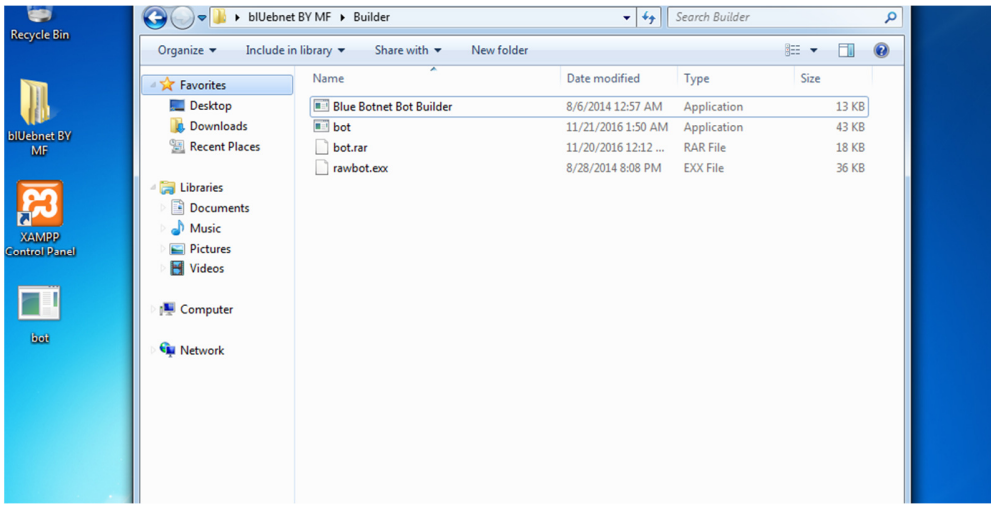


ขั้นตอนที่ 6 เข้า Folder blUebnet BY MF\Builder และเปิดไฟล์ Blue Botnet Bot Builder เพื่อทำการสร้างbot

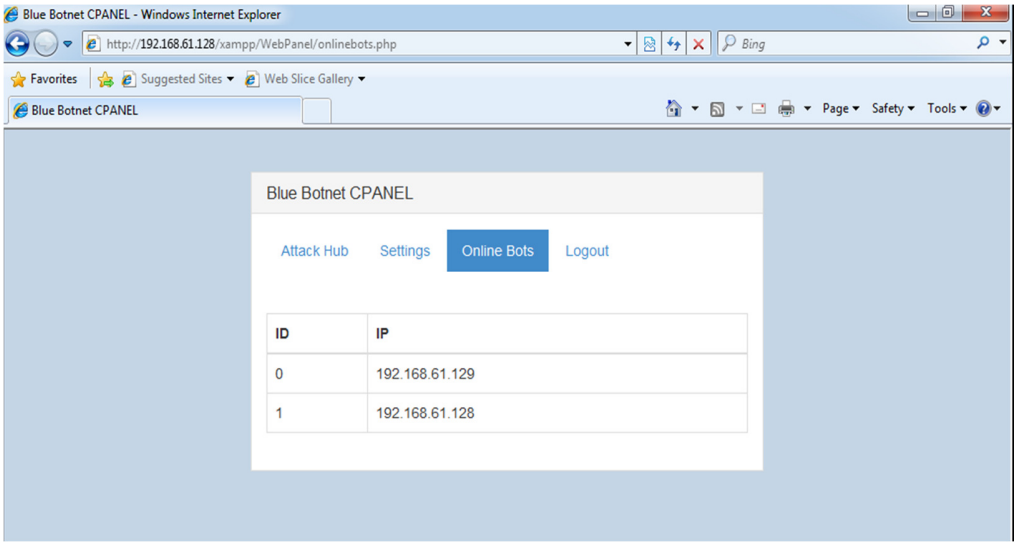


ขั้นตอนที่ 7 coppy Url ของหน้าเว็ป blue bot net นำมาใส่ในช่อง Link ในที่นี้คือ

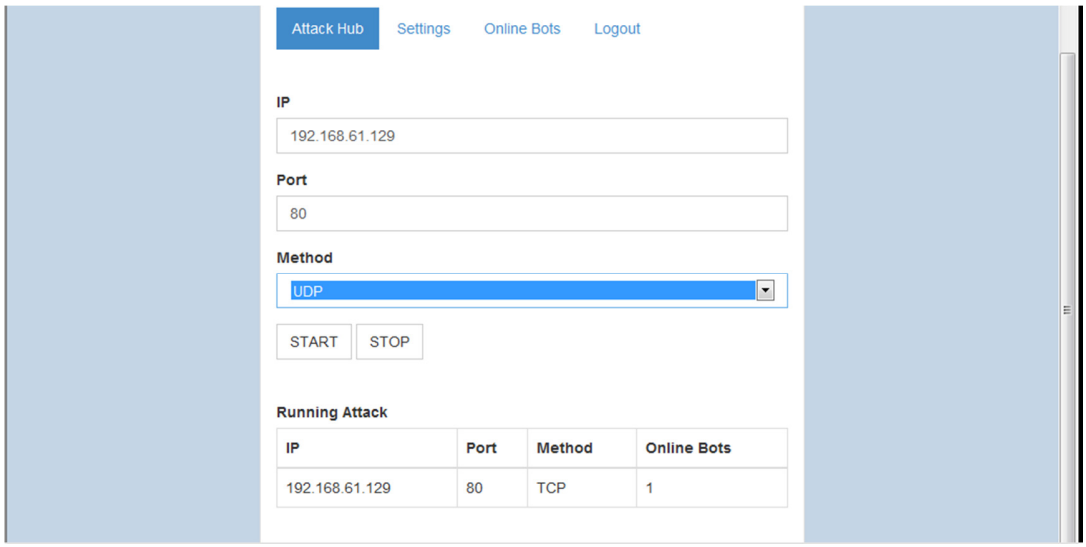
https://192.160.16.128/xampp/WebPanel/



ขั้นตอนที่ 8 จะได้ไฟล์ bot และในไปไว้ในเครื่องเป้าหมายที่ต้องการ เพื่อกดรันไฟล์

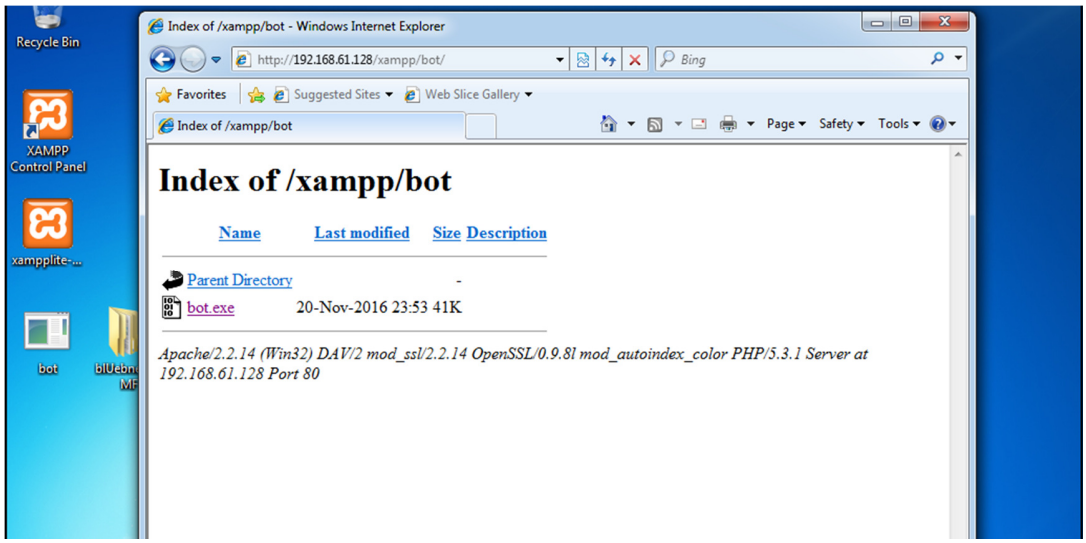


ขั้นตอนที่ 9 เมื่อมีเครื่องที่กดไฟล์ bot ที่ปล่อยไว้ หน้าเว็ปจะแสดง ip เครื่องที่ติดทันทีและแสดงจำนวนเครื่องทั้งหมดที่ติด

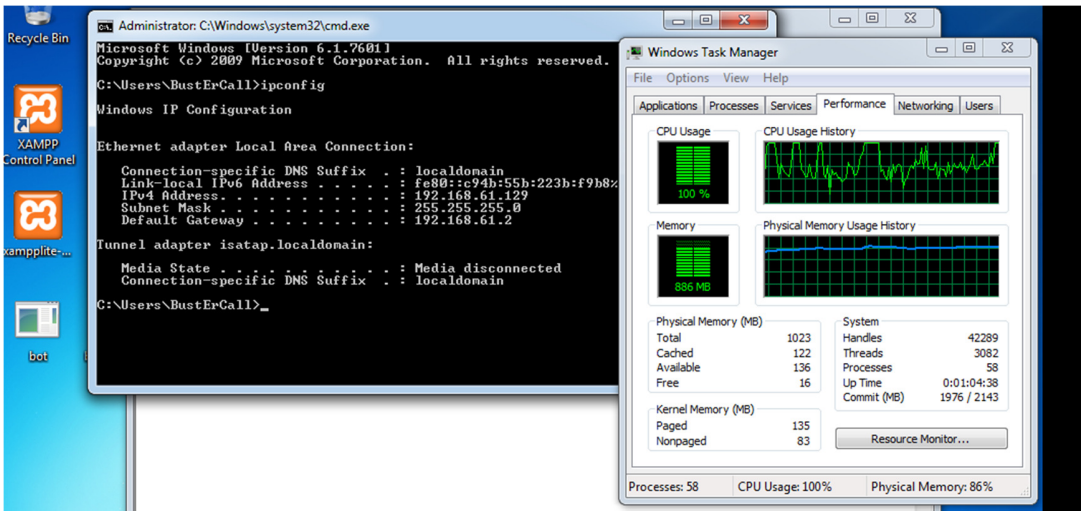


ขั้นตอนที่ 10 ทำการใส่เลข ip/port เลือก Method และกด StartหรือStop เพื่อทำการโจมตีหรือหยุด เครื่องที่ติด bot ตามต้องการ

ฝั่งเครื่องที่ถูกโจมตี



ภาพที่ 1 เมื่อเครื่องกดรันไฟล์ bot.exe จะติดbotnet ทันที

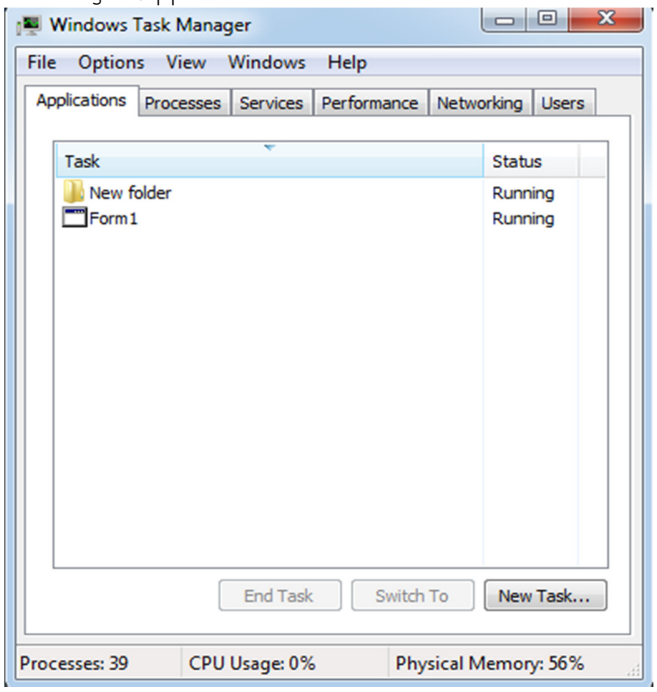


ภาพที่ 2 จะแสดงเครื่องที่ทำการติด bot ซึ่งจะเห็นได้ว่ามีการประมวลผลของ CPU เป็นอย่างมาก เนื่องจากถูกโจม

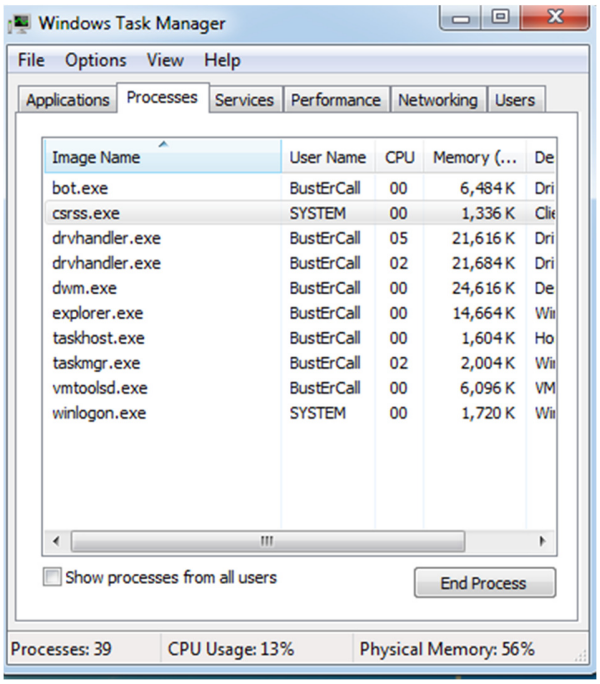
วิธีการกำจัดไฟล์ bot

- ทำการติดตั้งแอดตี้ไวรัสหรือเปิดไฟล์วอลล์

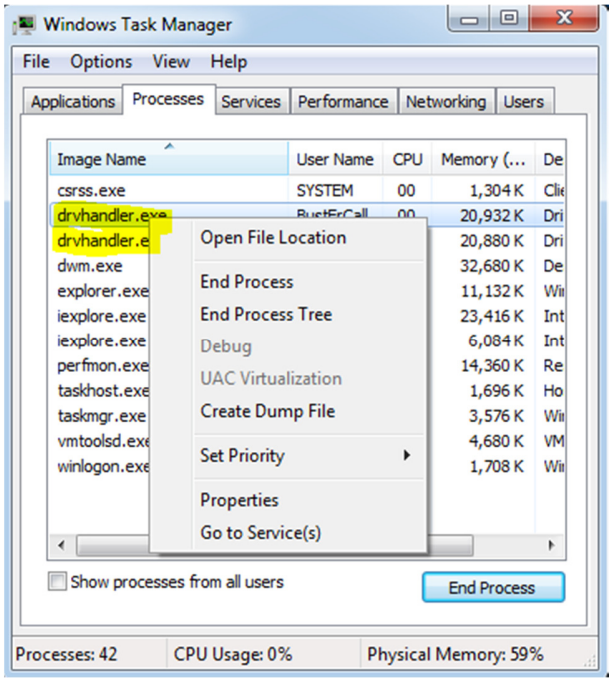
- เปิด Start task Manager \Appilicationd และเลือก Form1 กด Endtask



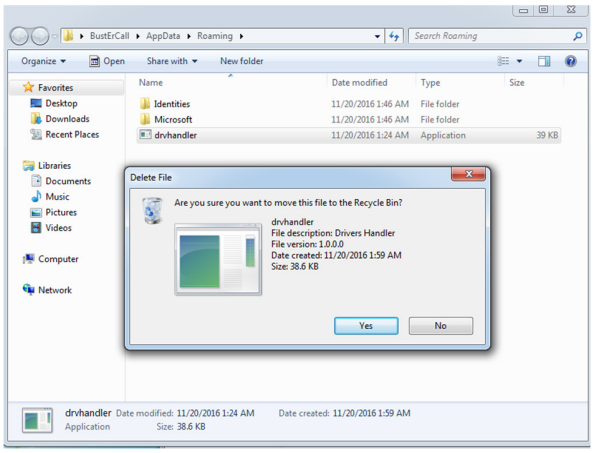
- เปิด Processes เลือก [bot.exe] กด End Process



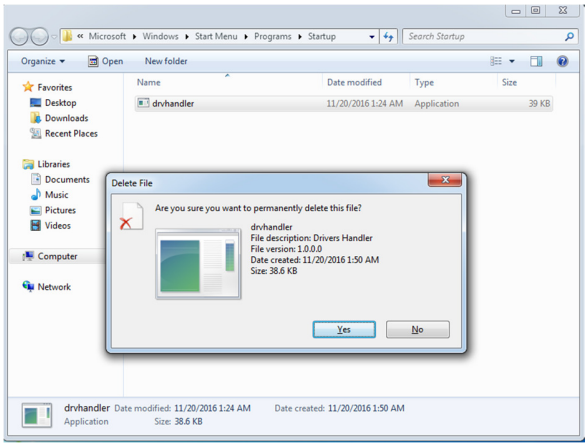
- ทำการคลิกขวาไฟล์ drvhandler.exe ทั้งสองไฟล์ แล้วกด Open File Location เพื่อทำการหาที่อยู่ไฟล์และกด End Process จากนั้นทำการลบทั้งสองไฟล์



- ทำการลบไฟล์ drvhandler.exe (1)



-ทำการลบไฟล์ drvhandler.exe (2)



6. แผนและระยะดำเนินงาน

ขั้นตอนการดำเนินงาน	พ.ศ.2559		
	กันยายน	ตุลาคม	พฤศจิกายน

1.เสนอหัวข้อโครงงาน												
2.ศึกษาบทความและค้นคว้าข้อมูล												
3.นำเสนอเค้าโครง												
4.ศึกษาเทคนิคและเครื่องมือที่ใช้												
5.วิเคราะห์และออกแบบ												
6.พัฒนาระบบ												
7.ทดสอบระบบ												
8.สรุปผล												
9.นำเสนอโครงงาน												

7. เอกสารอ้างอิง

1. บอตเน็ต BOTNET. (ม.ป.ป.). ค้นเมื่อ 20 พฤศจิกายน 2559, จาก http://www.it-know-ledge.com/Security-Network/