Razor Batch Virus Builder

โดย

1. นางสาวชัญญา	งามศิริอุดม	รหัสนักศึกษา 573021136-1
2. นางสาวศศิพิมพ์	ประสาทศรี	รหัสนักศึกษา 573021166-2
3. นางสาวทิวาพร	ดอนศิลา	รหัสนักศึกษา 573020418-6
4. นางสาววิลาณี	อำนาจเจริญ	รหัสนักศึกษา 573020435-6
5. นางสาวจิราพร	อเนกเวียง	รหัสนักศึกษา 573020409-7
6. นางสาวอริสา	ชาสี	รหัสนักศึกษา 573020448-7

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 ซึ่งเทคโนโลยีที่สามารถเข้าถึงผู้คนได้อย่างแพร่หลายคือด้านคอมพิวเตอร์ แต่ปัญหาที่มาพร้อมกับเทคโนโลยีด้านคอมพิวเตอร์คือ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การปลอมแปลงบุคคล หรือแม้กระทั่งไวรัส ซึ่งรายงานนี้ได้จัดทำขึ้นเพื่อศึกษาโปรแกรมสร้างไวรัสที่มีชื่อว่า Razor Batch Virus Builder เพื่อให้ผู้ใช้งานได้เรียนรู้วิธีการสร้างไฟล์ไวรัส ประโยชน์และโทษของไฟล์ไวรัส ทำให้สามารถนำไปประยุกต์ใช้ได้อย่างเหมาะสม

คณะผู้จัดทำ

สารบัญ

1. หลักการและเหตุผล

ปัจจุบันการประยุกต์ใช้เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตได้เกิดขึ้นอย่างรวดเร็ว จึงเป็นเหตุจูงใจที่ก่อให้เกิดภัยคุกคามและการโจมตีโครงสร้างพื้นฐานเครือข่ายของคอมพิวเตอร์และอินเทอร์เน็ตรวมถึงการล้วงลับข้อมูลที่สำคัญ และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากซอฟแวร์หรือการละเมิดลิขสิทธิ์โดยผิดกฎหมายซึ่งได้สร้างความเสียหายทางด้านข้อมูลและทรัพย์สินเป็นอย่างมาก

อีกหนึ่งสิ่งที่สำคัญเกี่ยวกับความปลอดภัยของคอมพิวเตอร์คือเรื่องของไวรัสคอมพิวเตอร์ ซึ่งเป็นเรื่องที่เราได้ยินได้ฟังอยู่เป็นประจำทุกวัน ทุกเวลาคือไวรัสติดเครื่องคอมพิวเตอร์ เรามักจะหาโปรแกรมกำจัดไวรัสมาทำการกำจัดไวรัสเหล่านั้น หลังจากที่ไวรัสตัวนั้นถูกกำจัดแล้ว จากนั้นอีกไม่นานก็จะมีไวรัสตัวใหม่ๆออกมาอีกไม่จบไม่สิ้น ซึ่งเป็นเหตุที่ทำให้ข้อมูลที่เป็นความลับหรือข้อมูลถูกขโมยและสร้างความรำคาญใจแก่ทุกๆคนเป็นอย่างมาก

จากข้อมูลข้างต้น ทำให้ทราบว่าการจัดการความปลอดภัยนั้นไม่ใช่เรื่องง่ายเนื่องจากจะต้องป้องกันและต้องคอยตรวจสอบติดตามอย่างสม่ำเสมอ ดังนั้นจึงต้องศึกษา เพราะอาชญากรรมทางคอมพิวเตอร์เป็นสิ่งที่เกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ หากเกิดความผิดพลาดเกิดขึ้น จะได้มีมาตรการรองรับได้อย่างท่วงทีผู้จัดทำจึงได้ศึกษาข้อมูลการทำงานของไวรัสว่ามีวิธีหรือกระบวนการทำงานอย่างไร และสามารถสร้างความเสียหายได้ร้ายแรงขนาดไหน เพื่อเป็นแนวทางในการป้องกันและรักษาความปลอดภัยของคอมพิวเตอร์และข้อมูลที่สำคัญได้อย่างปลอดภัยและทันท่วงที

2. วัตถุประสงค์

2.1 เพื่อศึกษากลไลการทำงานของไวรัส

2.2 เพื่อทดสอบความสามารถของเครื่องคอมพิวเตอร์

3. ประโยชน์ที่คาดว่าจะได้รับ

3.1 ได้รู้ถึงกระบวนการทำงานของไวรัส

3.2 ได้รู้ถึงความสามารถของเครื่องคอมพิวเตอร์

3.3 ได้เรียนรู้ถึงภาษาคอมพิวเตอร์ เพื่อนำไปเป็นความรู้ในการต่อยอดได้

4. ทฤษฎีที่เกี่ยวข้อง

4.1 ไวรัส (Virus)

4.1.1 ไวรัสคืออะไร

ไวรัส คือ โปรแกรมคอมพิวเตอร์โปรแกรมหนึ่งที่มีผู้เขียนขึ้นมา โดยมีเป้าหมายที่ชัดเจน คือ สร้างความเสียหายให้กับคอมพิวเตอร์ มีลักษณะคล้ายเชื้อโรคขนาดเล็ก ซึ่งถ้าไวรัสมันได้เข้าไปอยู่ในเครื่องคอมพิวเตอร์แล้ว มันจะทำงานด้วยตัวของมันเอง และจะก่อให้เกิดปัญหาตามมามากมาย เช่น ขัดขวางการอ่านข้อมูล ขัดขวางการเข้าถึงข้อมูลในหน่วยความจำ ขัดขวางการทำงานของอุปกรณ์ต่อพ่วงต่างๆ และที่สร้างความเสียหายอย่างมากที่สุด คือ การเข้าไปทำลายแฟ้มข้อมูลหรือเข้าไปทำลายระบบต่างๆ ของเครื่องคอมพิวเตอร์ จนบางครั้งไม่สามารถใช้งานได้อีกต่อไป การทำงานของไวรัสแต่ละตัวจะขึ้นอยู่กับวัตถุประสงค์ของผู้เขียนโปรแกรมนั้นขึ้นมา เช่น ทำลายระบบปฏิบัติการ โปรแกรมใช้งานหรือข้อมูลอื่น ๆ ที่อยู่ในคอมพิวเตอร์ หรือรบกวนการทำงาน

เช่น การบู๊ตระบบช้าลง เรียกใช้โปรแกรมได้ไม่สมบูรณ์ หรือเกิดอาการค้าง เกิดข้อความวิ่งไปมาที่หน้าจอ หรือกรอบข้อความเตือนไม่ทราบสาเหตุ เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้น โดยมีการรายงานว่ามีจำนวนเซกเตอร์ที่เสียเพิ่มขึ้นทั้ง ๆ ที่ยังไม่ได้ใช้โปรแกรมใด ๆ เข้าไปตรวจหาเลย ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ ๆ ก็หายไป

4.1.2 ประเภทของไวรัส

บูตเซกเตอร์ไวรัส Boot Sector Viruses หรือ Boot Infector Viruses คือไวรัสที่เก็บตัวเองอยู่ในบูตเซกเตอร์ ของดิสก์ การใช้งานของบูตเซกเตอร์คือ เมื่อเครื่องคอมพิวเตอร์เริ่มทำงานขึ้นมาตอนแรก เครื่อง จะเข้าไปอ่านบูตเซกเตอร์ โดยในบูตเซกเตอร์จะมีโปรแกรมเล็ก ๆ ไว้ใช้ในการเรียกระบบ ปฏิบัติการขึ้นมาทำงานอีกทีหนึ่ง บูตเซกเตอร์ไวรัสจะเข้าไปแทนที่โปรแกรมดังกล่าว และไวรัส ประเภทนี้ถ้าไปติดอยู่ในฮาร์ดดิสก์ โดยทั่วไป จะเข้าไปอยู่บริเวณที่เรียกว่า Master Boot Sector หรือ Parition Table ของฮาร์ดดิสก์นั้นถ้าบูตเซกเตอร์ของดิสก์ใดมีไวรัสประเภทนี้ติดอยู่ ทุก ๆ ครั้งที่บูตเครื่องขึ้นมาโดย พยายามเรียก ดอสจากดิสก์นี้ ตัวโปรแกรมไวรัสจะทำงานก่อนและจะเข้าไปฝังตัวอยู่ใน หน่วยความจำเพื่อเตรียมพร้อมที่ จะทำงานตามที่ได้ถูกโปรแกรมมา แล้วตัวไวรัสจึงค่อยไป เรียกดอสให้ขึ้นมาทำงานต่อไป ทำให้เหมือนไม่มีอะไรเกิดขึ้น

โปรแกรมไวรัส Program Viruses หรือ File Intector Viruses เป็นไวรัสอีกประเภทหนึ่งที่จะติดอยู่กับโปรแกรม ซึ่งปกติก็คือ ไฟล์ที่มีนามสกุลเป็น COM หรือ EXE และบางไวรัสสามารถเข้า ไปติดอยู่ในโปรแกรมที่มีนามสกุลเป็น sys และโปรแกรมประเภท Overlay Programsได้ด้วย โปรแกรมโอเวอร์เลย์ปกติจะเป็นไฟล์ที่มีนามสกุลที่ขึ้นต้นด้วย OV วิธีการที่ไวรัสใช้เพื่อที่จะ เข้าไปติดโปรแกรมมีอยู่สองวิธี คือ การแทรกตัวเองเข้าไปอยู่ในโปรแกรมผลก็คือหลังจากที่โปรแกรมนั้นติดไวรัสไปแล้ว ขนาดของโปรแกรมจะใหญ่ขึ้น หรืออาจมีการสำเนาตัวเองเข้าไปทับส่วนของโปรแกรมที่มีอยู่เดิมดังนั้นขนาดของโปรแกรมจะไม่เปลี่ยนและยากที่ จะซ่อมให้กลับเป็นดังเดิม การทำงานของไวรัส โดยทั่วไป คือ เมื่อมีการเรียกโปรแกรมที่ติดไวรัส ส่วนของไวรัสจะทำงานก่อนและจะถือโอกาสนี้ฝังตัวเข้าไปอยู่ในหน่วยความจำทันทีแล้วจึงค่อยให้ โปรแกรมนั้นทำงานตามปกติต่อไป เมื่อไวรัสเข้าไปฝังตัวอยู่ในหน่วยความจำแล้ว หลัง จากนี้ไปถ้ามีการเรียกโปรแกรมอื่น ๆ ขึ้นมาทำงานต่อ ตัวไวรัสก็จะสำเนาตัวเองเข้าไปในโปรแกรมเหล่านี้ทันที เป็นการแพร่ระบาดต่อไป วิธีการแพร่ระบาดของโปรแกรมไวรัสอีกแบบหนึ่งคือ เมื่อมีการเรียกโปรแกรมที่มีไวรัสติดอยู่ตัวไวรัสจะเข้าไปหาโปรแกรมอื่นๆ ที่อยู่ในดิสก์เพื่อทำสำเนาตัวเองลงไปทันทีแล้วจึงค่อยให้โปรแกรมที่ถูกเรียก นั้นทำงานตามปกติต่อไป

ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็น โปรแกรมธรรมดาทั่วๆไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน แต่เมื่อถูกเรียกขึ้นมาแล้วก็จะเริ่มทำลายตามที่โปรแกรมมาทันที ม้าโทรจันบางตัวถูกเขียนขึ้นมาใหม่ทั้งชุด โดยคนเขียนจะทำการตั้งชื่อโปรแกรมพร้อมชื่อรุ่นและคำอธิบายการใช้งานที่ดูสมจริง เพื่อหลอกให้คนที่จะเรียกใช้ตายใจ จุดประสงค์ของคนเขียนม้าโทรจันอาจจะเช่นเดียวกับคนเขียนไวรัส คือ เข้าไปทำอันตรายต่อข้อมูลที่มีอยู่ในเครื่อง หรืออาจมีจุดประสงค์เพื่อที่จะล้วงเอาความลับของระบบคอมพิวเตอร์ ม้าโทรจันอาจจะถือว่าไม่ใช่ไวรัส เพราะเป็นโปรแกรมที่ถูกเขียนขึ้นมาโดด ๆ และจะไม่มีการเข้าไปติดในโปรแกรมอื่นเพื่อสำเนาตัวเอง แต่จะใช้ความรู้เท่าไม่ถึงการณ์ของ ผู้ใช้เป็นตัวแพร่ระบาด ซอฟต์แวร์ที่มีม้าโทรจันอยู่ในนั้นและนับว่าเป็นหนึ่งในประเภทของโปรแกรมที่มีความอันตรายสูง เพราะยากที่จะตรวจสอบและสร้างขึ้นมาได้ง่าย ซึ่งอาจใช้แค่แบตช์ไฟล์ก็สามารถโปรแกรมประเภทม้าโทรจันได้

โพลีมอร์ฟิกไวรัสPolymorphic Viruses เป็นชื่อที่ใช้ในการเรียกไวรัสที่มีความสามารถในการแปรเปลี่ยนตัวเอง ได้เมื่อมีสร้างสำเนาตัวเองเกิดขึ้น ซึ่งอาจได้ถึงหลายร้อยรูปแบบ ผลก็คือ ทำให้ไวรัสเหล่านี้ยากต่อการถูกตรวจจับ โดยโปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกนอย่างเดียว ไวรัสใหม่ๆ ในปัจจุบันที่มีความสามารถนี้เริ่มมีจำนวนเพิ่มมากขึ้นเรื่อย ๆ

สทีลต์ไวรัส Stealth Viruses เป็นชื่อเรียกไวรัสที่มีความสามารถในการพรางตัวต่อการตรวจจับได้ เช่น ไฟล์อินเฟกเตอร์ ไวรัสประเภทที่ไปติดโปรแกรมใดแล้วจะทำให้ขนาดของ โปรแกรมนั้นใหญ่ขึ้น ถ้าโปรแกรมไวรัสนั้นเป็นแบบสทีลต์ไวรัส จะไม่สามารถตรวจดูขนาดที่แท้จริง ของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัว ไวรัสจะเข้าไปควบคุมดอส เมื่อมีการใช้คำสั่ง DIR หรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ดอสก็จะแสดงขนาดเหมือนเดิม ทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น

4.1.3 อาการของเครื่องที่ติดไวรัส

- ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
- ขนาดของโปรแกรมใหญ่ขึ้น
- วันเวลาของโปรแกรมเปลี่ยนไป
- ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อย ๆ
- เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
- เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้อยู่
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ขนาดของหน่วยความจำที่เหลือลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ไฟล์แสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ๆ ก็หายไป
- เครื่องทำงานช้าลง
- เครื่องบูตตัวเองโดยไม่ได้สั่ง
- ระบบหยุดทำงานโดยไม่ทราบสาเหตุ
- เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นโดยมีการรายงานว่าจำนวนเซกเตอร์ที่เสียมีจำนวน เพิ่มขึ้นกว่าแต่ก่อนโดยที่ยังไม่ได้ใช้โปรแกรมใดเข้าไปตรวจหาเลย

4.1.4 การตรวจหาไวรัส

การสแกน โปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกน (Scanning) เรียกว่า สแกนเนอร์ (Scanner) โดยจะมีการดึงเอาโปรแกรมบางส่วนของตัวไวรัสมาเก็บไว้เป็นฐานข้อมูล ส่วนที่ดึงมานั้นเราเรียกว่าไวรัสซิกเนเจอร์ (VirusSignature)และเมื่อสแกนเนอร์ถูกเรียกขึ้นมาทำงานก็จะเข้าตรวจหาไวรัสในหน่วยความจำ บูตเซกเตอร์และไฟล์โดยใช้ ไวรัสซิกเนเจอร์ที่มีอยู่ ข้อดีของวิธีการนี้ก็คือ เราสามารถตรวจสอบซอฟแวร์ที่มาใหม่ได้ทันทีเลยว่าติดไวรัสหรือไม่ เพื่อป้องกันไม่ให้ไวรัสถูกเรียกขึ้นมาทำงานตั้งแต่เริ่มแรก แต่วิธีนี้มีจุดอ่อนอยู่หลายข้อ คือ

1. ฐานข้อมูลที่เก็บไวรัสซิกเนเจอร์จะต้องทันสมัยอยู่เสมอ แลครอบคลุมไวรัสทุกตัว มากที่สุดเท่าที่จะทำได้

2. สแกนเนอร์จะไม่สามารถตรวจจับไวรัสที่ยังไม่มี ซิกเนเจอร์ของไวรัสนั้นเก็บอยู่ในฐานข้อมูลได้

3. ยากที่จะตรวจจับไวรัสประเภทโพลีมอร์ฟิก เนื่องจากไวรัสประเภทนี้เปลี่ยนแปลง ตัวเองได้

4. ไวรัสซิกเนเจอร์ที่ใช้สามารถนำมาตรวจสอบได้ก่อนที่ไวรัส จะเปลี่ยนตัวเองเท่านั้น

5. ถ้ามีไวรัสประเภทสทีลต์ไวรัสติดอยู่ในเครื่องตัวสแกนเนอร์อาจจะไม่สามารถ ตรวจหาไวรัสนี้ได้ ทั้งนี้ขึ้นอยู่กับความฉลาดและเทคนิคที่ใช้ของตัวไวรัสและ ของตัวสแกนเนอร์เองว่าใครเก่งกว่า

6. เนื่องจากไวรัสมีตัวใหม่ ๆ ออกมาอยู่เสมอ ๆ ผู้ใช้จึงจำเป็นจะต้องหาสแกนเนอร์ ตัวที่ใหม่ที่สุดมาใช้

7. ไวรัสบางตัวจะเข้าไปติดในโปรแกรมทันทีที่โปรแกรมนั้นถูกอ่าน และถ้าสมมติว่าสแกนเนอร์ที่ใช้ไม่สามารถตรวจจับได้ และถ้าเครื่องมีไวรัสนี้ติดอยู่ เมื่อมีการเรียกสแกนเนอร์ขึ้นมาทำงาน สแกนเนอร์จะเข้าไปอ่านโปรแกรมทีละโปรแกรมเพื่อตรวจสอบ ผลก็คือจะทำให้ไวรัสตัวนี้เข้าไปติดอยู่ในโปรแกรมทุกตัวที่ถูก สแกนเนอร์นั้นอ่านได้

8. สแกนเนอร์รายงานผิดพลาดได้ คือ ไวรัสซิกเนเจอร์ที่ใช้บังเอิญไปตรงกับที่มีอยู่ในโปรแกรมธรรมดาที่ไม่ได้ติดไวรัส ซึ่งมักจะเกิดขึ้นในกรณีที่ไวรัสซิกเนเจอร์ ที่ใช้มีขนาดสั้นไปก็จะทำให้โปรแกรมดังกล่าวใช้งานไม่ได้อีกต่อไป

4.1.5 การตรวจการเปลี่ยนแปลง

การตรวจการเปลี่ยนแปลง คือ การหาค่าพิเศษอย่างหนึ่งที่เรียกว่า เช็คซัม (Checksum) ซึ่งเกิดจากการนำเอาชุดคำสั่งและ ข้อมูลที่อยู่ในโปรแกรมมาคำนวณ หรืออาจใช้ข้อมูลอื่น ๆ ของไฟล์ ได้แก่ แอตริบิวต์ วันและเวลา เข้ามารวมในการคำนวณด้วย เนื่องจากทุกสิ่งทุกอย่าง ไม่ว่าจะเป็นคำสั่งหรือข้อมูลที่อยู่ในโปรแกรม จะถูกแทนด้วยรหัสเลขฐานสอง เราจึงสามารถนำเอาตัวเลขเหล่านี้มาผ่านขั้นตอนการคำนวณทางคณิตศาสตร์ได้ ซึ่งวิธีการคำนวณเพื่อหาค่าเช็คซัมนี้มีหลายแบบ และมีระดับการตรวจสอบแตกต่างกันออกไป เมื่อตัวโปรแกรม ภายในเกิดการเปลี่ยนแปลง ไม่ว่าไวรัสนั้นจะใช้วิธีการแทรกหรือเขียนทับก็ตาม เลขที่ได้จากการคำนวณครั้งใหม่ จะเปลี่ยนไปจากที่คำนวณได้ก่อนหน้านี้

ข้อดีของการตรวจการเปลี่ยนแปลงก็คือ สามารถตรวจจับไวรัสใหม่ๆ ได้ และยังมีความสามารถในการตรวจจับไวรัสประเภทโพลีมอร์ฟิกไวรัสได้อีกด้วย แต่ก็ยังยากสำหรับสทีลต์ไวรัส ทั้งนี้ขึ้นอยู่กับความฉลาดของโปรแกรมตรวจหาไวรัสเองด้วยว่าจะสามารถถูกหลอกโดยไวรัสประเภทนี้ได้หรือไม่ และมีวิธีการตรวจการเปลี่ยนแปลงนี้จะตรวจจับไวรัสได้ก็ต่อเมื่อไวรัสได้เข้าไปติดอยู่ในเครื่องแล้วเท่านั้น และค่อนข้างเสี่ยงในกรณีที่เริ่มมีการคำนวณหาค่าเช็คซัมเป็นครั้งแรก เครื่องที่ใช้ต้องแน่ใจว่าบริสุทธิ์พอ คือต้องไม่มีโปรแกรมใด ๆ ติดไวรัส มิฉะนั้นค่าที่หาได้จากการคำนวณที่รวมตัวไวรัสเข้าไปด้วย ซึ่งจะลำบากภายหลังในการที่จะตรวจหาไวรัสตัวนี้ต่อไป

4.1.6 การเฝ้าดู

เพื่อที่จะให้โปรแกรมตรวจจับไวรัสสามารถเฝ้าดูการทำงานของเครื่องได้ตลอดเวลานั้น จึงได้มีโปรแกรมตรวจจับไวรัสที่ถูกสร้างขึ้นมาเป็นโปรแกรมแบบเรซิเดนท์หรือ ดีไวซ์ไดรเวอร์ โดยเทคนิคของการเฝ้าดูนั้นอาจใช้วิธีการสแกนหรือตรวจการเปลี่ยนแปลงหรือสองแบบรวมกันก็ได้

การทำงานโดยทั่วไปก็คือ เมื่อซอฟแวร์ตรวจจับไวรัสที่ใช้วิธีนี้ถูกเรียกขึ้นมาทำงานก็จะเข้าไปตรวจในหน่วยความจำของเครื่องก่อนว่ามีไวรัสติดอยู่หรือไม่โดยใช้ไวรัสซิกเนเจอร์ ที่มีอยู่ในฐานข้อมูล จากนั้นจึงค่อยนำตัวเองเข้าไปฝังอยู่ในหน่วยความจำ และต่อไปถ้ามีการเรียกโปรแกรมใดขึ้นมาใช้งาน โปรแกรมเฝ้าดูนี้ก็จะเข้าไปตรวจโปรแกรมนั้นก่อน โดยใช้เทคนิคการสแกนหรือตรวจการเปลี่ยนแปลงเพื่อหาไวรัส ถ้าไม่มีปัญหา ก็จะอนุญาตให้โปรแกรมนั้นขึ้นมาทำงานได้ นอกจากนี้โปรแกรมตรวจจับ ไวรัสบางตัวยังสามารถตรวจสอบขณะที่มีการคัดลอกไฟล์ได้อีกด้วย

ข้อดีของวิธีนี้คือ เมื่อมีการเรียกโปรแกรมใดขึ้นมา โปรแกรมนั้นจะถูกตรวจสอบก่อนทุกครั้งโดยอัตโนมัติ ซึ่งถ้าเป็นการใช้สแกนเนอร์ จะสามารถทราบได้ว่าโปรแกรมใดติดไวรัสอยู่ ก็ต่อเมื่อทำการเรียกสแกนเนอร์นั้นขึ้นมาทำงานก่อนเท่านั้น

ข้อเสียของโปรแกรมตรวจจับไวรัสแบบเฝ้าดูก็คือ จะมีเวลาที่เสียไปสำหรับการตรวจหาไวรัสก่อนทุกครั้ง และเนื่องจากเป็นโปรแกรมแบบเรซิเดนท์หรือดีไวซ์ไดรเวอร์ จึงจำเป็นจะต้องใช้หน่วยความจำส่วนหนึ่งของเครื่องตลอดเวลาเพื่อทำงาน ทำให้หน่วยความจำในเครื่องเหลือน้อยลง และเช่นเดียวกับสแกนเนอร์ ก็คือ จำเป็นจะต้องมีการปรับปรุง ฐานข้อมูลของไวรัสซิกเนเจอร์ให้ทันสมัยอยู่เสมอ

4.1.7 คำแนะนำและการป้องกันไวรัส

- สำรองไฟล์ข้อมูลที่สำคัญ
- สำหรับเครื่องที่มีฮาร์ดดิสก์ อย่าเรียกดอสจากฟลอปปีดิสก์
- ป้องกันการเขียนให้กับฟลอปปีดิสก์
- อย่าเรียกโปรแกรมที่ติดมากับดิสก์อื่น
- เสาะหาโปรแกรมตรวจหาไวรัสที่ใหม่และมากกว่าหนึ่งโปรแกรมจากคนละบริษัท
- เรียกใช้โปรแกรมตรวจหาไวรัสเป็นช่วง ๆ
- เรียกใช้โปรแกรมตรวจจับไวรัสแบบเฝ้าดูทุกครั้ง
- เลือกคัดลอกซอฟแวร์เฉพาะที่ถูกตรวจสอบแล้วในบีบีเอส
- สำรองข้อมูลที่สำคัญของฮาร์ดดิสก์ไปเก็บในฟลอปปีดิสก์
- เตรียมฟลอปปีดิสก์ที่ไว้สำหรับให้เรียกดอสขึ้นมาทำงานได้
- เมื่อเครื่องติดไวรัส ให้พยายามหาที่มาของไวรัสนั้น

5. วิธีการดำเนินการ

5.1 เสนอหัวข้อโครงงาน

5.1.1 ศึกษาหัวข้อโครงงานที่สนใจ

5.1.3 กำหนดหัวข้อโครงงาน

5.1.4 เสนอหัวข้อโครงงานกับอาจารย์ที่ปรึกษา

5.2 ศึกษาบทความและค้นคว้าข้อมูล

5.2.1 ศึกษาค้นคว้าโปรแกรม Razor Batch Virus Builder

5.2.2 ศึกษาหลักการและขั้นตอนการสร้างไฟล์ไวรัส

5.3 นำเสนอเค้าโครง

5.3.1 นำเสนอเค้าโครงกับอาจารย์ที่ปรึกษาประจำรายวิชา

5.4. ศึกษาเทคนิคและเครื่องมือที่ใช้

5.4.1 ศึกษาวิธีใช้โปรแกรม Razor Batch Virus Builder

5.4.2 ศึกษาวิธีการเขียนไฟล์ไวรัส

5.5 วิเคราะห์และออกแบบ

5.5.1ไฟล์ไวรัสสามารถปิด fire wall อัตโนมัติ

5.5.2 ไฟล์ไวรัสสามารถตัดการใช้งานอินเทอร์เน็ต

5.6 พัฒนาระบบ

5.6.1 ใช้โปรแกรม Razor Batch Virus Builder เขียนไฟล์ไวรัสให้สามารถrun บน ระบบปฏิบัติการ window 7

5.7 ทดสอบระบบ

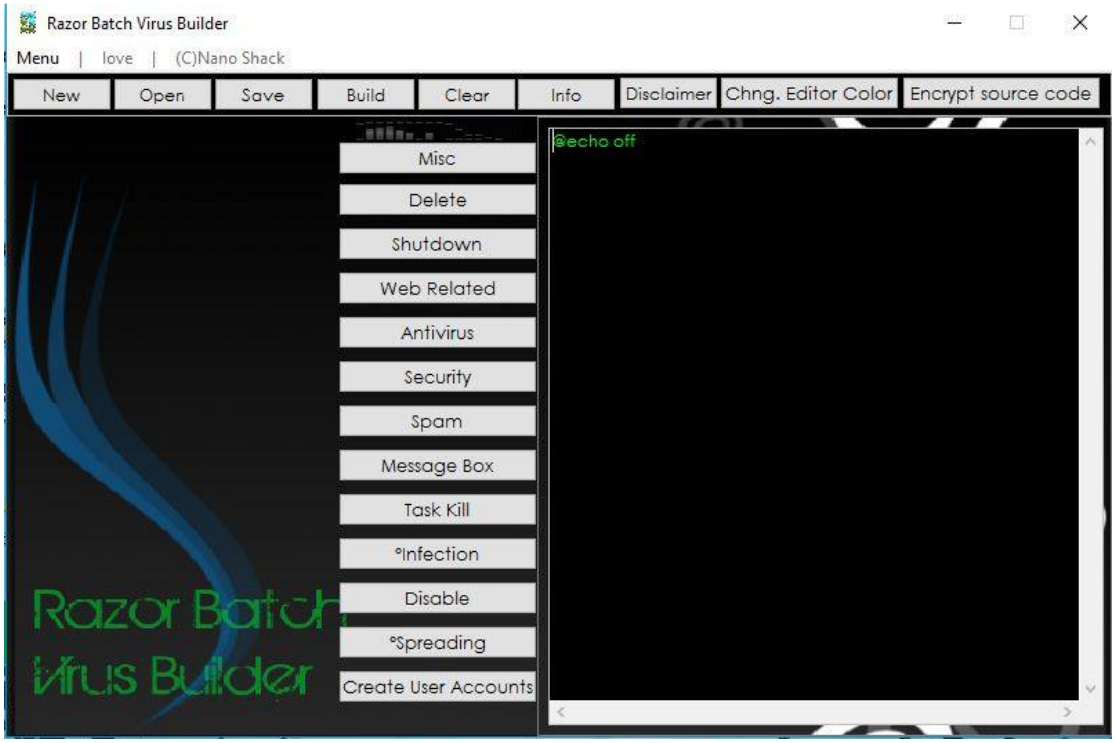
5.7.1นำไฟล์ไวรัสที่สร้างขึ้นไปใส่ไว้ในเครื่องเป้าหมายแล้วดูผลลัพธ์

5.8 สรุปผล

5.8.1 สรุปผลการดำเนินงานตามวัตถุประสงค์และจัดทำเล่มโครงงาน

5.9 นำเสนอโครงงาน

คู่มือการใช้งาน โปรแกรม Razor Batch Virus Builder



ภาพที่ 1 หน้าหลักของโปรแกรม โดยจะมีเมนูต่างให้เราสามรถเลือกใช้งาน

ปุ่ม Misc เมื่อคลิกจะมีแถบเมนูเพิ่มขึ้นมาอีกเมนูทางซ้าย ได้แก่

1. Confuse File Extension ปรับเปลี่ยนนามสกุลของไฟล์

2. Swap Mouse สามารถทำให้ Mouse สลับการคลิก

3.Open Disk Tray สามารถเปิดถาดใส่แผ่น Cd/Dvd

4. Change User Password สามารถเปลี่ยนรหัสผ่านของผู้ใช้

5. Self Destruct ทำลายตัวเองเป็นการลบไฟล์

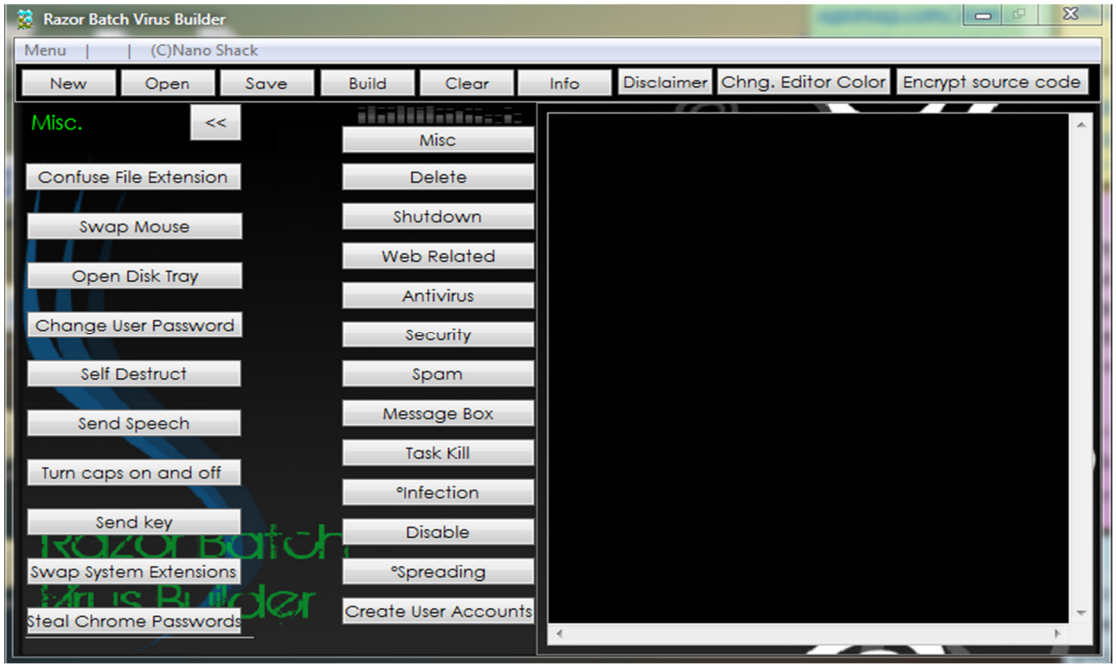
6. Send Speech ส่งคำพูด

7. Turn Caps on and off เปิด/ปิด capslock

8. Send key

9. Swap System Extensionsเปลี่ยน System Extensions

10. Steal Chorme Passwords ขโมยรหัสผ่าน Chorme



ภาพที่ 2 เมื่อคลิกจะมีแถบเมนูเพิ่มขึ้นมาอีกเมนูทางซ้าย

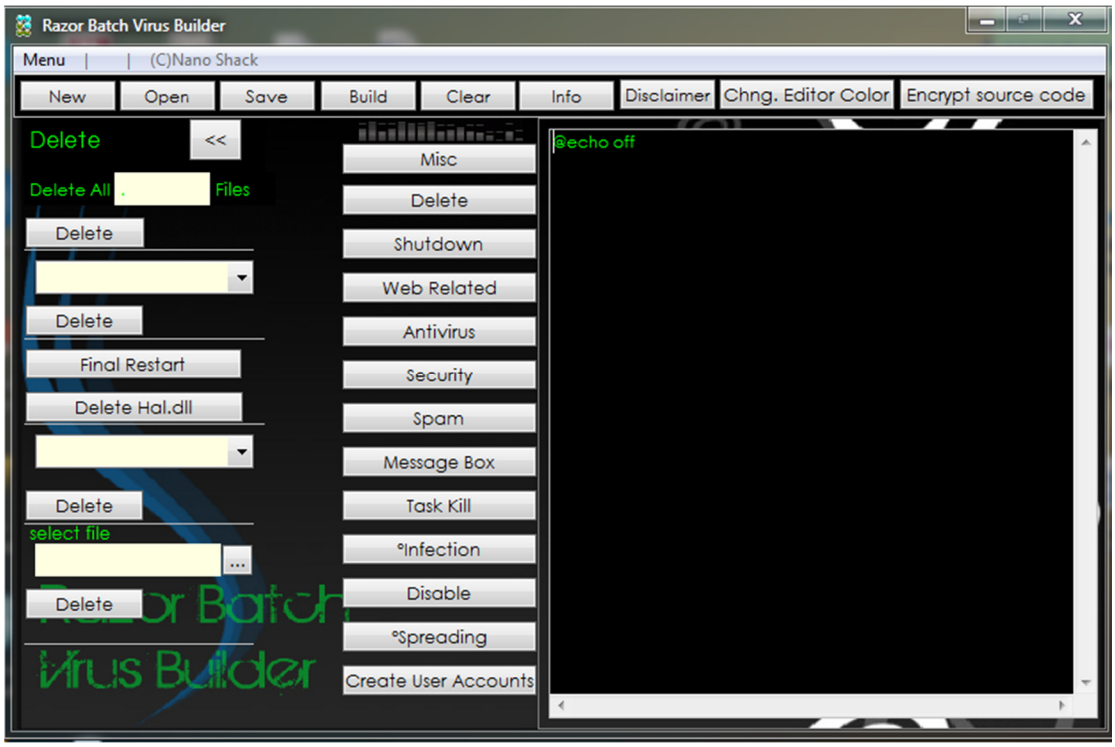
ปุ่ม Delete เมื่อคลิกจะมีแถบเมนูเพิ่มขึ้นมาอีกเมนูทางซ้าย มีช่องให้กรอกไฟล์ที่จะลบสามารถเลือกได้ว่าจะลบที่ใด ลบที่ My Document, My Music, My Pictures

1. Final Restart หลังจากการลบเสร็จแล้วรีสตาร์ทเครื่องคอมพิวเตอร์

2. Delete Hal.dll คือลบHal.dll ซึ่งถ้าเกิด error “Cannot find hal.dll” แสดงว่าเกิดปัญหาขึ้นกับ Windows

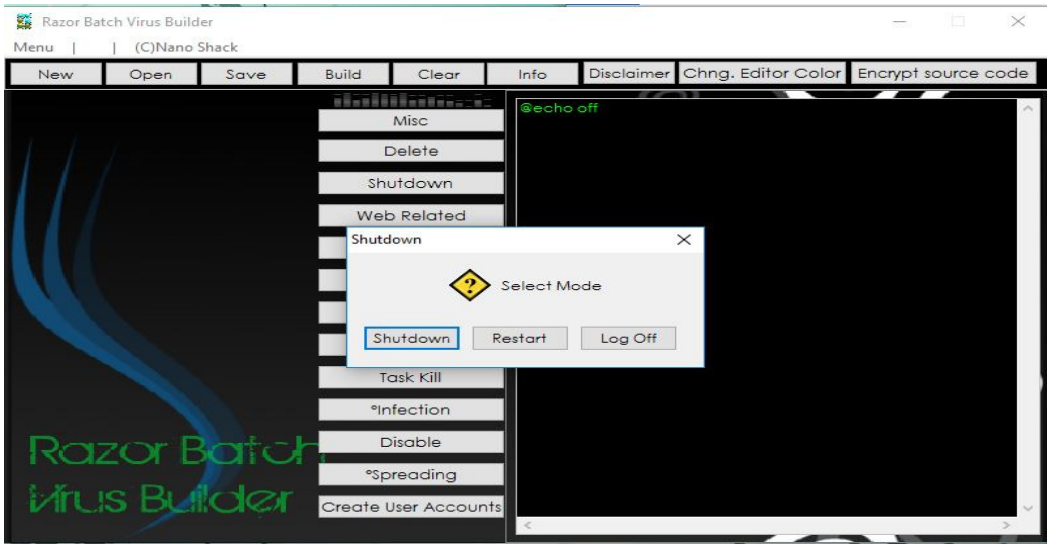
3. Library file หรือไฟล์ที่เปรียบเสมือนเป็นห้องสมุดของวินโดวส์ แล้วหล่ะครับ นั่นคือ ไฟล์ “hal.dll”ในเครื่องวินโดวส์ของเราได้เสียหาย ถูกลบหรือย้ายไปจากที่ๆมันควรจะอยู่ เลยทำให้วินโดวส์ไม่สามารถบู้ตเครื่องเข้าสู่ระบบได้

4. Select file เลือกไฟล์ที่จะ Delete

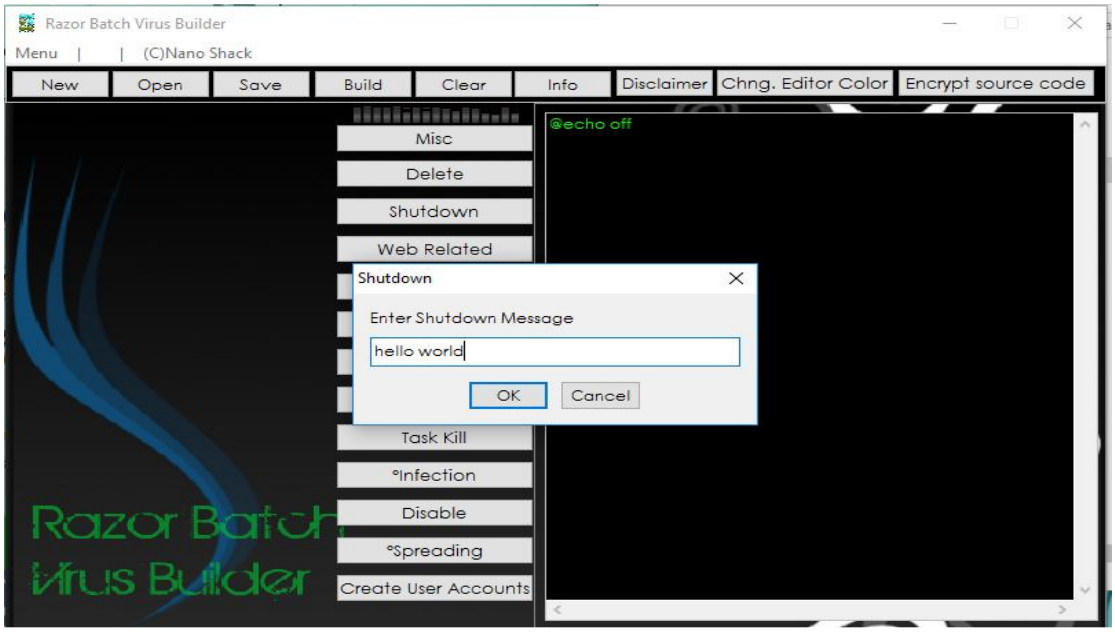


ภาพที่ 3 เมื่อคลิกจะมีแถบเมนูเพิ่มขึ้นมาอีกเมนูทางซ้าย มีช่องให้กรอกไฟล์ที่จะลบสามารถเลือกได้ว่าจะลบที่ใด ลบที่ My Document, My Music, My Pictures

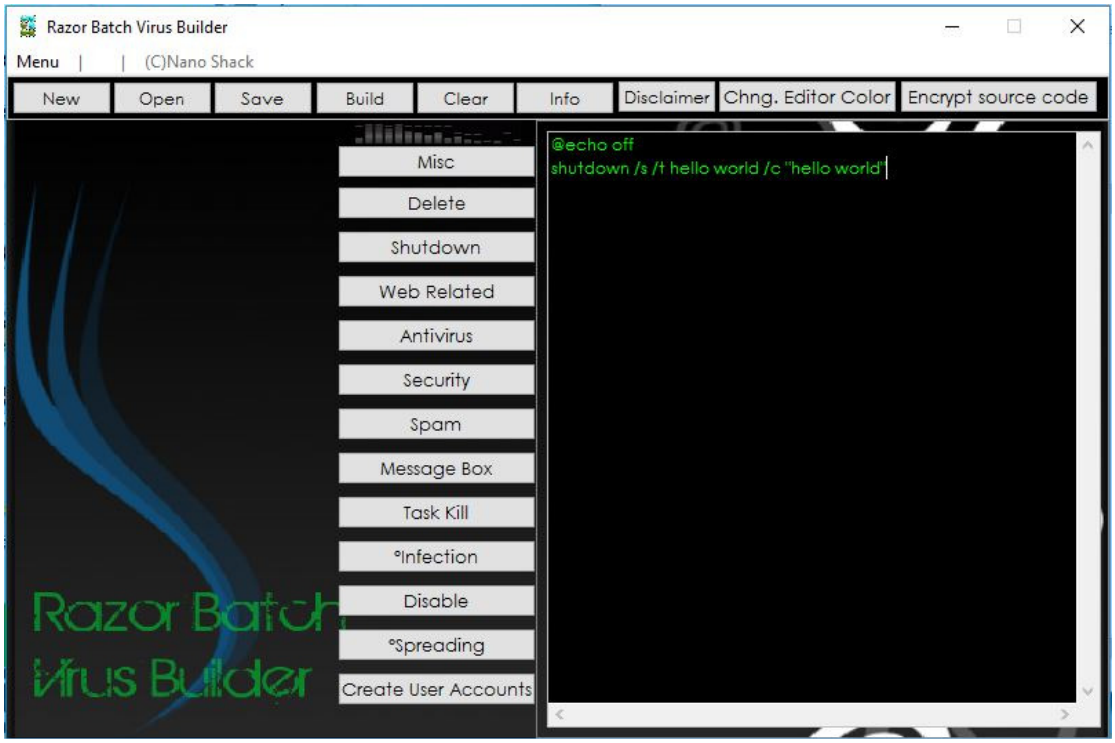
ปุ่ม Shutdown



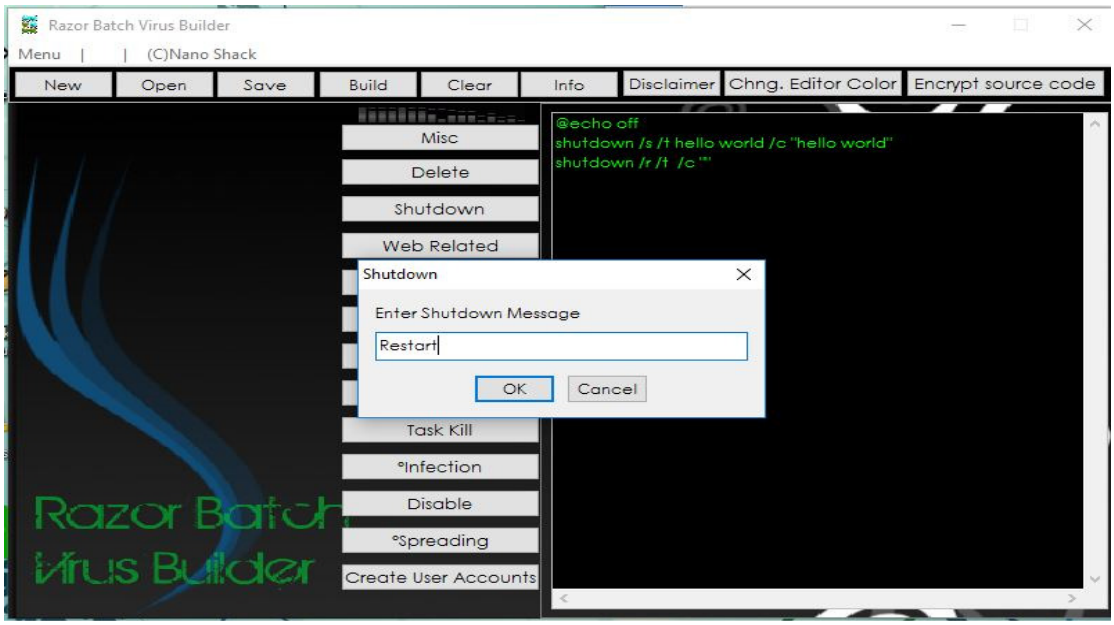
ภาพที่ 4 จะมีเมนูให้เลือก 3 เมนู ได้แก่ Shutdown, Restart, Log Off



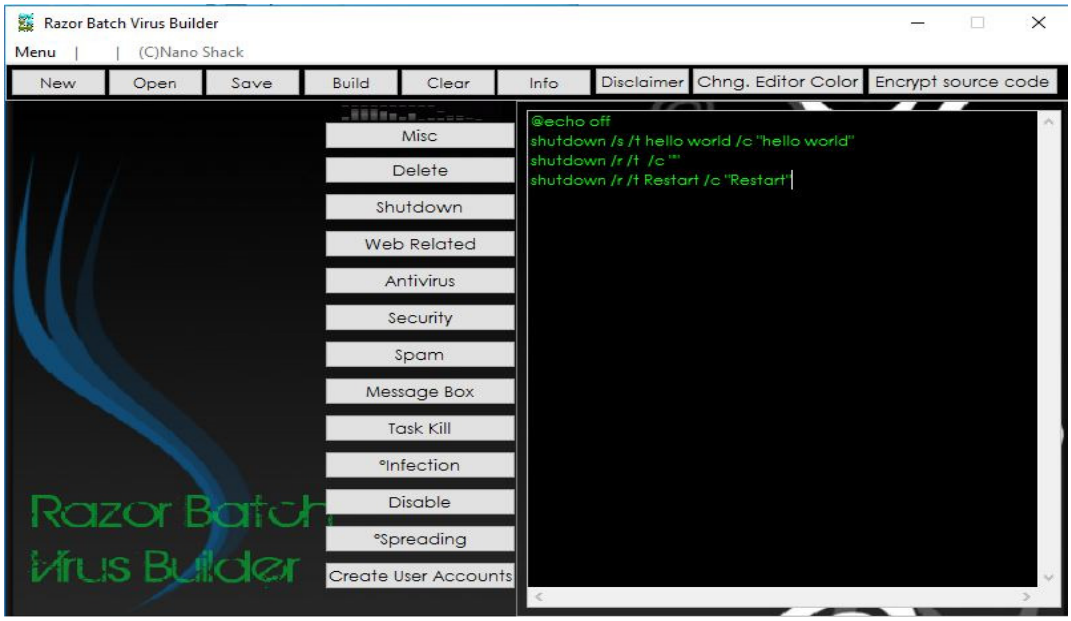
ภาพที่ 5 ถ้าเลือกเมนู Shutdown โปรแกรมจะให้กรอก Enter Shutdown Massage เพื่อที่ว่าก่อนเครื่องคอมพิวเตอร์จะ shutdown จะมีการแสดงข้อความออกมา



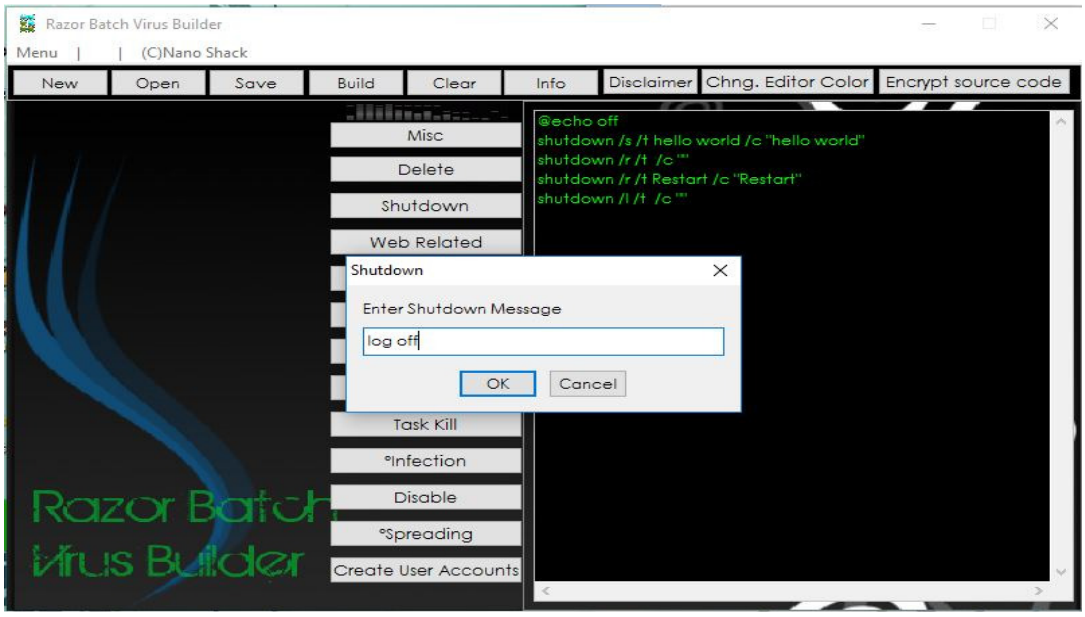
ภาพที่ 6 โปรแกรมแสดงข้อความออกมาก่อนที่เครื่องจะดับ



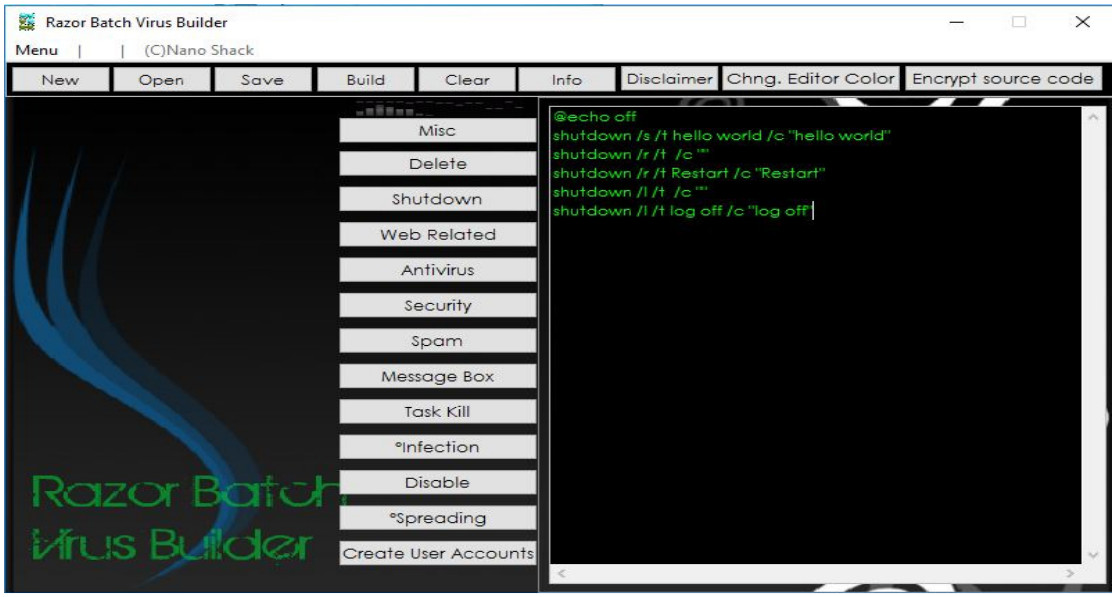
ภาพที่ 7 ถ้าเลือกเมนู Restart โปรแกรมจะให้กรอก Enter Shutdown Massage เพื่อที่ว่าก่อนที่คอมพิวเตอร์จะทำการ Restart จะมีการแสดงข้อความออกมา



ภาพที่ 8 โปรแกรมแสดงข้อความออกมาก่อนที่คอมพิวเตอร์จะทำการ Restart



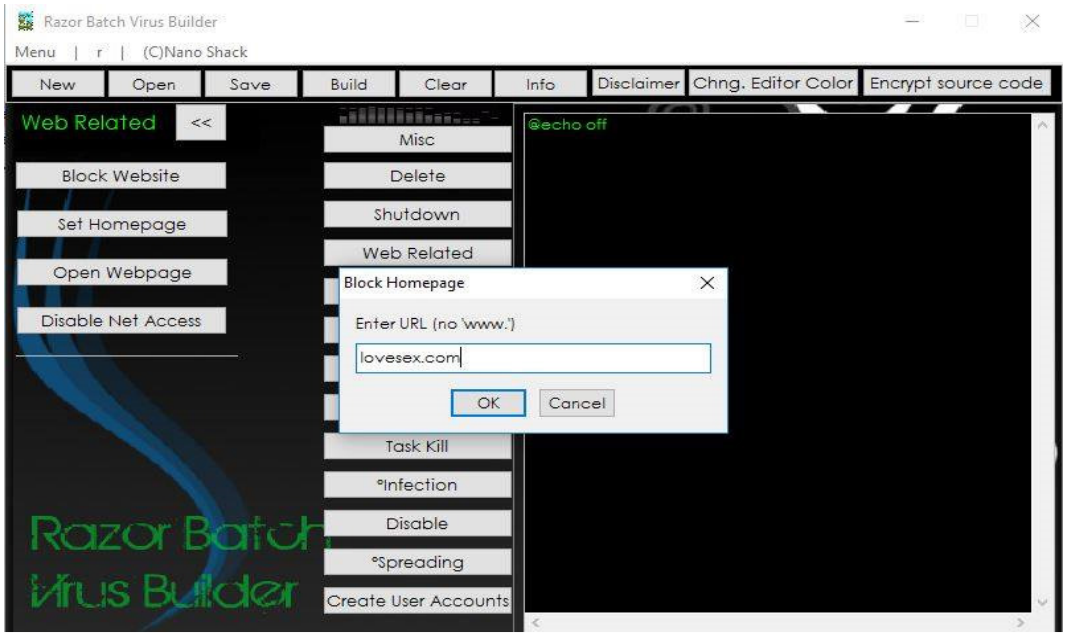
ภาพที่ 9 ถ้าเลือกเมนู Log off โปรแกรมจะให้กรอก Enter Shutdown Massage เพื่อที่ว่าก่อนที่คอมพิวเตอร์จะทำการ Log off หรือการออกจากรหัสที่เคยตั้งไว้ จะมีการแสดงข้อความออกมา



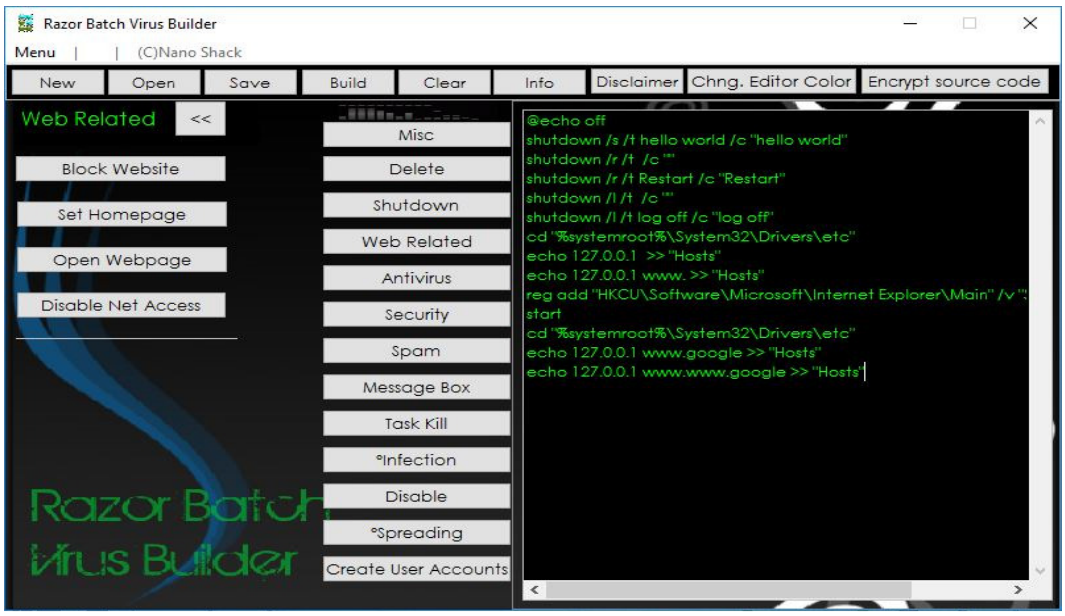
ภาพที่ 10 โปรแกรมแสดงข้อความออกมาก่อนที่คอมพิวเตอร์จะทำการ Log off

ปุ่ม Web Related โดยจะมีเมนูให้เลือก 4 เมนู ได้แก่

- **Block Website**

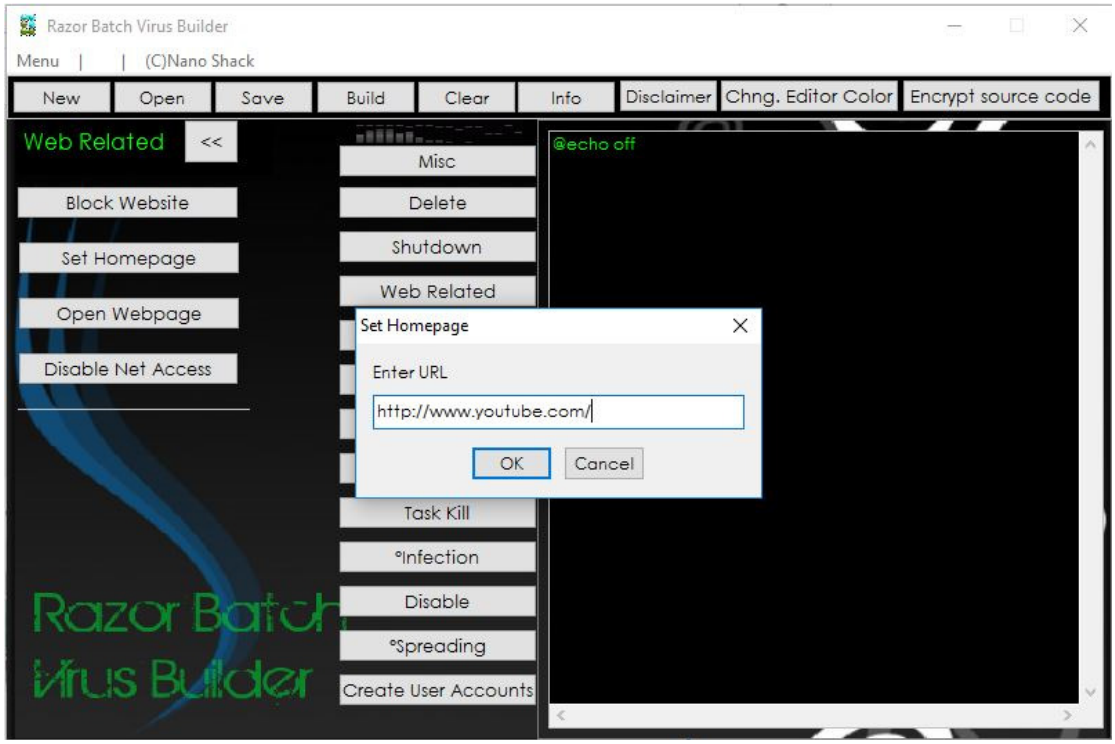


ภาพที่ 11 โปรแกรมจะให้กรอก URL ของเว็บต่างๆ ที่ต้องการจะ Block ซึ่งในที่นี้จะไม่สามารถบล็อก URL ที่เป็น www ได้

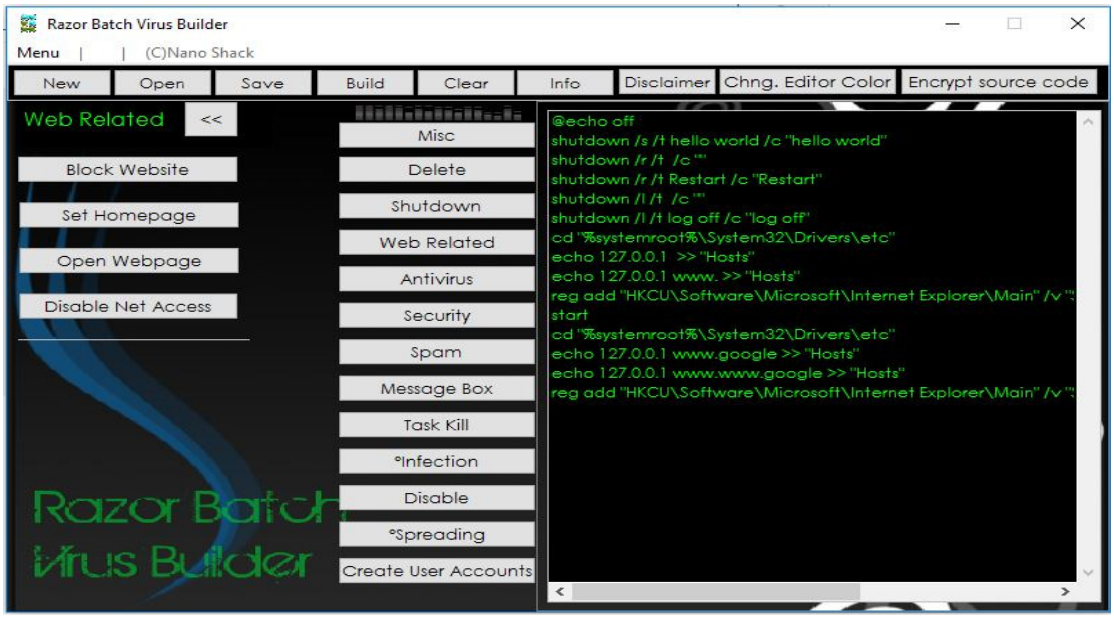


ภาพที่ 12 โปรแกรมจะแสดง URL ของเว็บที่ต้องการจะ Block

- **Set Homepage**

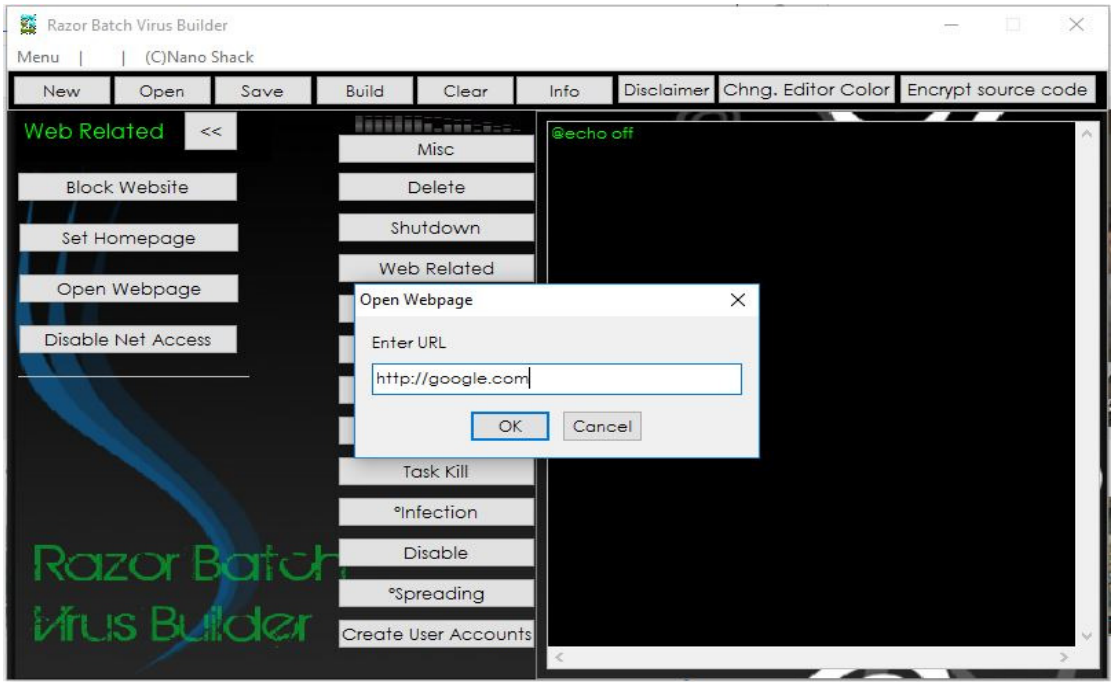


ภาพที่ 13 โปรแกรมจะให้กรอก URL ของเว็บต่างๆ ที่ต้องการจะเข้าดูหน้า Homepage นั้นๆ

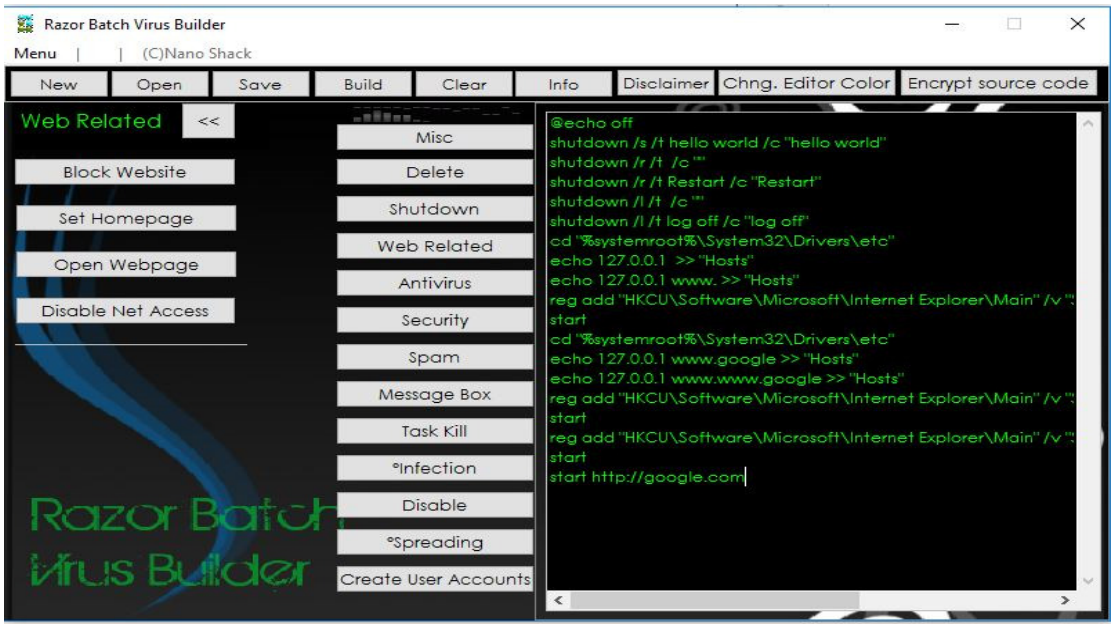


ภาพที่ 14 โปรแกรมจะแสดง URL ของเว็บที่ต้องการจะเข้าดู

- **Open Webpage**

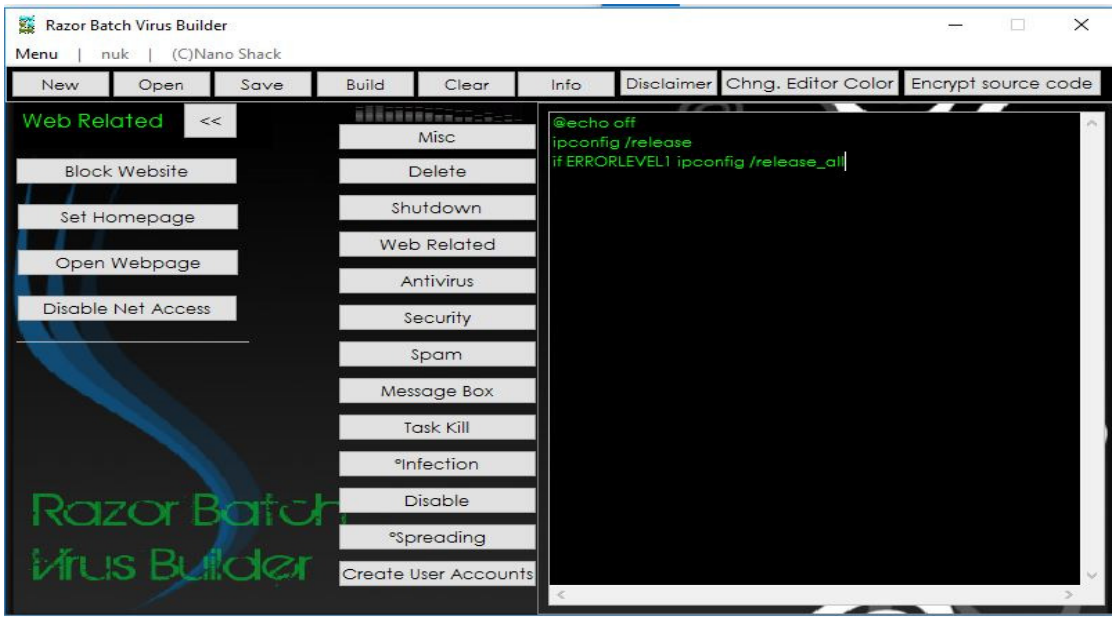


ภาพที่ 15 โปรแกรมจะให้กรอก URL ของเว็บต่างๆ ที่ต้องการจะเปิด



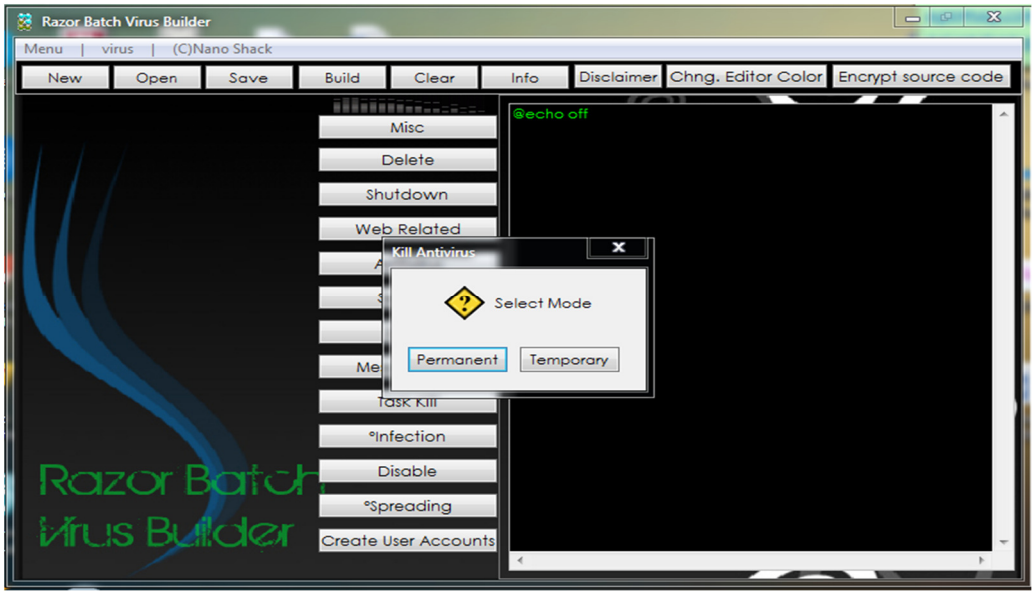
ภาพที่ 16 โปรแกรมจะแสดง URL ของเว็บที่ต้องการจะเปิด

- Disable Net Access

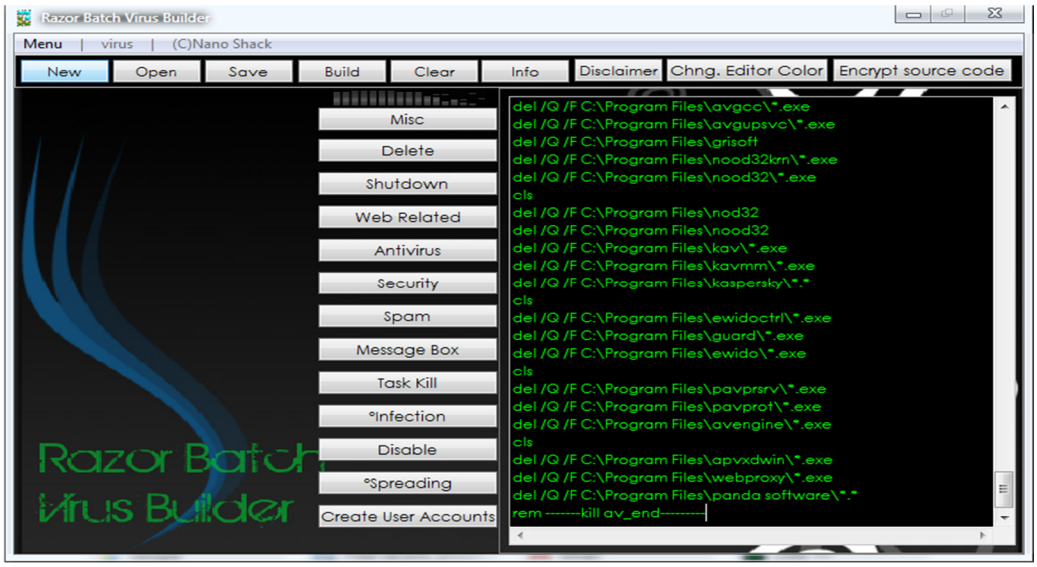


ภาพที่ 17 เป็นการตัด internet ซึ่งจะไม่สามารถใช้งานได้

ปุ่ม Antivirus

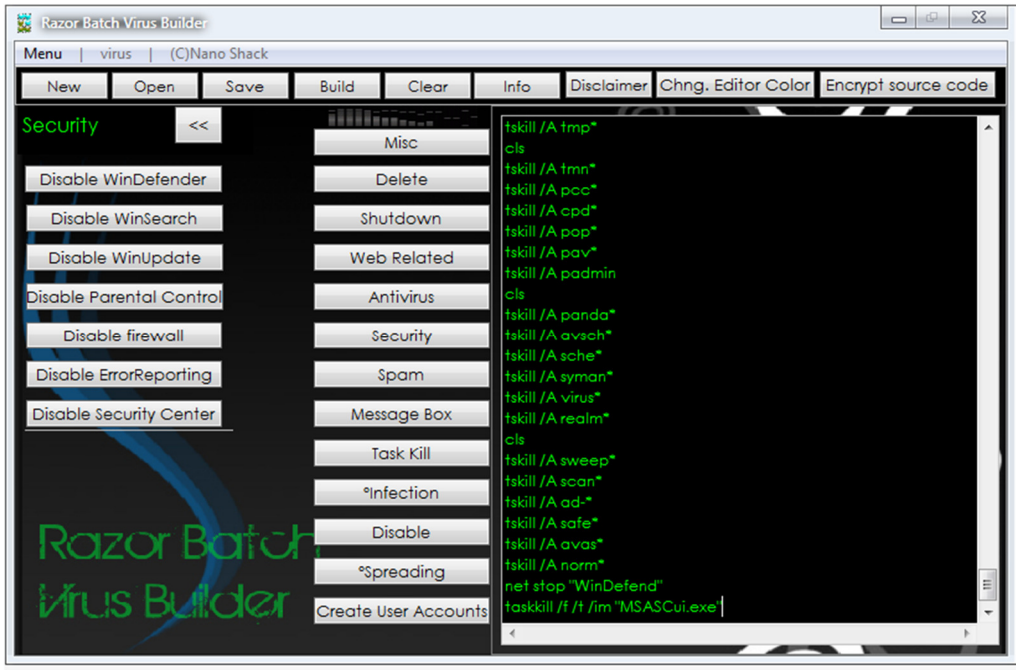


ภาพที่ 18 มี 2 Mode ให้เลือก คือ Permanent และ Temporary ปิดการใช้งานป้องกันไวรัสของระบบ



ภาพที่ 19 เป็นการปิดใช้งานป้องกันไวรัสของระบบ ซึ่งจะมี C:\\Program ที่เราต้องการปิด

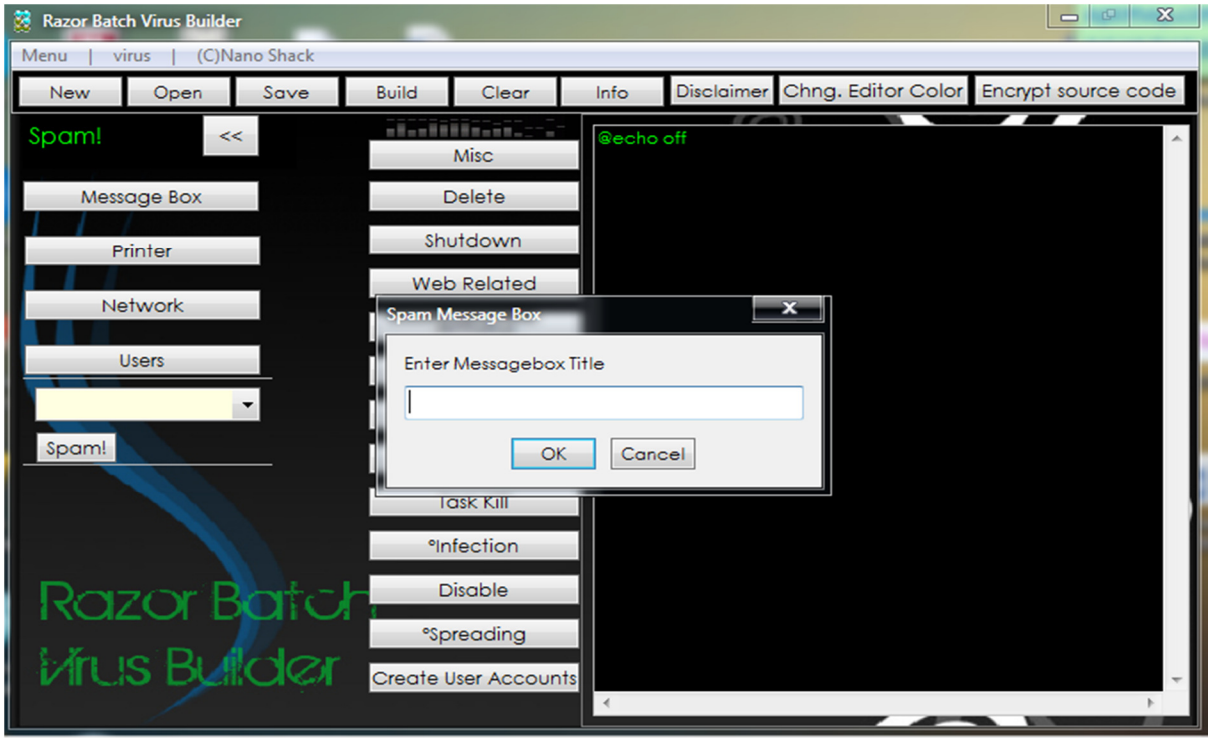
ปุ่ม Security



ภาพที่ 20 เมื่อคลิกจะมีแถบเมนูเพิ่มขึ้นมาอีกเมนูทางซ้าย ได้แก่

- Disable WinDefender สามารถปิดการใช้งาน โปรแกรม WinDefenderเป็นโปรแกรมสแกนไวรัสที่มาพร้อมกับ Windows
- DisableWinSearch สามารถปิดการใช้งานช่อง Search ของ Start Menu หรือที่ ช่อง Search ที่ Windows Explore
- DisableWinUpdate สามารถปิดการใช้งานการ Update โปรแกรม Security และโปรแกรมอื่นๆ
- DisableParental Control สามารถปิดการใช้งานParental controls ระบบที่ช่วยควบคุมการเข้าใช้งานคอมพิวเตอร์
- Disable firewall สามารถปิดการใช้งาน firewall ของเครื่องคอมพิวเตอร์
- DisableErroReporting สามารถปิดการใช้งานการแจ้งเตือนความผิดพลาดของ Windows
- DisableSecurity Center สามารถปิดการใช้งานWindows Security Monitor ไม่ให้แจ้งเตือนบนหน้าจอคอมพิวเตอร์

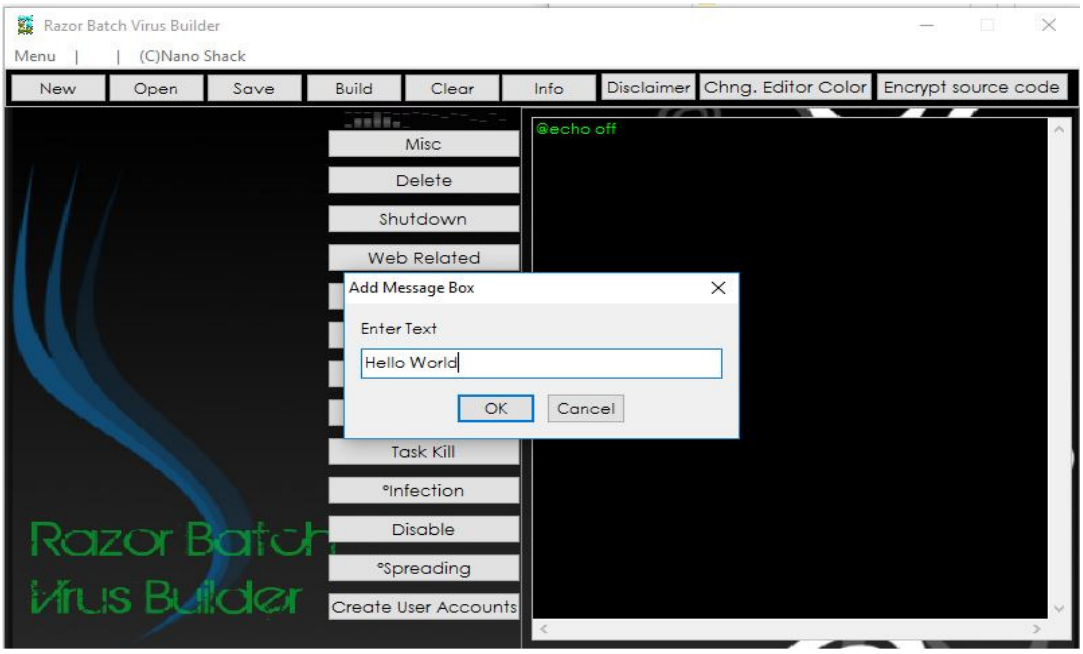
ปุ่ม Spam



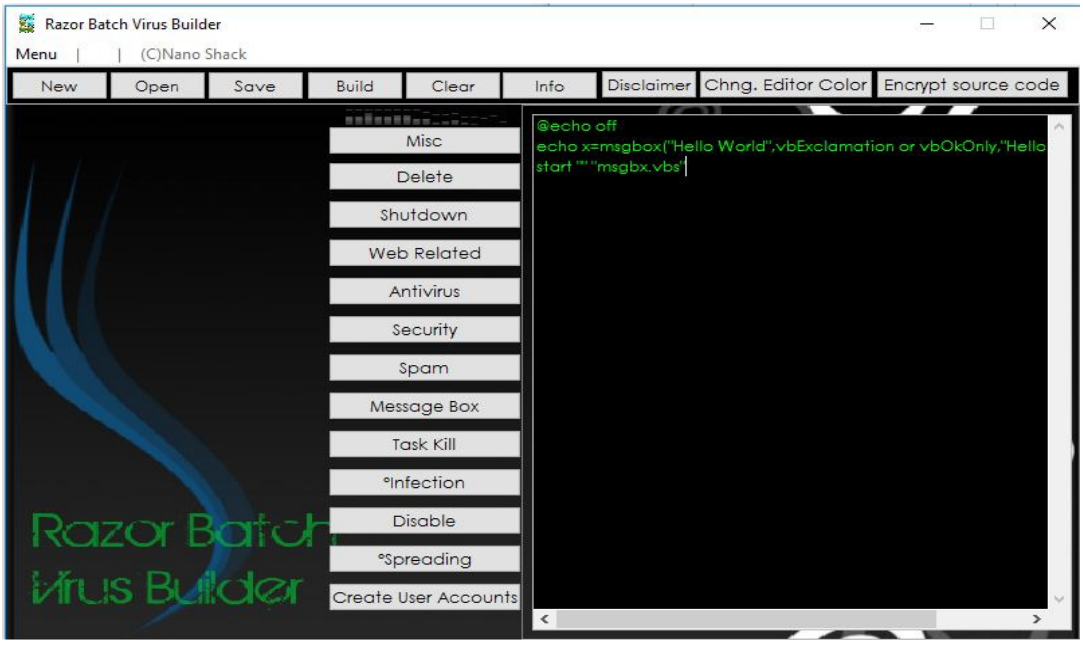
ภาพที่ 21 เมื่อคลิกจะมีแถบเมนูเพิ่มขึ้นมาอีกเมนูทางซ้าย ได้แก่

- Message Box เป็นการสร้างไวรัสที่เป็นกล่องข้อความ
- Network ส่งกล่องข้อความไปยังวงแลน
- Userส่งกล่องข้อความไปให้ User โดยสุ่ม User ที่จะส่ง

ปุ่ม Message Box เป็นการสร้างไวรัสที่เป็นกล่องข้อความที่จะแสดงบนจอภาพ พร้อมด้วยข้อความบางอย่าง

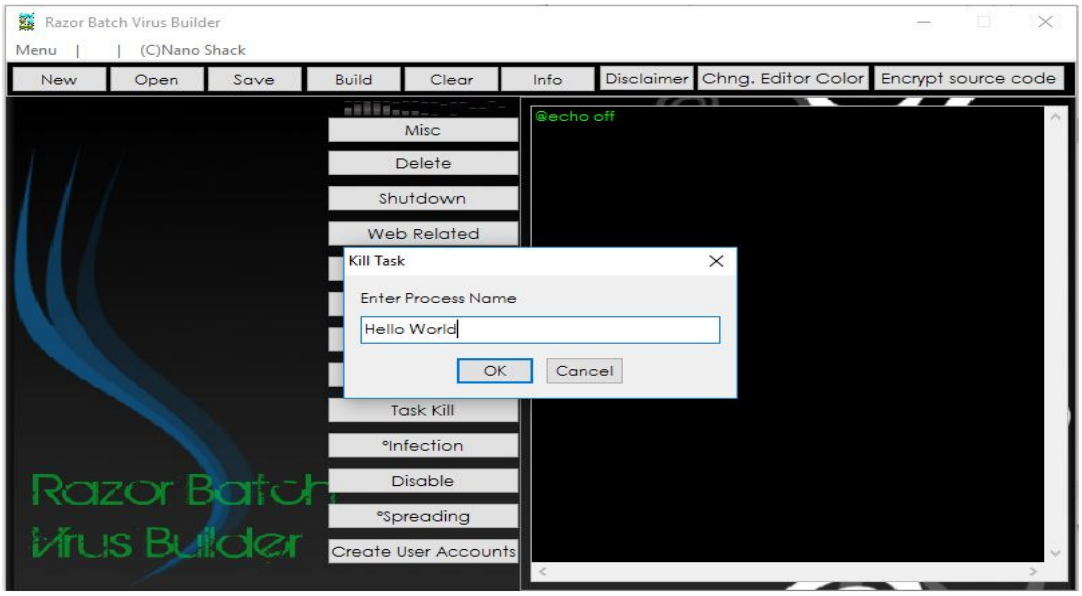


ภาพที่ 22 โปรแกรมจะให้กรอก Enter Text ที่ต้องการจะให้แสดง เป็นการแสดงข้อความ

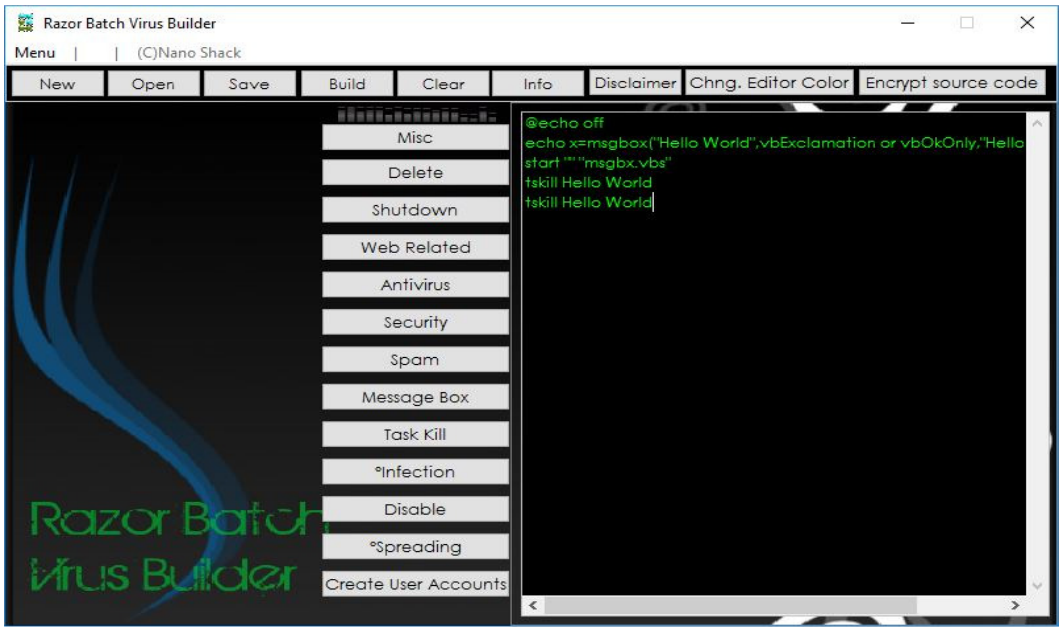


ภาพที่ 23 จะมีการแสดงข้อความที่เรากรอกในที่นี้เรากรอกคำว่า Hello World

ปุ่ม Task Kill เป็นการลบโปรแกรมที่ไม่มีการใช้งาน

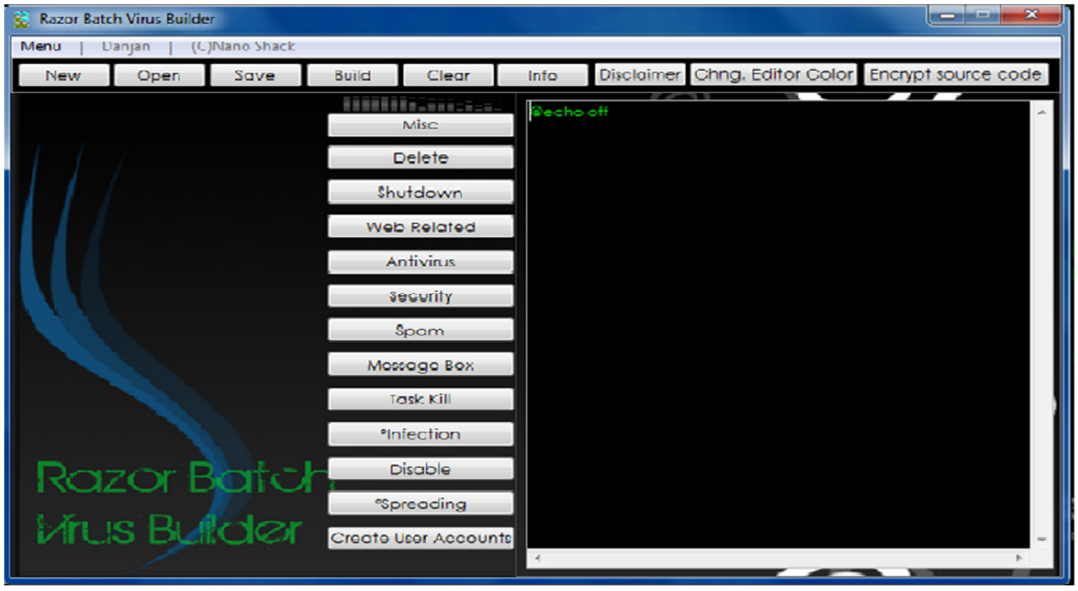


ภาพที่ 24 โปรแกรมจะให้กรอก Enter Process Name ซึ่ง Task Kill เป็นตัวปิดโปรแกรมที่ไม่ต้องการใช้



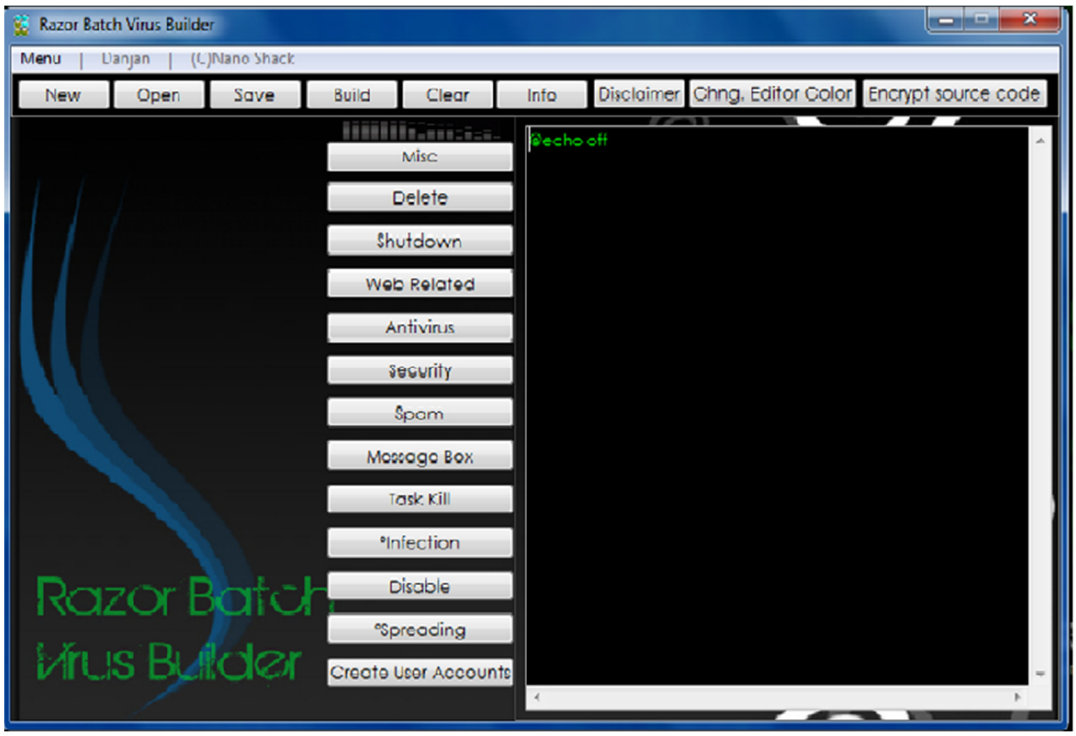
ภาพที่ 25 จะมีการแสดงข้อความที่เรากรอกในที่นี้เรากรอกคำว่า Hello World

ปุ่ม Infection



ภาพที่ 26 เป็นกลไกทำหน้าที่คัดลอกตัวเองไปฝังหรือแนบกับโปรแกรมหรือไฟล์อื่น สรุปคือทำหน้าที่แพร่กระจาย และ ค้นหาช่องโหว่ หรือ จุดอ่อนของคอมพิวเตอร์ในเครือข่าย

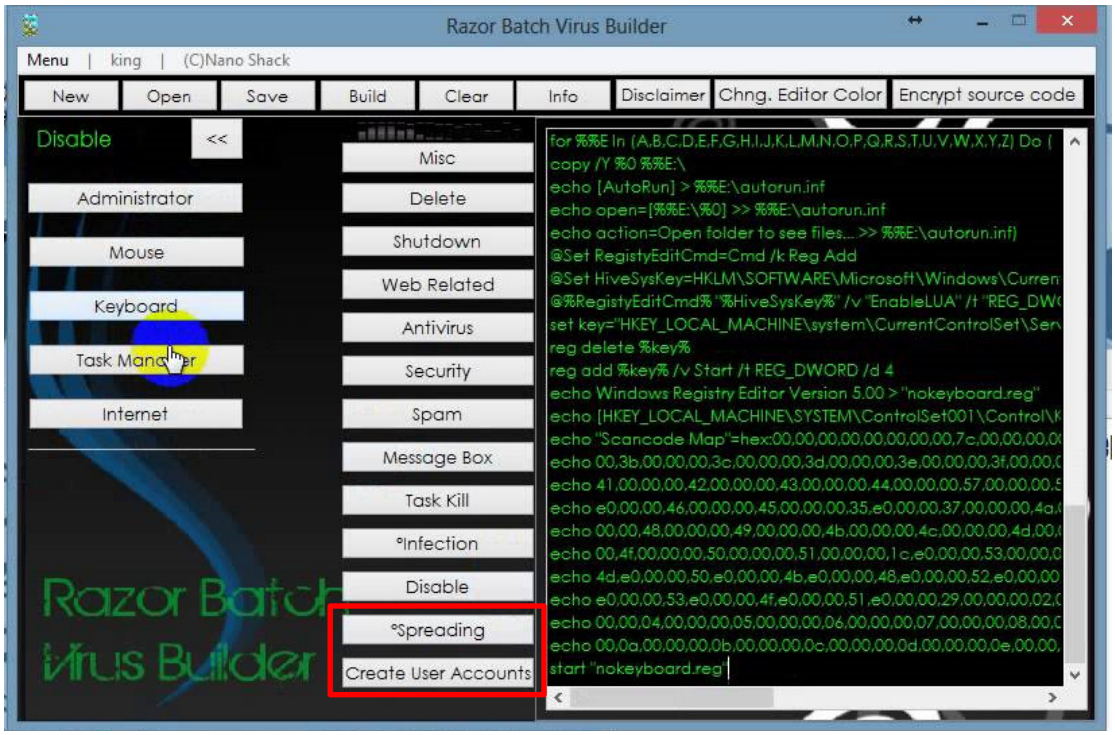
ปุ่ม Disable



ภาพที่ 27 คือการ เลือกเซ็ตให้ปิดการทำงานของศูนย์รักษาความปลอดภัยอัตโนมัติเป็นการปิดการทำงานของ Services ไม่ให้มีการทำงาน

ปุ่ม Spreading

ปุ่ม Create User Accounts



ภาพที่ 28 Spreading เป็นฟังก์ชันที่สามารถแพร่กระจายไปทั่วคอมพิวเตอร์โดยนำไฟล์ที่สร้างขึ้นไปใส่ไว้ในเครื่องเป้าหมาย ไวรัสจะทำการสำเนาตัวเองไปไว้ตามโฟล์เดอร์ต่างๆ

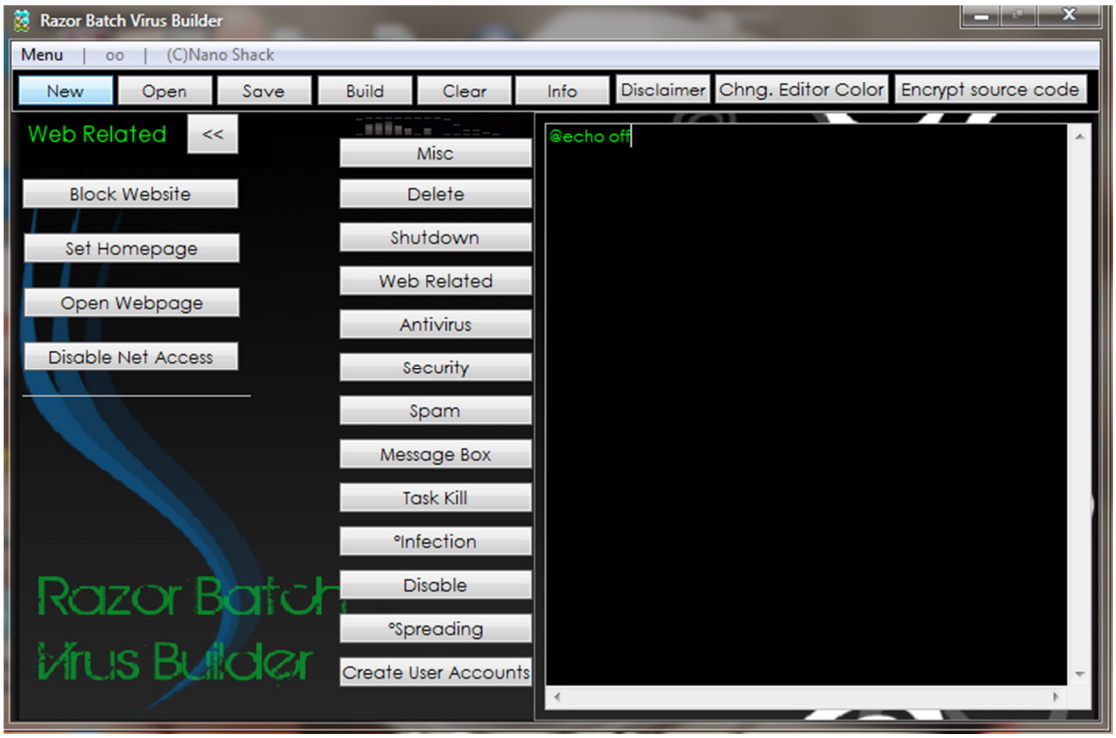
Create User Accounts เป็นฟังก์ชันที่จะสร้างบัญชีผู้ใช้ขึ้นมาใหม่โดยอัตโนมัติ บัญชีของคุณจะส่งผลกระทบต่อโปรแกรมประยุกต์ต่าง ๆ ที่ติดตั้งในขณะที่การตั้งค่าและเอกสารที่บันทึกไว้จะถูกเก็บไว้ทั้งหมดเฉพาะในบัญชีของคุณ

ตัวอย่างการสร้างไวรัส

เป็นไวรัสที่สามารถ Block เว็บ เพื่อให้ไม่สามารถเข้าถึงได้

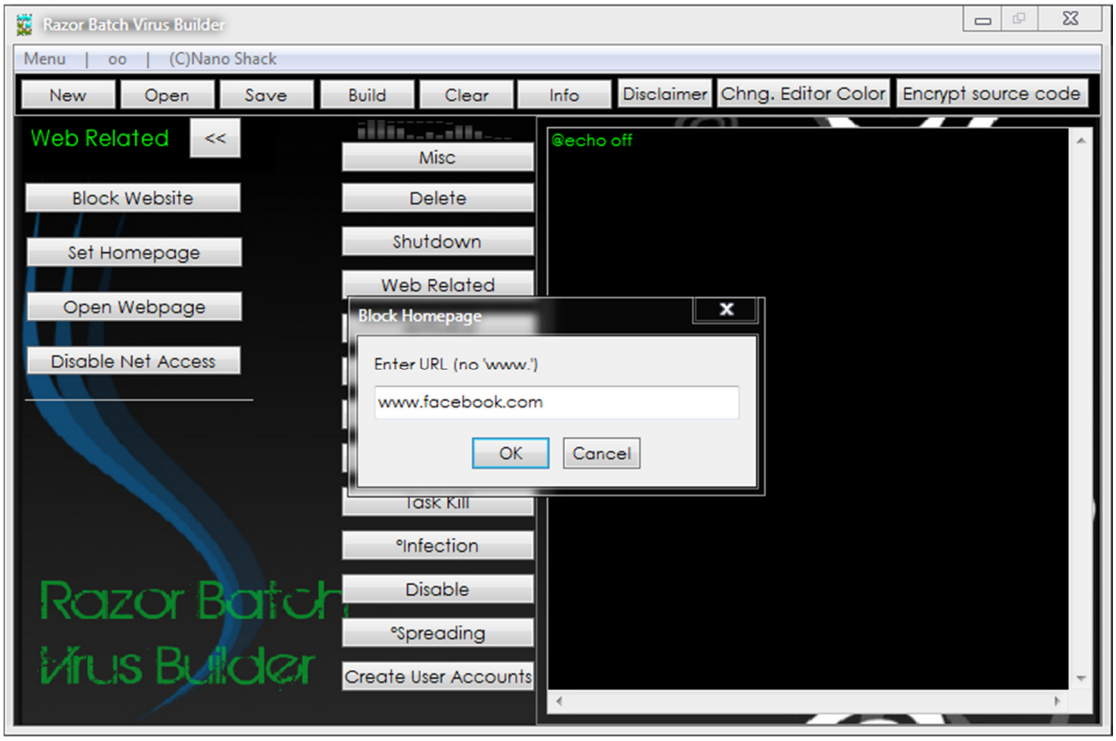
1.เปิดโปรแกรม Razor Batch Virus Builder

คลิกที่ Web Related แล้วคลิกที่ Block Website



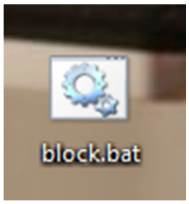
2.ใส่ URL ของเว็บที่ต้องการ

เช่น www.facebook .com แล้วกด OK

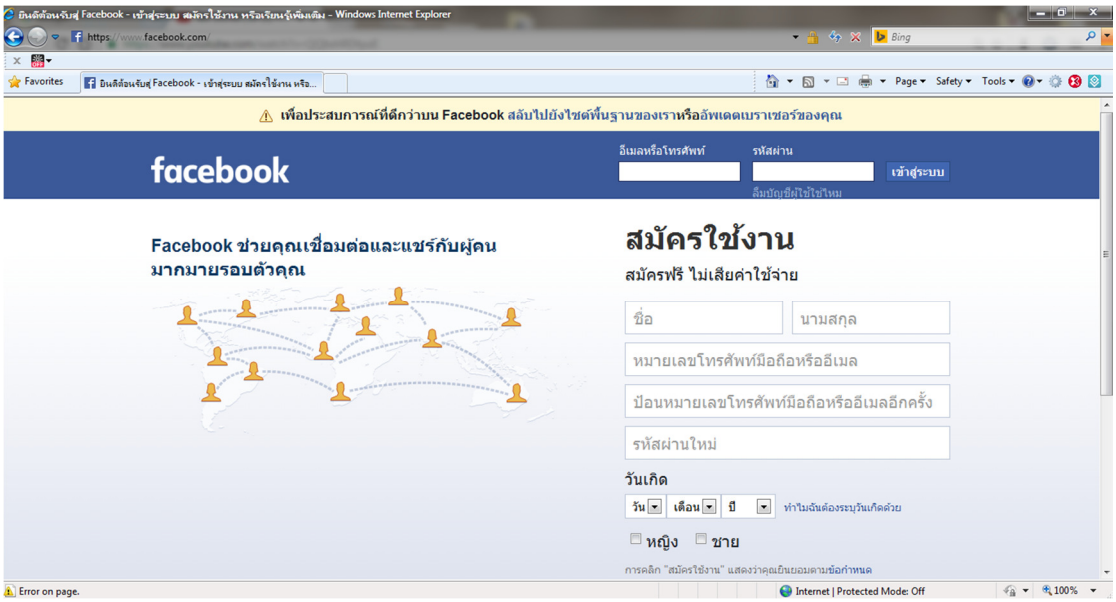


Code ที่ได้

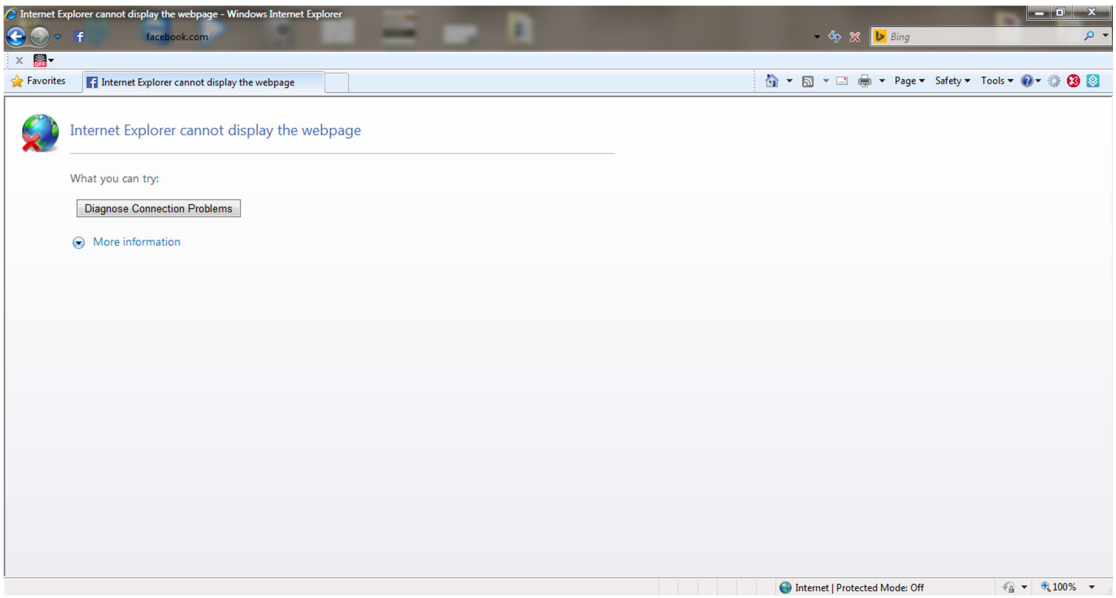
3.กด Build เพื่อสร้างไวรัส ที่เป็นนามสกุล .bat



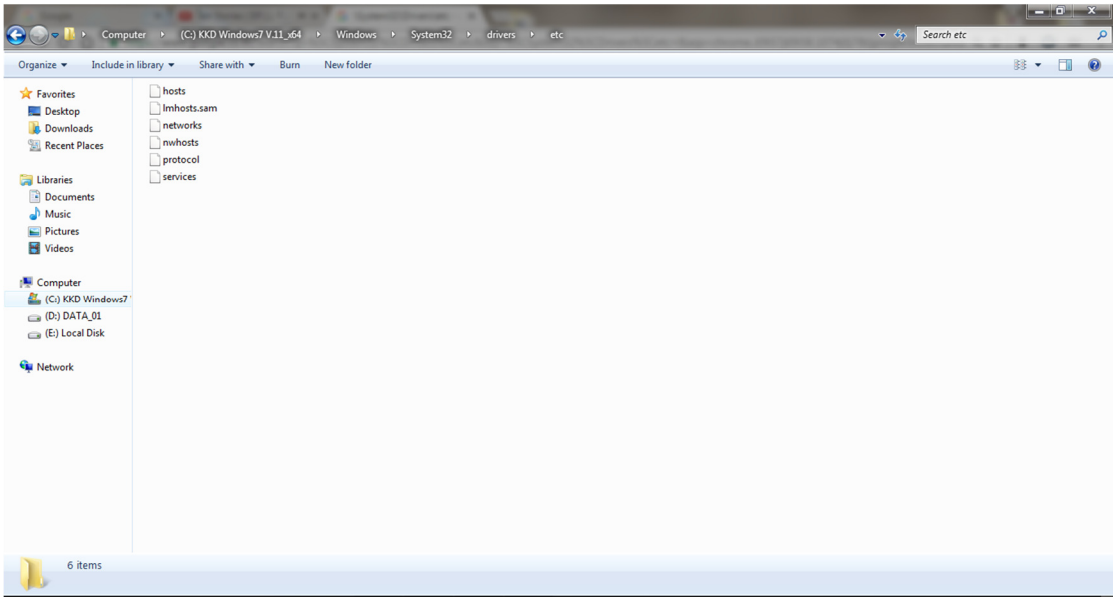
4. ก่อนเปิดไฟล์ไวรัส www.facebook.com ยังสามารถเข้าได้



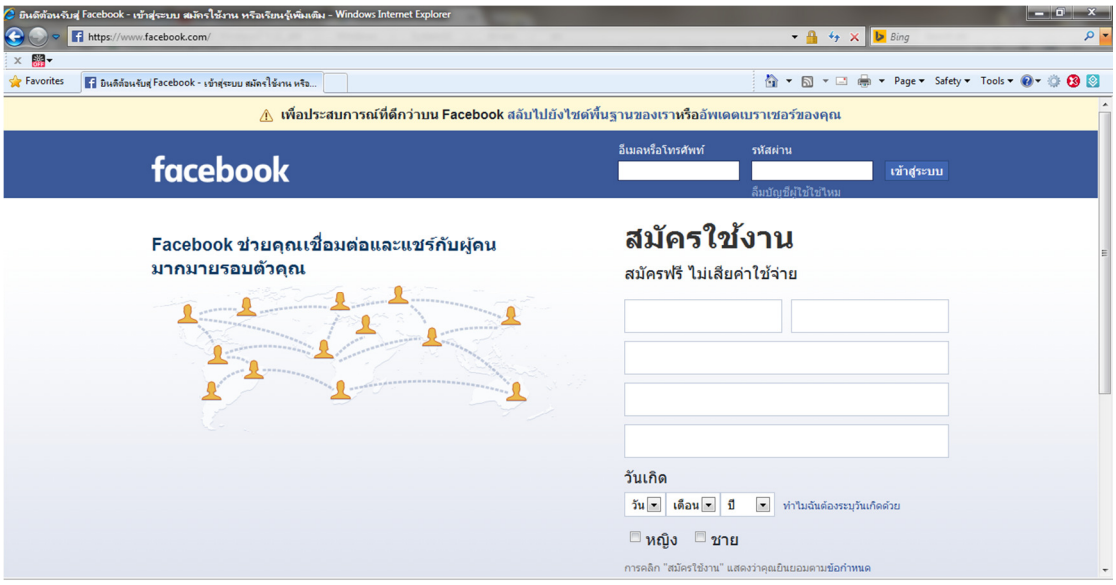
5.เปิดไฟล์ไวรัส จะทำให้ไม่สามารถเข้า www.facbook.com ไม่ได้



6.วิธีแก้ คือ ให้เข้าไปที่ c:\windows\system32\drivers\etc\hosts แล้วทำการลบไฟล์ในโฟลเดอร์ทิ้งให้หมด



7.หลังจากลบไฟล์ในโฟลเดอร์ทิ้งเรียบร้อย www.facebook.com ก็สามารถเข้าได้ตามปกติ



6. แผนและระยะดำเนินงาน

ระยะเวลาตั้งแต่เดือนกันยายน 2559 ถึง เดือนพฤศจิกายน 2559

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]. ไวรัสคอมพิวเตอร์. (ม.ป.ป.). ค้นเมื่อ 5 พฤศจิกายน 2559, จาก http://web.ku.ac.th/schoolnet/snet1/software/virus

[2]. ไวรัสคอมพิวเตอร์คืออะไร. (ม.ป.ป.). ค้นเมื่อ 5 พฤศจิกายน 2559, จาก http:// www.lampang.go.th/db_lap/virus.html