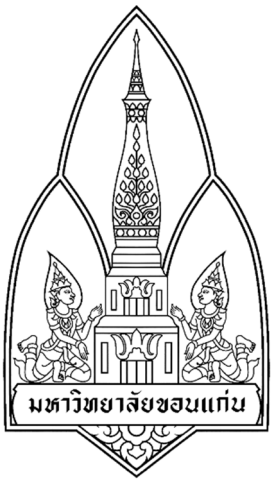


Security Tool Virus 123

รายวิชา:322 379 Information and Communication Technology Security

เสนอ ผศ.ดร.จักรชัย โสอินทร์

สมาชิกกลุ่ม 6

นาย พิชเญศ พกัตรหาญ 573020814-8

นางสาว ธันยพร เต็งตังลา 573020807-2

นางสาว ธนพร สาโคตร 573021396-5

นาย ยงศักดิ์ ไร่ไสว 573020819-8

นายวรรณกรณ์ นันท์แพง 573021408-4

นางสาว กัญญาพัชร ยอดกลาง 573020797-2

สาขาเทคโลยีสารสนเทศและการสื่อสาร (โครงการพิเศษ)

ภาควิชา วิทยาศาสตร์คอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

หลักการและเหตุผล

ปัจจุบันมีโปรแกรมที่สร้างแอนตี้ไวรัสมากมายแต่เรายังไม่ทราบว่าไวรัสสร้างอย่างไรมีความซับซ้อนอย่างไร ทำให้เกิดการศึกษาและค้นคว้าถึงวิธีและ รูปแบบที่แอบแฝงต่างๆของไวรัส ไวรัสตัวแรกที่เกิดขึ้นเป็นวิทยานิพนธ์ว่าด้วยความไม่ปลอดภัยของระบบคอมพิวเตอร์แล้วเกิดเหตุหลุดออกมาการมีไวรัสเป็น การสร้างภูมิคุ้มกันอย่างหนึ่งเป็นการเตือนให้รู้ถึงช่องโหว่ของระบบรักษาความปลอดภัยและทำให้เกิดการเรียนรู้ในความเสียหายที่เกิดขึ้น

วัตถุประสงค์

- เพื่อศึกษาวิธีการสร้างไวรัส
- เพื่อศึกษาช่องทางต่างๆที่เป็นตัวนำพาไวรัส
- เพื่อศึกษาหาแนวทางป้องกันและแก้ไขเมื่อพบเจอไวรัส

งานที่เกี่ยวข้อง

Virus# Cut Network/Internet

เป็น code virus อย่างง่ายๆโดยการเขียนไวรัสตัวนี้จะทำการตัดการทำงานของ Internetออก

```
@echo off

TITLE Mr_Unlocker

ipconfig /release
```

Virus# Combo Virus

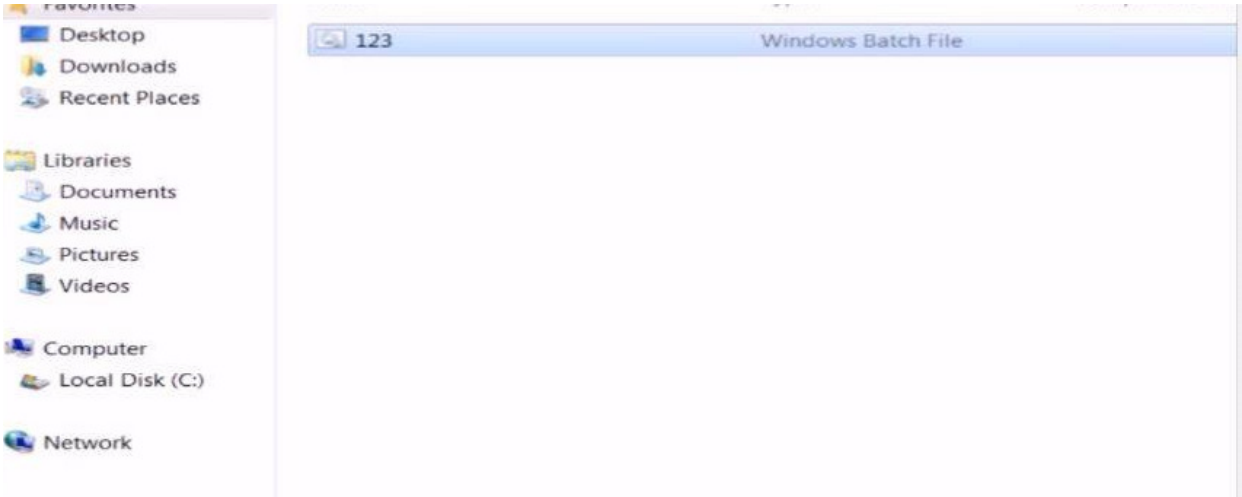
อธิบาย เป็นตัวต่อของไวรัสที่ทา การตัดการทา งานของ Internet ซึ่งเมื่อคลกิ ไฟล์ Auto Run จะทำการ flood network และทา การ loop จนกว่า Networkจะทำงาน ไม่ได้

```
@echo off TITLE Mr_Unlocker :CRASH net send * WORKGROUP ENABLED net send * WORKGROUP ENABLED GOTO CRASH
```

ภาพรวม

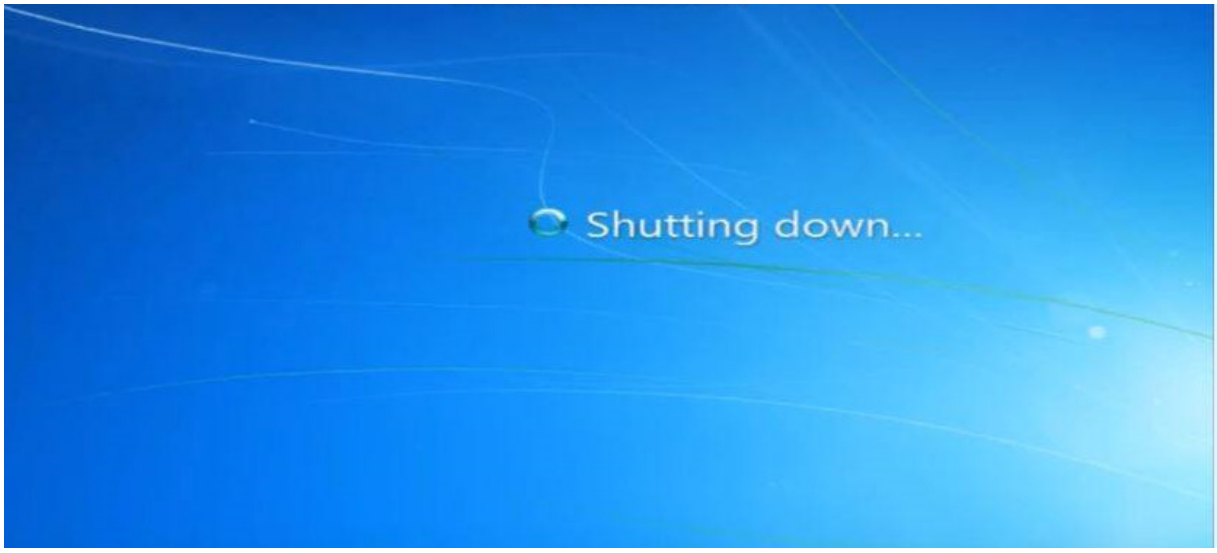
อธิบายทำงานของไวรัส

การสร้างไวรัส123 เราจะทำการเขียนไวรัสขึ้นมาด้วย textหรือNote pad ก็ได้ ตัวโค๊ดนี้จะเป็นโค๊ดที่ใช้ในการรันใน commandหรือ cmd เมื่อทำการเขียนไฟล์ไวรัสเสร็จ ในการวนลูปเราสามารถกำหนดระยะเวลาได้ว่า เมื่อคอมพิวเตอร์ทำการรีเครื่องใช้เวลาเท่าไหร่ถึงจะรีอีกรอบ ซึ่งผู้จัดทำได้ทำการตัดไว้ 3 วินาที



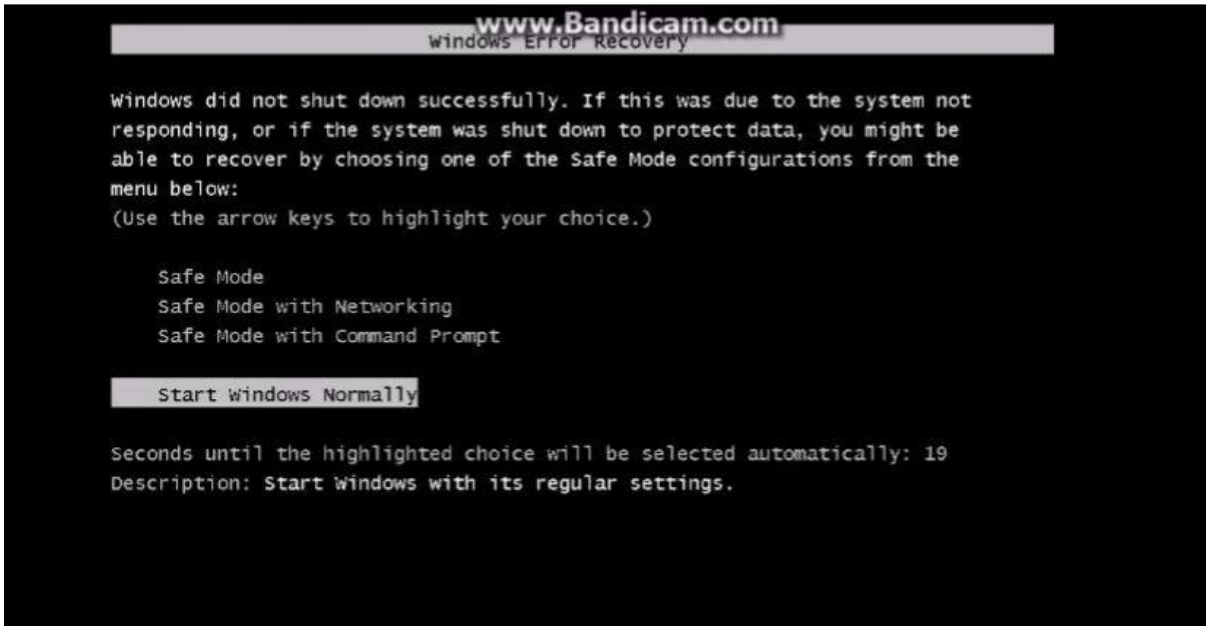
เราได้ทำการเซฟไฟล์ ชื่อไฟล์ว่า 123 นามสกุลไฟล์เป็น .bat เพื่อให้ทำการรันได้อัตโนมัติ

เมื่อทำการคลิ๊กไฟล์ก็จะปรากฏหน้าต่างมาสักครู่แล้วก็จะหายไปพร้อมเครื่องของเราที่เริ่มทำการรีสตาร์ทและจะทำการวนลูปซ้ำๆ

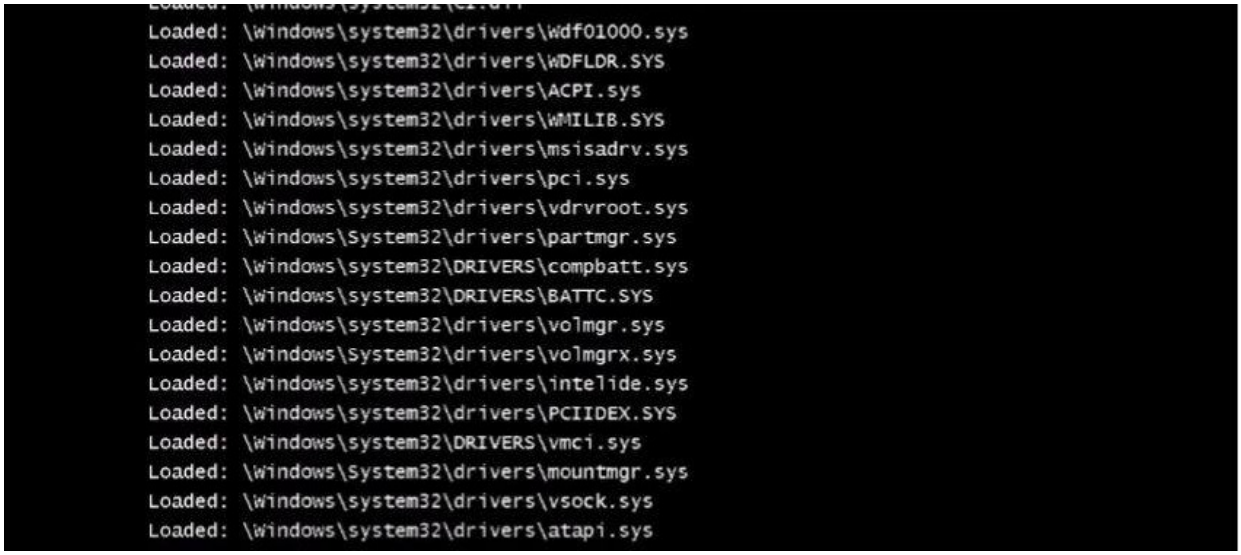


วิธีแก้ไขไวรัส

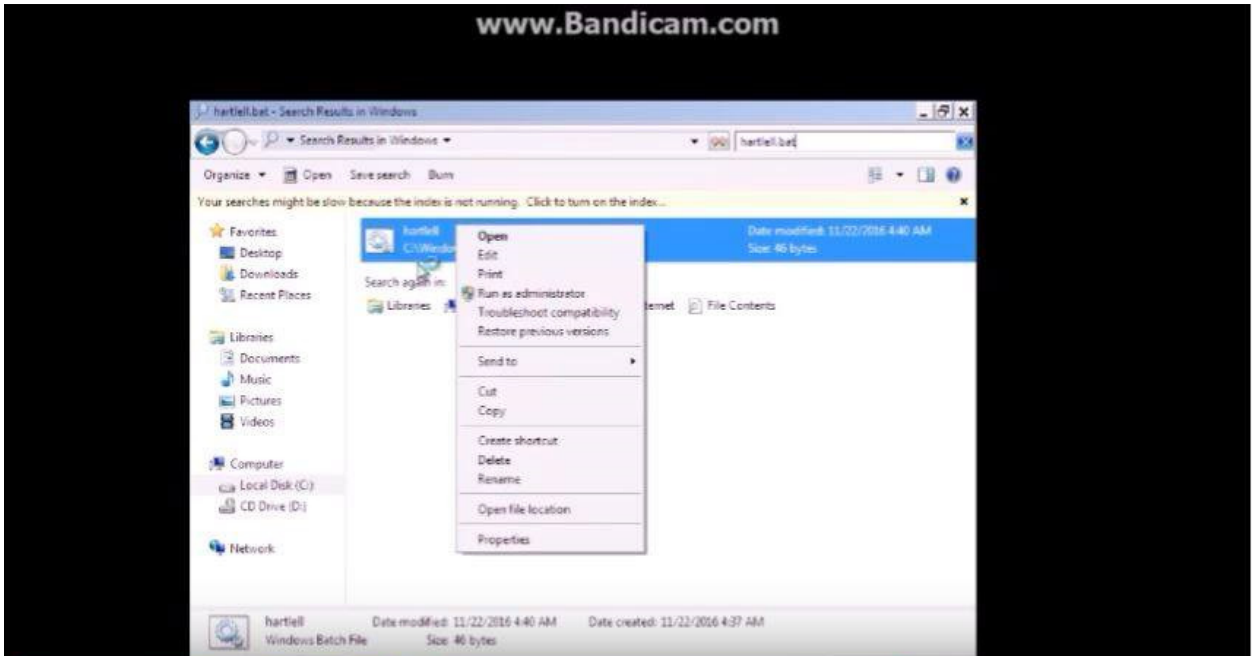
เมื่อเครื่องทำการรีอีกครั้งให้กดF2ย้ำๆหลายครั้ง



ให้ทำการเลือกเซฟโหมดเพื่อจะทำการนำไฟล์ไวรัสที่อยู่ภายในเครื่องออก

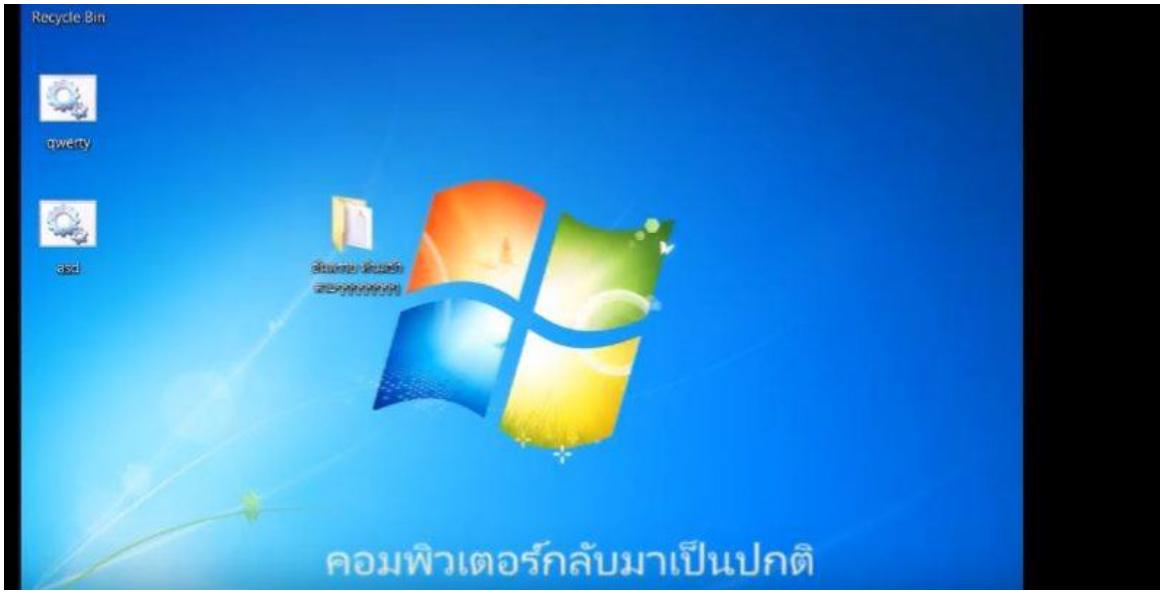


เมื่อเลือกเซฟโหมดจะปรากฏหน้าตาแบบนี้ขึ้นมา



เมื่อatเข้ามาวินโด่วเรียบร้อยแล้วให้ทำการเปิดดูไดร์ฟซีแล้วเข้าไปที่ Users และให้ทำการค้นหาไฟล์ hartlell.batเป็นไฟล์ที่ถูกฝั่งจากการรัน 123.batนั้นเอง ให้ทำการลบออกและลองรีสตาร์ท


Shutting down...
ให้ทำการRestartอีกรอบ


Recycle Bin
qwerty
asd
คอมพิวเตอร์กลับมาเป็นปกติ