Virus มีเพลิน

Information and Communication Technology Security

ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

เสนอ

รศ.ดร.จักรชัย โสอินทร์

ผู้จัดทำ

นายเฟรม พานิชพัฒน์	573020816-4
นางสาวชิดชนก เกษรสมบัติ	573021392-3
นางสาวนาราภัทร คำสวาท	573021415-7
นายธีรภัส นิลประไพ	573020808-3
นางสาวศิริรัตน์ แร่วงคต	573020826-1
นางสาวจิระภาพร จันทคีรีเขต	573021387-6
นางสาวชนันท์ภัคค์ ทวีชัยจุทานนท์	573020800-9
นางสาวประกายกาญจน์ วิทยาเรืองสิน	573020810-6

ภาคเรียนที่ 1 ปีการศึกษา 2559

ภาควิชาวิทยาการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศและการสื่อสาร

คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

หลักการและเหตุผล

เนื่องจากในปัจจุบันคอมพิวเตอร์เข้ามามีส่วนสำคัญในชีวิตประจำวันซึ่งมีโปรแกรมที่ช่วยในการจัดการงานต่างๆ มากมายซึ่งโปรแกรมเหล่านี้อาจมีค่าลิขสิทธิ์ที่แพง จึงทำให้ผู้ใช้งานจำนวนไม่น้อยหันมาโหลดโปรแกรมเถื่อน ที่ต้องทำการ Crack เพื่อให้สามารถเปิดใช้งานคุณสมบัติให้คล้ายกับโปรแกรมของแท้ได้ โปรแกรมเถื่อนเหล่านี้อาจมีผู้ที่ไม่หวังดีจะแฝงไวรัสเพื่อโจมตีคอมพิวเตอร์ผู้อื่นทำให้เกิดความเสียหายต่อเครื่องคอมพิวเตอร์และข้อมูลสำคัญภายในเครื่องได้

ดังนั้นผู้จัดทำจึงได้ศึกษาการสร้างไวรัส เพื่อโจมตีเครื่องคอมพิวเตอร์และหาวิธีการในการแก้ปัญหาเมื่อเครื่องคอมพิวเตอร์ติดไวรัส

วัตถุประสงค์

1. เพื่อทดสอบระบบความปลอดภัยของ Windows
2. เพื่อศึกษาการสร้างไวรัสที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์
3. เพื่อหาวิธีการในการแก้ปัญหา
4. เพื่อใช้ในรายวิชา 322376 Information And Communication Technology Security

งานที่เกี่ยวข้อง

1. ม้าโทรจัน (Trojan Horse)

เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็นโปรแกรมธรรมดาทั่วๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียนขึ้นมาทำงาน แต่เมื่อถูกเรียกขึ้นมาก็จะเริ่มทำลายตามที่โปรแกรมมาทันที ม้าโทรจันบางตัวถูกเขียนขึ้นมาใหม่ทั้งชุด โดยคนเขียนจะทำการตั้งชื่อโปรแกรมพร้อมชื่อรุ่นและคำอธิบาย การใช้งานที่ดูสมจริง เพื่อหลอกให้คนที่จะเรียกใช้ตายใจ

จุดประสงค์ของคนเขียนม้าโทรจันคือเข้าไปทำอันตรายต่อข้อมูลที่มีอยู่ในเครื่องหรืออาจมีจุดประสงค์เพื่อที่จะล้วงเอาความลับของระบบคอมพิวเตอร์ ม้าโทรจันถือว่าไม่ใช่ไวรัส เพราะเป็นโปรแกรมที่ถูกเขียนขึ้นมาโดดๆ และจะไม่มีการเข้าไปติดในโปรแกรมอื่นเพื่อสำเนาตัวเอง แต่จะใช้ความรู้เท่าไม่ถึงการณ์ของผู้ใช้ เป็นตัวแพร่ระบาดซอฟต์แวร์ที่มี ม้าโทรจันอยู่ในนั้นและนับว่าเป็นหนึ่งในประเภทของโปรแกรมที่มีความอันตรายสูง เพราะยากที่จะตรวจสอบและ สร้างขึ้นมาได้ง่าย ซึ่งอาจใช้แค่แบต์ไฟล์ก็สามารถโปรแกรมม้าโทรจันได้

อ้างอิง : *https://smil3nr6868.wordpress.com/2012/07/07*

อ้างอิง : *http://www.internetdict.com/wp-content/uploads/related_images/2016/01/20/what-is-the-trojan-horse-virus_1.jpg*

2. **W32.MSN.Worm**

ประเภท Worm ลักษณะที่หนอนใช้ส่งจะประกอบไปด้วยข้อความต่างๆ แล้วตามด้วยไฟล์ Image.zip และสามารถแพร่กระจายผ่านทางโปรแกรมสนทนา MSN Messenger

ผลเสียที่เกิด

1) เครื่องอาจทำงานผิดพลาด : เนื่องจากหนอนชนิดนี้ทำการแก้ไขค่าในรีจิสทรี สร้างไฟล์ขึ้นมา รวมทั้งมีการยุติการทำงานบางเซอร์วิสของระบบปฏิบัติการด้วย
2) เปิดการเชื่อมต่อที่ผิดปกติ : หนอนชนิดนี้จะส่งไฟล์ของหนอนไปยังบัญชีรายชื่ออื่นๆ ที่อยู่ในลิสต์ของโปรแกรมสนทนา MSN Messenger

วิธีป้องกัน

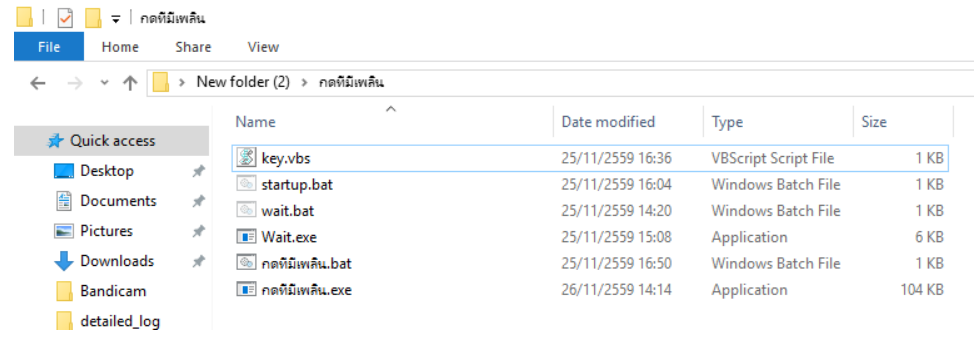
1) ห้ามรับหรือรันไฟล์ที่ถูกส่งด้วยโปรแกรมสนทนา (Chat) ต่างๆ เช่น MSN, Yahoo, IRC, ICQ หรือ Pirch เป็นต้น จากบุคคลที่ไม่รู้จักหรือไม่มั่นใจว่าผู้ส่งเป็นใครและไม่ทราบว่าไฟล์ดังกล่าวนั้นเป็นไฟล์อะไร
2) สร้างแผ่นกู้ระบบฉุกเฉิน (Emergency disk) ของโปรแกรมป้องกันไวรัส และปรับปรุงฐานข้อมูลในแผ่นอยู่เสมอ ติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) ของทุกซอฟต์แวร์อยู่เสมอ โดยเฉพาะ Internet Explorer และระบบปฏิบัติการ ให้เป็นเวอร์ชันใหม่ที่สุด
3) ติดตั้งโปรแกรมป้องกันไวรัส และต้องทำการปรับปรุงฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ

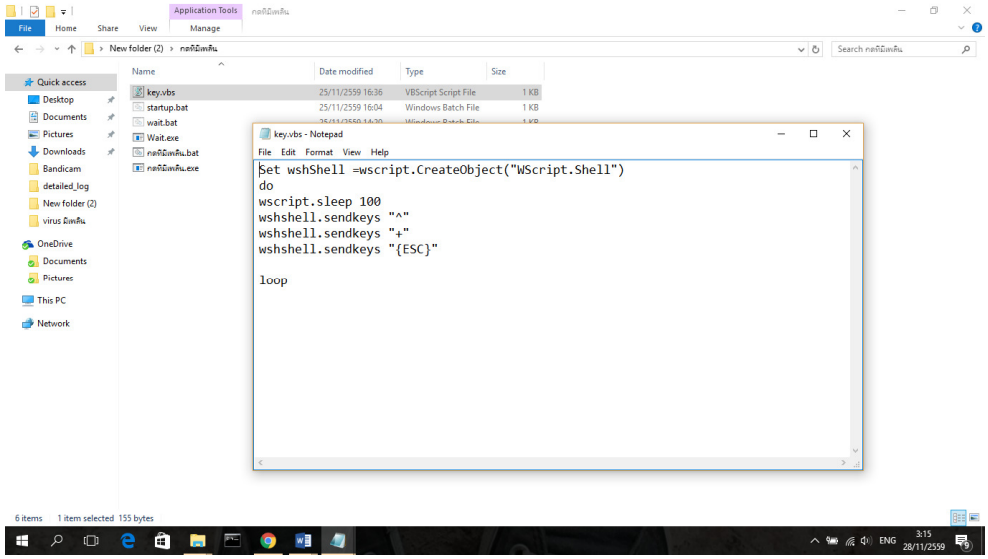
อ้างอิง : *https://smil3nr6868.wordpress.com/2012/07/07/*

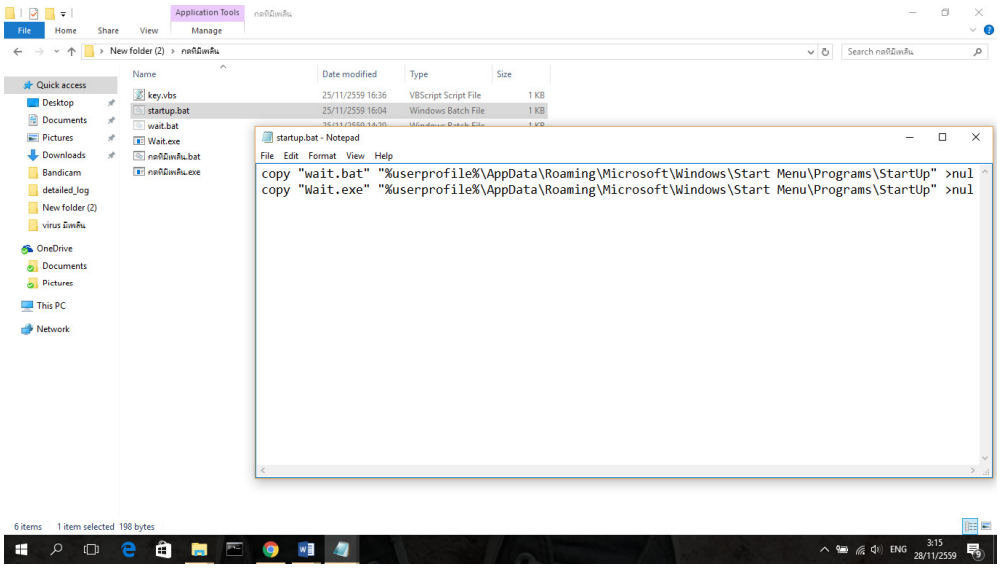
อ้างอิง : *http://www.comnetsite.com/images/pv-tip30_msnworm.gif*

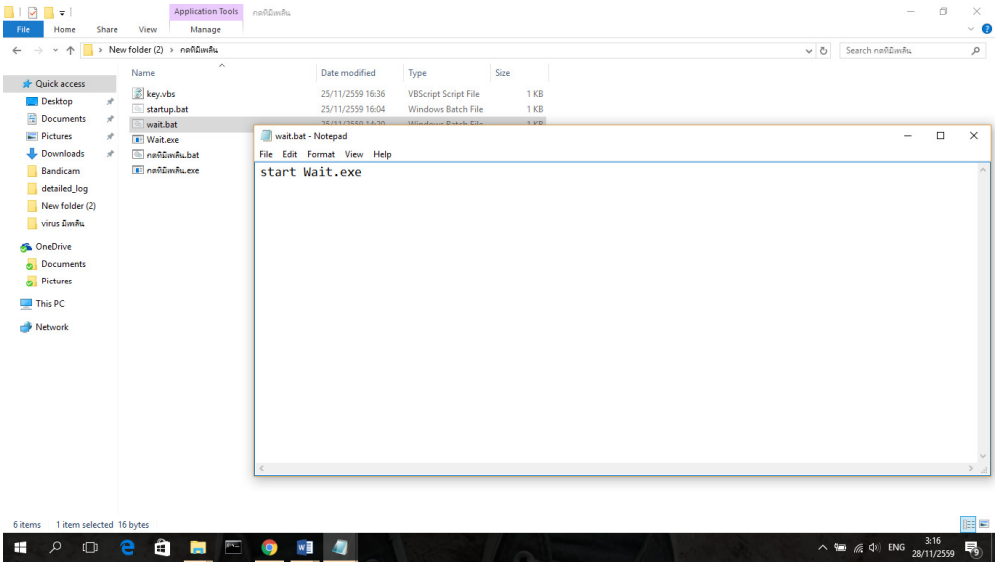
ขั้นตอนวิธีการ

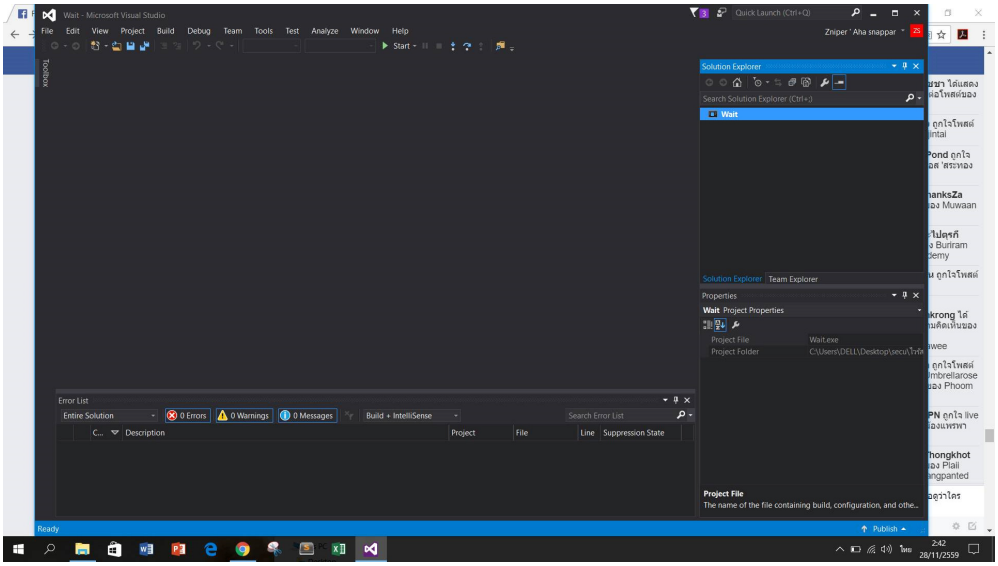
1. เตรียมโปรแกรมที่ใช้ในการเขียนไวรัส ในที่นี้ใช้โปรแกรม Visual Studio 2015, Notepad ซึ่งในแต่ละไฟล์จะมีคำสั่งที่ใช้ในการโจมตีเครื่องคอมพิวเตอร์

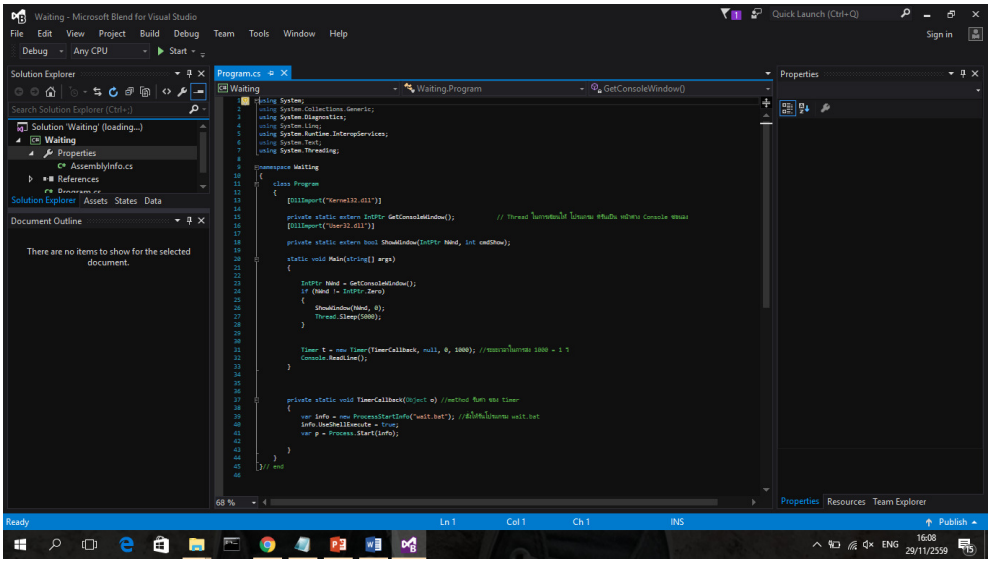


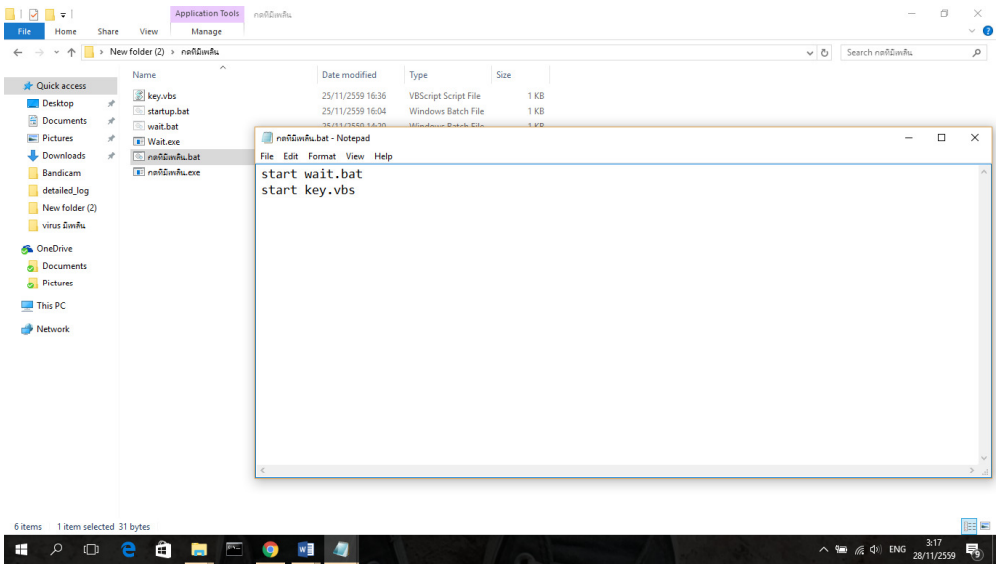





wait.bat - Notepad
File Edit Format View Help
start Wait.exe

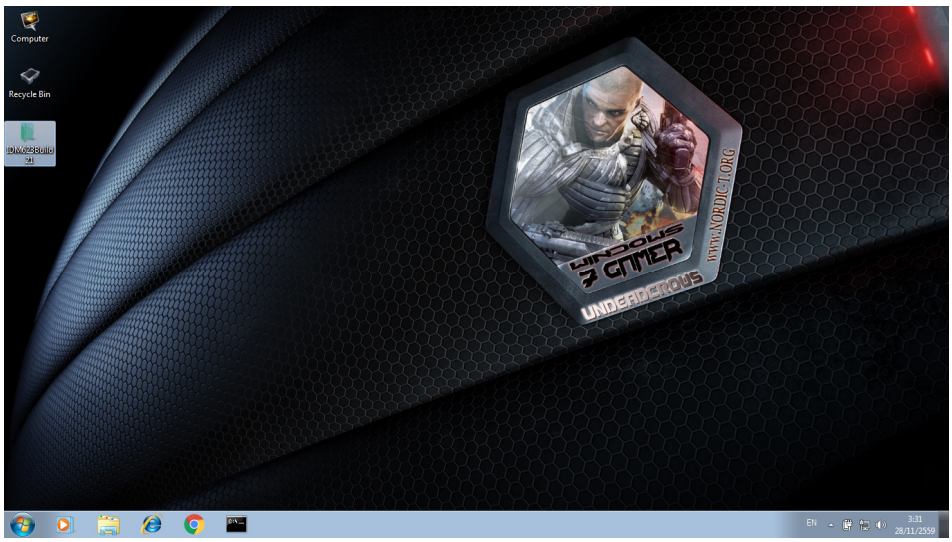


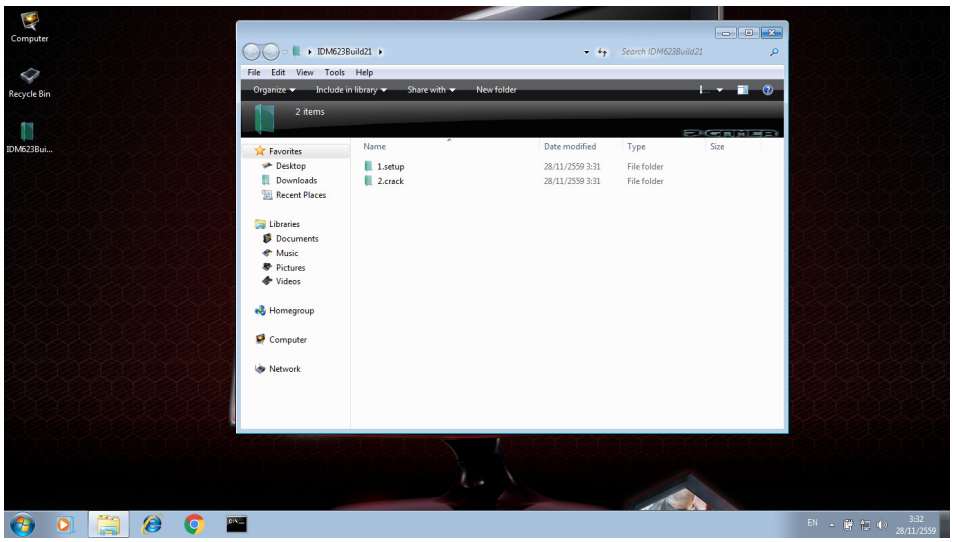




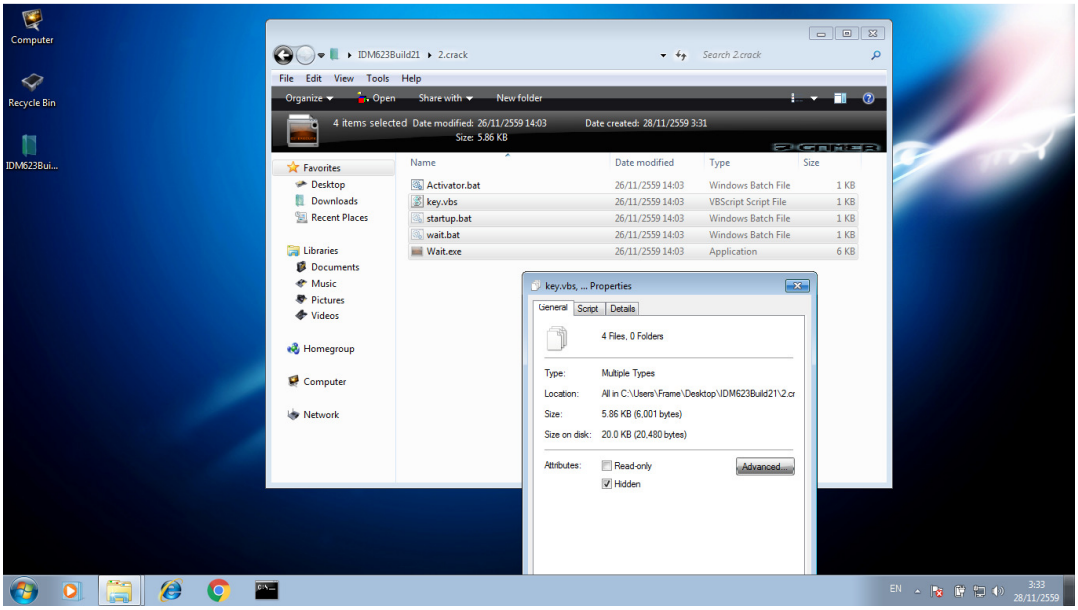
2. ขั้นตอนการโจมตี

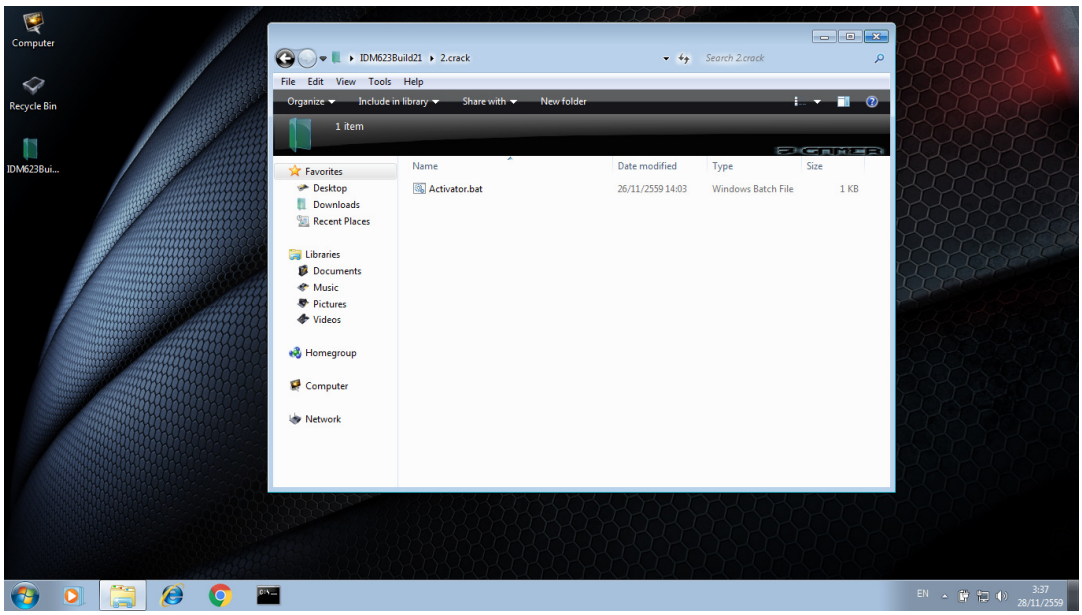
2.1 นำไวรัสแฝงไปกับโปรแกรม ในที่นี้ใช้โปรแกรม IDM ในการแฝงไปกับตัว Activator



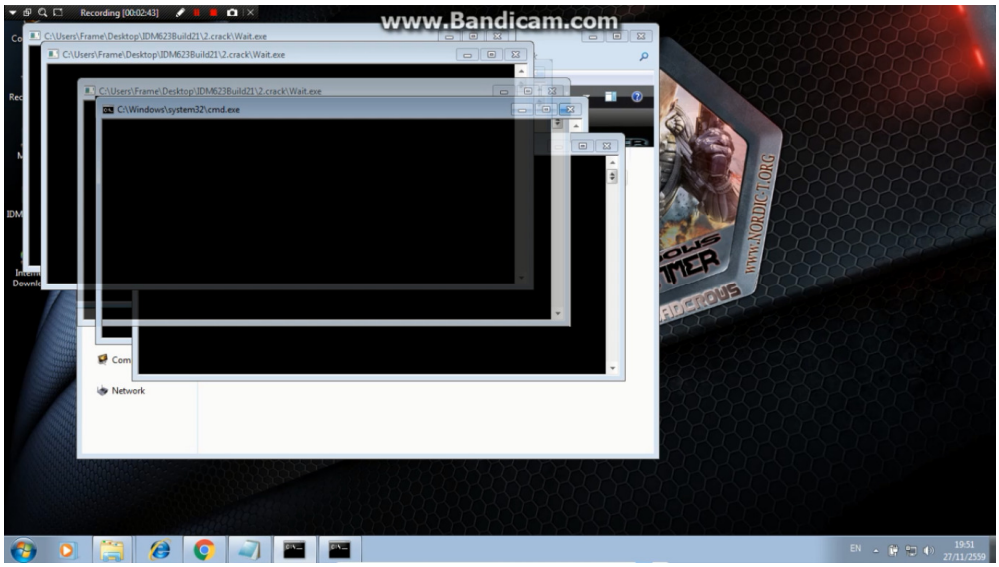


2.2 ทำการซ่อนไฟล์ให้เหลือเพียงไฟล์ Activator.bat ซึ่งทำการเปลี่ยนชื่อเรียบร้อยแล้ว



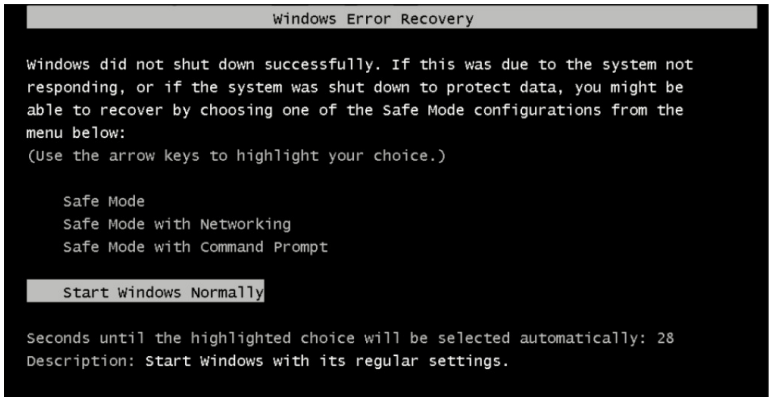


2.3 เมื่อเหยื่อทำการทำการติดตั้งโปรแกรมและทำการคลิ้กที่ Activator ไวรัสจะเริ่มทำงาน ส่งผลให้เครื่องค้างและคีบอร์ดรวน

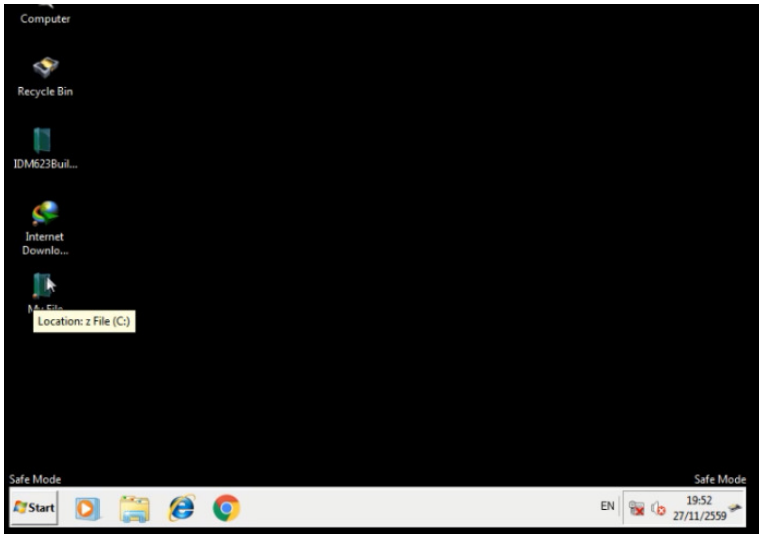


3. การแก้ไขหลังจากไวรัสทำงาน

3.1 ให้ทำการปิดเครื่องทันทีโดยกดที่ปุ่มเพาเวอร์ค้างไว้จนดับจากนั้นเปิดเครื่องเพื่อเข้าสู่เซฟโหมด



3.2 เมื่อเข้าสู่เซฟโหมดแล้วให้ทำการเข้าไปลบโปรแกรมและไวรัสที่ส่งผลอันตรายต่อเครื่องคอมพิวเตอร์



3.3 ทำการเปิดเครื่องขึ้นมาใหม่แล้วทำการรีสตาร์ทเครื่อง 1 ครั้ง

การป้องกันและหลีกเลี่ยงไวรัส

1) เครื่องคอมพิวเตอร์ควรติดตั้งโปรแกรมแอนตี้ไวรัสที่มีการอัพเดทฐานข้อมูลไวรัสเสมอ
2) ไม่ควรดาวน์โหลดโปรแกรมเถื่อนจากเว็บไซต์ต่างๆเพราะอาจจะมีไวรัสติดมาพร้อมกับโปรแกรม
3) ควรใช้โปรแกรมฟรีจากทางเว็บไซต์ผู้ผลิตเพื่อหลีกเลี่ยงการใช้โปรแกรมเถื่อนที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์
4) อย่าตั้งค่าให้โปรแกรมอีเมลเปิดไฟล์ที่แนบมาโดยอัตโนมัติ ควรจะต้องตรวจสอบก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา
5) สแกนไฟล์แนบท้ายของอีเมลทุกฉบับ หรือแม้แต่อีเมลจากคนรู้จัก
6) ตั้งค่าระบบป้องกันให้ทำงานทันทีที่เริ่มเปิดคอมพิวเตอร์ใช้งาน
7) ควรสแกนแฟลชไดรฟ์ก่อนใช้งานทุกครั้ง เพราะแฟลชไดรฟ์เป็นพาหะในการนำข้อมูลจากพีซีเครื่องหนึ่งมาใส่ในอีกเครื่อง