คำนำ

ปัญหาเรื่องเครื่องคอมพิวเตอร์ติดไวรัสและสปายแวร์ เป็นปัญหาที่สำคัญอย่างยิ่งต่อการทำงาน อาจทำให้เกิดความเสียหายต่อข้อมูล หรือโปรแกรม การจัดการความรู้เรื่องการเตือนภัยไวรัสคอมพิวเตอร์แก่ผู้ใช้งาน จึงเป็นสิ่งที่จำเป็นและเป็นประโยชน์อย่างยิ่งต่อหน่วยงาน ศูนย์สารสนเทศ กรมวิชาการเกษตร จึงจัดทำคู่มือเล่มนี้ขึ้น เพื่อใช้เป็นแนวทางป้องกันและแก้ไขปัญหาการติดไวรัสคอมพิวเตอร์และสปายแวร์

คณะกรรมการจัดการความรู้
ศูนย์สารสนเทศ กรมวิชาการเกษตร

สารบัญ

บทนำ

ระยะเวลาที่ผ่านมา ไวรัสคอมพิวเตอร์ได้สร้างความเสียหายแก่ระบบคอมพิวเตอร์ทั่วโลกเป็นอย่างมาก เป้าหมายการสร้างความเสียหายที่เกิดจากไวรัสคอมพิวเตอร์ชนิดใหม่ๆ ในปัจจุบันได้ส่งผลกระทบต่อสังคมและเศรษฐกิจในทุกๆ ด้าน การพัฒนาการของไวรัสโดยเทคนิคแบบใหม่ และแนวคิดในการเขียนโปรแกรมมีแนวโน้มที่จะสร้างความเสียหายในวงกว้างมากขึ้น การจัดการความรู้เรื่องไวรัสคอมพิวเตอร์จึงเป็นสิ่งจำเป็นและมีประโยชน์อย่างยิ่งต่อผู้ใช้คอมพิวเตอร์ในองค์การ เพื่อใช้เป็นแนวทางการป้องกันและแก้ไขปัญหาการติดไวรัสคอมพิวเตอร์

ประวัติความเป็นมาของไวรัสคอมพิวเตอร์

โปรแกรมที่สามารถสำเนาตัวเองได้เกิดขึ้นเป็นครั้งแรกในปี พ.ศ. 2526 โดย ดร.เฟรดเดอริก โคเฮน นักวิจัยของมหาวิทยาลัยเพนซิลวาเนีย สหรัฐอเมริกา ได้ศึกษาโปรแกรมลักษณะนี้และได้ตั้งชื่อว่า "ไวรัส" แต่ไวรัสที่แพร่ระบาดและสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ตามที่มีการบันทึกไว้ครั้งแรกเมื่อปี พ.ศ. 2529 ด้วยผลงานของไวรัสที่ชื่อ "เบรน (Brain)" ซึ่งเขียนขึ้นโดยโปรแกรมเมอร์สองพี่น้องชาวปากีสถานชื่อ อัมจาด (Amjad) และเบซิท (Basit) เพื่อป้องกันการคัดลอกทำสำเนาโปรแกรมของพวกเขาโดยไม่จ่ายเงิน

ไวรัสคอมพิวเตอร์ในยุคแรกๆ ระบาดโดยการละเมิดทำสำเนาซอฟท์แวร์ลิขสิทธิ์ที่มีโปรแกรมไวรัสคอมพิวเตอร์ติดอยู่ด้วยการใช้แผ่นดิสต์เก็ตหรือซีดีรอม แต่ในปัจจุบันเนื่องจากการเติบโตของเครือข่ายคอมพิวเตอร์ทำให้ไวรัสยุคหลังๆ มีความสามารถในการทำสำเนาคัดลอกและแพร่กระจายตัวเองได้มากขึ้น รวมทั้งมีความรุนแรงมากกว่าเดิมซึ่งในปัจจุบันนี้พบว่ามีมากกว่า 40,000 ชนิด และยังเกิดเพิ่มขึ้นอีกอยู่ทุกๆ วัน อย่างน้อยวันละ 4-6 ชนิด

ความหมายของไวรัสคอมพิวเตอร์

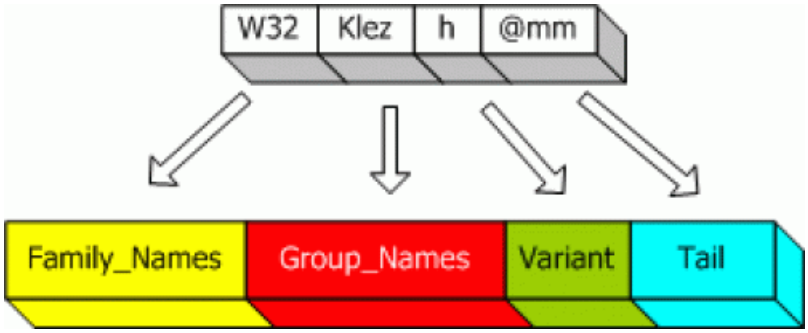
ไวรัสคอมพิวเตอร์ คือ โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเอง โดยมีลักษณะเลียนแบบสิ่งมีชีวิต คือ เจริญเติบโตเองได้ ขยายและแพร่กระจายตัวเองได้ สามารถอยู่รอดได้ด้วยการอำพรางตน เหมือนกับไวรัสที่เป็นเชื้อโรคร้ายทำลายสิ่งมีชีวิตทั้งหลายนั่นเอง

ไวรัสคอมพิวเตอร์ สามารถสำเนาตัวเองให้แพร่กระจายไปยังไฟล์ในระบบคอมพิวเตอร์จากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ผ่านตัวกลางที่เป็นพาหะ เช่น การสำเนาไฟล์ด้วยแผ่นดิสค์เก็ตระหว่างเครื่อง การสำเนาข้อมูลผ่านระบบเครือข่ายหรือระบบสื่อสาร

การที่คอมพิวเตอร์เครื่องใดติดไวรัส หมายความว่า ไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสเป็นโปรแกรมชนิดหนึ่ง การที่จะเข้าไปอยู่ในหน่วยความจำได้จะต้องมีการถูกเรียกใช้งานหรือถูกกระตุ้นให้ทำงาน (ขึ้นอยู่กับประเภทของไวรัสชนิดนั้นๆ) ซึ่งโดยปกติผู้ใช้เครื่องมักไม่รู้ตัวว่าได้ปลุกไวรัสคอมพิวเตอร์ให้ขึ้นมาทำงานแล้ว

การทำงานของไวรัส

การทำงานของไวรัสแต่ละตัวขึ้นอยู่กับวัตถุประสงค์ของผู้เขียนโปรแกรมนั้นขึ้นมา เช่น ทำลายระบบปฏิบัติการ โปรแกรมใช้งานหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือรบกวนการทำงาน เช่น การบู๊ตระบบช้าลง เรียกใช้โปรแกรมได้ไม่สมบูรณ์ หรือเกิดอาการค้าง (แฮงค์ไม่ทราบสาเหตุ) เกิดข้อความวิ่งไปมาที่หน้าจอ หรือกรอบข้อความเตือนไม่ทราบสาเหตุ เป็นต้น ส่วนประกอบของชื่อไวรัสนั้นแบ่งได้เป็นส่วนๆ ดังภาพที่ 1



ภาพที่ 1 ส่วนประกอบต่างๆ ของชื่อไวรัส

1. ส่วนแรกแสดงชื่อตระกูลของไวรัส (Family_Names) ส่วนใหญ่จะตั้งตามชนิดของปัญหาที่ไวรัสก่อขึ้น หรือภาษาที่ใช้ในการพัฒนา เช่น เป็นม้าโทรจัน ถูกพัฒนาด้วย Visual Basics Script หรือเป็นไวรัสที่รันบนระบบปฏิบัติการวินโดวส์ 32 บิต เป็นต้น ซึ่งชื่อของตระกูลของไวรัสที่ค้นพบในปัจจุบันดังตารางที่ 1

ตารางที่ 1 รายชื่อตระกูลของไวรัส

Family Names	ความหมาย
WM	ไวรัสที่เป็นมาโครของโปรแกรม Word
W97M	ไวรัสที่เป็นมาโครของโปรแกรม Word 97
XM	ไวรัสที่เป็นมาโครของโปรแกรม Excel
X97M	ไวรัสที่เป็นมาโครของโปรแกรม Excel 97
W95	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 95
W32/Win32	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 32 บิต
WNT	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ NT 32 บิต
I-Worm/Worm	หนอนอินเทอร์เน็ต
Trojan/Troj	ม้าโทรจัน
VBS	ไวรัสที่ถูกพัฒนาด้วย Visual Basic Script
AOL	ม้าโทรจัน America Online
PWSTEAL	ม้าโทรจันที่มีความสามารถในการขโมยรหัสผ่าน
Java	ไวรัสที่ถูกพัฒนาด้วยภาษาจาวา
Linux	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์
Palm	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการ Palm OS
Backdoor	เปิดช่องให้ผู้บุกรุกเข้าถึงเครื่องได้
HILLW	บ่งบอกว่าไวรัสถูกคอมไพล์ด้วยภาษาระดับสูง

2. ส่วนชื่อของไวรัส (Group_Name) เป็นชื่อดั้งเดิมที่ผู้เขียนไวรัสเป็นคนตั้ง โดยปกติจะถูกแทรกไว้อยู่ในโค้ดของไวรัส และในส่วนนี้เองจะใช้เรียกชื่อไวรัสเปรียบเสมือนเรียกชื่อเล่น ตัวอย่างเช่น ชื่อของไวรัสคือ W32.Klez.h@mm ถูกเรียกว่า Klez.h เพื่อให้สั้นและกระชับขึ้น

3. ส่วนของ Variant รายละเอียดส่วนนี้จะบอกว่าสายพันธุ์ของไวรัสชนิดนั้นๆ มีการปรับปรุงสายพันธุ์จนมีความสามารถต่างจากสายพันธุ์เดิมที่มีอยู่ variant มี 2 ลักษณะคือ

- Major_Variants จะตามหลังส่วนชื่อของไวรัส เพื่อบ่งบอกว่ามีความแตกต่างกันอย่างชัดเจน เช่น หนอนชื่อ VBS.LoveLetter.A (A เป็น Major_Variant) แตกต่างจาก VBS.LoveLetter อย่างชัดเจน

- Minor_Variants ใช้บ่งบอกในกรณีที่แตกต่างกันเล็กน้อย ในบางครั้ง Minor_Variant เป็นตัวเลขที่บอกขนาดไฟล์ของไวรัส ตัวอย่างเช่น W32.Funlove.4099 หนอนชนิดนี้มีขนาด 4099 KB.

4. ส่วนท้าย (Tail) เป็นส่วนที่จะบอกว่าวิธีการแพร่กระจาย ประกอบด้วย

- @M หรือ @m บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "mailer" ที่จะส่งตัวเองผ่านทางอี-เมล์เมื่อผู้ใช้ส่งอี-เมล์เท่านั้น

- @MM หรือ @mm บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "mass-mailer" ที่จะส่งตัวเองผ่านทุกอี-เมล์แอดเดรสที่อยู่ในเมล์บอกซ์

ตัวอย่าง W32.HILLW.Lovgate.C@mm แสดงว่าอยู่ในตระกูลที่มีผลกระทบต่อระบบปฏิบัติการวินโดวส์ 32 บิต และถูกคอมไพล์ด้วยภาษาระดับสูง

- ชื่อของไวรัสคือ Lovgate

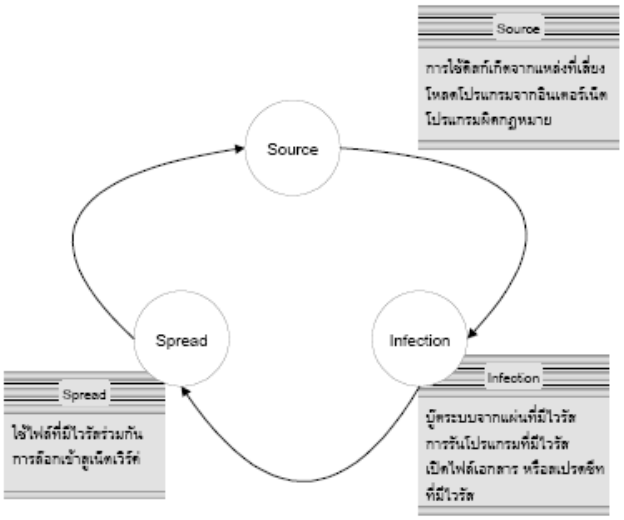
- มี variant คือ C

- มีความสามารถในการแพร่กระจายผ่านทางอี-เมล์โดยส่งไปยังทุกอี-เมล์แอดเดรสที่อยู่ในเมล์บอกซ์

จากส่วนประกอบของชื่อไวรัสที่ได้อธิบายไว้ข้างต้น จะเห็นได้ว่าชื่อของไวรัสนั้นสามารถบอกถึงประเภทของไวรัส ชื่อดั้งเดิมของไวรัสที่ผู้เขียนไวรัสเป็นคนตั้ง สายพันธุ์ต่างๆ ของไวรัสที่ถูกพัฒนาต่อไป และวิธีการแพร่กระจายตัวของไวรัสเองด้วย

วงจรชีวิตของไวรัสคอมพิวเตอร์

การทำงานของไวรัสคอมพิวเตอร์ มีรูปแบบเฉพาะที่แตกต่างจากโปรแกรมทั่วไป ซึ่งลักษณะหรือพฤติกรรมที่แสดงออกนั้นทำให้สามารถศึกษาถึงวงจรชีวิตและการทำงานในแต่ละช่วง โดยแบ่งออกได้เป็น 3 ช่วง คือ แหล่งที่มาของไวรัส (source) ช่วงการติดเชื้อ (infection) และช่วงการแพร่กระจาย (spead) ดังภาพที่ 2



ภาพที่ 2 วงจรชีวิตของไวรัสคอมพิวเตอร์

เทคโนโลยีของไวรัสคอมพิวเตอร์

เทคนิคต่างๆ ถูกนำมาใช้ในการพัฒนาขีดความสามารถของไวรัสเพื่อให้สามารถหลบหลีกการตรวจสอบและการค้นหา โดยเทคนิคเหล่านี้มีการเปลี่ยนแปลงไปในทางที่ซับซ้อนมากขึ้นตามประเภทการทำลาย

Stealth เป็นเทคนิคที่ออกแบบให้โปรแกรมสามารถป้องกันตัวเองจากการค้นหา หรือกำจัดได้ โดยทั่วไปจะใช้วิธีขัดขวาง (Interrupt) การทำงานของกระบวนการอ่านของระบบดิสก์ โดยเมื่อไฟล์ที่ไม่มีไวรัสถูกอ่านขึ้นมามันจะถูกแทรกรหัสของไวรัสเข้าไป (Read stealth Virus) นอกจากนั้นไวรัสที่เปลี่ยนแปลงขนาดของไฟล์ข้อมูล ไดเรคทอรี่ของข้อมูล (Size stealth Virus) เมื่อไวรัสจะแทรกรหัสระหว่างการอ่านข้อมูล เช่น ไวรัสมีขนาดข้อมูล 1,024 ไบต์ และไฟล์ข้อมูลเดิมมีขนาด 4,096 ไบต์ ขนาดของไฟล์จะเป็น (1,024 + 4,096) 5,120 ไบต์ ซึ่งขนาดของไฟล์ที่เปลี่ยนแปลงนั้นถูกตรวจพบได้ ไวรัสจะขัดขวางการทำงานของระบบไดเรคทอรี่ โดยอ่านค่าขนาดไฟล์ที่เป็น 5,120 ไบต์ขึ้นมา และลบออกด้วยขนาดของตัวเอง และจะส่งผลที่ได้ไปยังระบบเพื่อแสดงผลอีกครั้ง

Polymorphic อาศัยการเปลี่ยนแปลงรูปแบบของไวรัส มีการแบ่งรหัสของตัวไวรัสเป็นส่วนย่อยแทรกอยู่ระหว่างแฟ้มข้อมูล เมื่อแฟ้มข้อมูลทำงาน รหัสไวรัสจะถูกนำไปรวมกันในหน่วยความจำ การใช้การเข้ารหัสและการถอดรหัสก่อนการทำงานของคีย์เฉพาะ ทำให้ยากต่อการตรวจสอบรหัสจากลายเซ็นต์ไวรัส (Virus Signature) ซึ่งเป็นรหัสเฉพาะของไวรัสที่ผู้เขียนโปรแกรมป้องกันไวรัสได้ถอดรหัสออกมา ซึ่งไวรัสแต่ละตัวก็จะมีรูปแบบของข้อมูลที่แตกต่างกันโดยพื้นฐานของไวรัสประเภทนี้มาจากโครงสร้างของ TPE (Trident Polymophic Engine) และ MtE (Mutation Engine) ซึ่งมีรายงานการค้นพบในยุโรปช่วงปี พ.ศ. 2535

Multipartite การทำงานหลากรูปแบบในตัวเอง สามารถแพร่กระจายทางไฟล์ปกติ สามารถแพร่กระจายในส่วนของ Boot Record ของระบบดิสก์ได้ เมื่อไฟล์ข้อมูลเอกสารที่ติดไวรัส

ประเภทนี้ ถูกอ่านขึ้นมาทำงาน ไวรัสก็จะทำงานโดยการคัดลอกตัวเองเข้าไปบันทึกหรือเขียนทับข้อมูลในส่วนของระบบ Boot Record เมื่อมีการบูตครั้งต่อไป ไฟล์ทุกไฟล์ที่ถูกเรียกใช้งานก็จะติดไวรัส

Companion Virus เทคนิคนี้ถูกคิดค้นขึ้นมาโดยอาศัยช่องว่างในการทำงานของระบบปฏิบัติการ และการทำงานตามเงื่อนไขที่ถูกต้องของระบบปฏิบัติการในการทำลายระบบและแพร่กระจาย การทำตัวเสมือนหนึ่งเป็นโปรแกรมปกติของระบบถูกนำมาใช้ โดยอาศัยหลักในการรันโปรแกรมแบบลำดับ ถ้าชื่อไฟล์เหมือนกัน ไฟล์นามสกุลที่เป็น .Com จะทำงานก่อนไฟล์ที่มีนามสกุลเป็น .EXE เสมอ เมื่อไฟล์ CHKDSK.COM ซึ่งเป็นโปรแกรมไวรัส เมื่อเราเรียกไฟล์ CHKDSK มาทำงานในครั้งต่อไปไฟล์ CHKDSK.COM เป็นไวรัสจะทำงานก่อน

Malicious Program เป็นเทคนิคที่เกิดขึ้นในช่วงหลังๆ จากที่มีการใช้โปรแกรมจาวา และ Active X ซึ่งเป็นภาษาที่นิยมใช้กับอินเตอร์เน็ต โดยอาศัยช่องว่างของการรักษาความปลอดภัยภายในโปรแกรม บราวเซอร์และอี-เมล์ โปรแกรมที่ใช้การสื่อสารพูดคุยผ่านเน็ตเวิร์ค โดยไวรัสจะเข้าควบคุมระบบจากระยะไกล หรือการขโมยข้อมูลรหัสผ่านเข้าสู่ระบบจากเครื่องเป้าหมายและส่งคืนไปยังผู้ที่เข้าโจมตีระบบ ลักษณะเหล่านี้มักจะเป็นโปรแกรมประเภทหลุมพราง (Trojan Horse) เป้าหมายไม่ได้เน้นการทำลายไฟล์หรือข้อมูล แต่มีจุดประสงค์ในการเข้ายึดครองระบบ

ประเภทของไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์แบ่งเป็น 5 ประเภท ได้แก่

1. บูตเซ็กเตอร์ไวรัส (Boot Sector Virus) คือ ไวรัสคอมพิวเตอร์ที่แพร่เข้าสู่เป้าหมายในระหว่างเริ่มทำการบูตเครื่อง ส่วนมากจะติดต่อเข้าสู่แผ่นดิสก์เก็ตระหว่างกำลังสั่งปิดเครื่อง เมื่อนำแผ่นที่ติดไวรัสนี้ไปใช้กับเครื่องคอมพิวเตอร์เครื่องอื่นๆ ไวรัสก็จะเข้าสู่เครื่องคอมพิวเตอร์ตอนเริ่มทำงานทันที บูตไวรัสเซ็กเตอร์ จะติดต่อเข้าไปอยู่ส่วนหัวสุดของฮาร์ดดิสก์ ที่มาสเตอร์บูตเรคคอร์ด (master boot record) และจะโหลดตัวเองเข้าไปสู่หน่วยความจำก่อนที่ระบบปฏิบัติการจะเริ่มทำงาน ทำให้เหมือนไม่มีอะไรเกิดขึ้น

2. ไฟล์ไวรัส (file virus) เป็นไวรัสที่ใหญ่ที่สุด โดยไวรัสประเภทนี้จะซ่อนตัวเองไปกับไฟล์ เช่น โปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ต นามสกุล .exe, .com, .sys, .dll และโปรแกรมประเภทแชร์แวร์ เป็นต้น

3. มาโครไวรัส (macro virus) เป็นไวรัสที่ก่อกวนโปรแกรมสำนักงานต่างๆ เช่น MS-Word, Excel, Powerpoint ซึ่งจะใช้ลักษณะพิเศษของโปรแกรมที่มีการเขียนโปรแกรมด้วยมาโครเป็นชุดคำสั่งเล็กๆ ทำงานอัตโนมัติ มักจะทำให้ไฟล์มีขนาดใหญ่ขึ้นผิดปกติ การทำงานหยุดชะงักโดยไม่ทราบสาเหตุ หรือทำให้ไฟล์เสียหาย ขัดขวางกระบวนการพิมพ์ เป็นต้น

4. หนอน (Worm) โดยที่จริงแล้วหนอนไวรัสยังไม่ถือว่าเป็นไวรัสคอมพิวเตอร์ เนื่องจากจะไม่ติดกับโปรแกรมใดๆ หนอนไวรัสอาจจะเป็นโปรแกรมหนึ่งหรือชุดคำสั่งโปรแกรมซึ่งสามารถทำสำเนาได้เองและจะติดกับคอมพิวเตอร์ในระบบเครือข่าย (Network) เป้าหมายของหนอนไวรัสคือการโจมตีผ่านเครือข่ายซึ่งมีตั้งแต่ขัดขวางการทำงานไปจนถึงทำให้เครือข่ายล่ม

5. โทรจัน (Trojan) คือ โปรแกรมจำพวกหนึ่งที่ออกแบบมาเพื่อให้แฝงตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่างๆ และส่งกลับไปยังผู้ประสงค์ร้าย เพื่อใช้โจมตีระบบในภายหลังจะถูกแนบมากับอีการ์ด อีเมล์ หรือโปรแกรมที่มีให้ดาวน์โหลดตามอินเทอร์เน็ตในเว็บไซต์ใต้ดิน

สปายแวร์ (Spyware) คืออะไร

คือ โปรแกรมเล็กๆ ที่ถูกเขียนขึ้นมาสอดส่อง (สปาย) การใช้งานเครื่องคอมพิวเตอร์ ทั้งนี้เพื่อโฆษณาสินค้าต่างๆ สปายแวร์บางตัวก็สร้างความรำคาญเพราะจะเปิดหน้าต่างโฆษณาบ่อยๆ แต่บางตัวร้ายกว่านั้น คือ ทำให้ไม่สามารถใช้อินเตอร์เน็ท เพราะจะโชว์หน้าต่างโฆษณา หรืออาจจะป๊อปอัพหน้าต่างเป็นสิบๆ หน้าต่าง ซึ่งบางครั้งจะเชื่อมโยงไปยังเว็บประเภทลามกอนาจารหรือผิดกฎหมาย

สาเหตุที่คอมพิวเตอร์ติดสปายแวร์

ผู้ใช้คอมพิวเตอร์ส่วนใหญ่ไม่เคยดูแลเครื่องของตัวเองเลย ไม่เคยป้องกัน ไม่เคยบำรุงรักษา มักเกิดปัญหาง่ายๆ ดังนี้

1. เข้าเยี่ยมเวปไซท์ต่างๆ และดาวน์โหลดโปรแกรมโดยไม่ได้อ่านหรือศึกษารายละเอียดของโปรแกรมที่จะดาวน์โหลด

2. ดาวน์โหลดโปรแกรมฟรี (Freeware) มาใช้ โปรแกรมฟรีหลายตัวมีสปายแวร์ติดมาด้วย ตัวอย่างเช่น โปรแกรม Kazaa Media Desktop ซึ่งเป็นโปรแกรมให้ผู้ใช้แลกเปลี่ยนไฟล์กัน เหมือนกับโปรแกรม Napster ขณะนี้มีผู้ใช้โปรแกรม Kazaa เป็นล้านๆ คน เพราะสามารถใช้ดาวน์โหลดเพลง MP3 ฟรีได้ ซึ่ง Kazaa นั้น มีอยู่ 2 แบบ คือ แบบใช้ฟรีกับแบบเสียเงิน ถ้าเป็นแบบฟรีแถมสปายแวร์มาด้วยกว่า 10 ตัว

3. เปิดโปรแกรมที่ส่งมากับอีเมล์ บางครั้งเพื่อนส่งอีเมล์มาให้พร้อมโปรแกรมสวยงาม ซึ่งเพื่อนเองก็ไม่รู้ว่ามีสปายแวร์อยู่ด้วยก็ส่งต่อๆ กันไปทำให้ระบาดไปสู่เครื่องอื่นๆ

ประเภทของสปายแวร์

สปายแวร์ แบ่งเป็นประเภทต่างๆ ดังนี้

1. Adware เป็นสปายแวร์ที่จะคอยส่งแบนเนอร์โฆษณามาที่คอมพิวเตอร์ของผู้ใช้ สาเหตุที่จัดให้ Adware เป็นสปายแวร์ก็เพราะมีส่วนประกอบของโปรแกรมที่สามารถติดตามข้อมูลของผู้ใช้และส่งข้อมูลนั้นออกไปที่อื่นได้

2. Dialer เป็นสปายแวร์ที่อยู่บนเวปโป๊ต่างๆ และใช้โมเด็มของเหยื่อหมุนโทรศัพท์ทางไกลต่อไปยังต่างประเทศ

3. Hijacker เป็นสปายแวร์ที่สามารถเปลี่ยนแปลง Start Page และ Bookmark บนโปรแกรมบราวเซอร์ต่างๆ

4. BHO (Browser Helper Objects) เป็นสปายแวร์ที่ยัดเยียดฟังก์ชั่นที่ไม่พึงประสงค์ให้บนโปรแกรมบราวเซอร์

5. Toolbar บางอย่างก็จัดเป็นสปายแวร์ที่ยัดเยียดเครื่องมือที่ไม่พึงประสงค์ให้บนโปรแกรมบราวเซอร์ด้วย

เมื่อ Spyware เข้ามาอยู่ในเครื่องผู้ใช้ มันก็จะแสดงลักษณะพิเศษของโปรแกรมออกมา คือ นำเสนอหน้าเว็บโฆษณาเชิญชวนให้คลิกทุกครั้งที่ผู้ใช้ออนไลน์อินเทอร์เน็ต โดยมาในรูปต่างๆ กัน ดังนี้

1. มี Pop up ขึ้นมาบ่อยครั้งที่เข้าเว็บ
2. ทูลบาร์มีแถบปุ่มเครื่องมือเพิ่มขึ้น
3. หน้า Desktop มีไอคอนประหลาดๆ เพิ่มขึ้น
4. เมื่อเปิด Internet Explorer หน้าเว็บแรกที่พบแสดงเว็บที่ไม่เคยพบเห็นมาก่อน
5. เว็บใดที่ผู้ใช้ไม่สามารถเข้าได้ หน้าเว็บโฆษณาของ Spyware จะมาแทนที่

อาการของคอมพิวเตอร์ที่ติดไวรัส

- เนื้อที่ฮาร์ดดิสก์ลดลงโดยไม่ทราบสาเหตุ ทั้งที่ไม่ได้ลงโปรแกรม หรือบันทึกข้อมูล
- วินโดวส์แสดงไดอะล็อกบ็อกซ์ข้อความโดยไม่ทราบสาเหตุ หรือมีโปรแกรมบางตัวทำงานโดยที่ไม่ได้สั่ง
- คอมพิวเตอร์ทำงานช้า อืดผิดปกติ ทั้งๆที่ไม่ได้ใช้โปรแกรมอะไร
- ไฟล์ข้อมูลมีขนาดใหญ่ขึ้นมาก ทุกครั้งที่ใช้งาน
- การเปิดหรือการโหลด เข้าใช้งานโปรแกรมเข้าสู่หน่วยความจำใช้เวลานานขึ้น
- เครื่องคอมพิวเตอร์เกิดอาการแฮงค์ (Hang) โดยไม่ทราบสาเหตุ อยู่ๆโปรแกรมก็ปิดเอง
- เปิดเครื่องคอมพิวเตอร์ไม่ได้ บูตเครื่องจากฮาร์ดดิสก์ไม่ได้
- เปิดไฟล์เอกสารไม่ได้ทั้งๆที่เคยเปิดอยู่ทุกวัน หรือเปิดได้แต่เป็นตัวอักษรประหลาดๆ ปนมาด้วย
- เครื่องคอมพิวเตอร์มีการกระทำที่แปลกๆ สุดแต่ผู้เขียนโปรแกรมไวรัสจะกำหนดมา เช่น อาจส่งเสียงพิสดารต่างๆ หรือกดอักษร A หนึ่งครั้ง ก็แสดงอักษร A ออกมาได้หลายสิบตัว
- เปิดเล่น โปรแกรม IE, Mozilla Firefox เข้าเว็บ สแกนไวรัส.com แล้วมีข้อความโฆษณาหรือข้อความแปลกๆ ขึ้นที่หน้าจอ
- โปรแกรมป้องกันไวรัสไม่สามารถเปิดได้ หรือเปิดโปรแกรมต่างๆ ไม่ได้ อยู่ดีๆ โปรแกรมที่ใช้ทุกวันก็หายไป
- เครื่องมีการรีสตาร์ทหรือปิดเองขณะใช้งาน หรือไม่สามารถบูตเข้าวินโดวส์ได้
- ฮาร์ดดิสก์ หรือ CPU ทำงานมากอย่างผิดสังเกต หรือไฟแสดงการทำงานของอุปกรณ์เครือข่าย (เช่น Broadband Modem, Hub, Switch) ติดตลอดเวลา โดยที่ท่านไม่ได้ใช้งานอะไรเป็นพิเศษ
- มีไฟล์ต่างๆ เช่น Autorun.inf หรือไฟล์นามสกุล .vbs ในไดรฟ์ต่างๆ โดยที่ไม่ได้สร้างขึ้น
- ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อยๆ
- เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ ๆ ก็หายไป

การตรวจหาไวรัสคอมพิวเตอร์และการกำจัดไวรัสคอมพิวเตอร์

การสแกน โปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกน (Scanning) เรียกว่า สแกนเนอร์ (Scanner) โดยจะมีการดึงเอาโปรแกรมบางส่วนของตัวไวรัส มาเก็บไว้เป็นฐานข้อมูล ส่วนที่ดึงมานั้นเราเรียกว่า ไวรัสซิกเนเจอร์ (Virus Signature) และเมื่อสแกนเนอร์ถูกเรียกขึ้นมาทำงาน ก็จะเข้าตรวจหาไวรัสในหน่วยความจำ บูตเซกเตอร์ และไฟล์โดยใช้ ไวรัสซิกเนเจอร์ที่มีอยู่ ข้อดีของวิธีการนี้ก็คือ เราสามารถตรวจสอบซอฟต์แวร์ที่มาใหม่ ได้ทันทีเลยว่าติดไวรัสหรือไม่ เพื่อป้องกันไม่ให้ไวรัสถูกเรียกขึ้นมาทำงานตั้งแต่เริ่มแรก แต่วิธีนี้มีจุดอ่อนอยู่หลายข้อ คือ

1. ฐานข้อมูลที่เก็บไวรัสซิกเนเจอร์จะต้องทันสมัยอยู่เสมอ และครอบคลุมไวรัสให้มากที่สุดเท่าที่จะทำได้ เพราะสแกนเนอร์จะไม่สามารถตรวจจับไวรัสที่ยังไม่มีซิกเนเจอร์ของไวรัสนั้น เก็บอยู่ในฐานข้อมูลได้

2. ยากที่จะตรวจจับไวรัสประเภทโพลีมอร์ฟิก เนื่องจากไวรัสประเภทนี้เปลี่ยนแปลง ตัวเองได้ จึงทำให้ไวรัสซิกเนเจอร์ที่ใช้สามารถนำมาตรวจสอบได้ก่อนที่ไวรัสจะเปลี่ยนตัวเองเท่านั้น

3. ถ้ามีไวรัสประเภทสทีลต์ไวรัสติดอยู่ในเครื่องตัวสแกนเนอร์อาจจะไม่สามารถ ตรวจหาไวรัสนี้ได้ ทั้งนี้ขึ้นอยู่กับความฉลาดและเทคนิคที่ใช้ระหว่างไวรัส และสแกนเนอร์ เนื่องจากมีไวรัสใหม่ๆ ออกมาอยู่เสมอๆ ผู้ใช้จึงจำเป็นจะต้องหาสแกนเนอร์ ตัวที่ใหม่ที่สุดมาใช้ มีไวรัสบางตัวจะเข้าไปติดในโปรแกรมทันทีที่โปรแกรมนั้นถูกอ่าน และถ้าสมมติว่าสแกนเนอร์ที่ใช้ไม่สามารถตรวจจับได้ และถ้าเครื่องมีไวรัสนี้ติดอยู่ เมื่อมีการเรียกสแกนเนอร์ขึ้นมาทำงาน สแกนเนอร์จะเข้าไปอ่านโปรแกรมทีละโปรแกรมเพื่อตรวจสอบ ผลก็คือ จะทำให้ไวรัสตัวนี้เข้าไปติดอยู่ในโปรแกรมทุกตัวที่ถูกสแกนเนอร์นั้นอ่านได้ สแกนเนอร์รายงานผิดพลาดได้ คือ ไวรัสซิกเนเจอร์ที่ใช้บังเอิญไปตรงกับที่มี อยู่ในโปรแกรมธรรมดาที่ไม่ได้ติดไวรัส ซึ่งมักจะเกิดขึ้นในกรณีที่ไวรัสซิกเนเจอร์ที่ใช้มีขนาดสั้นไป ก็จะทำให้โปรแกรมดังกล่าวใช้งานไม่ได้อีกต่อไป

การตรวจการเปลี่ยนแปลง การหาค่าพิเศษอย่างหนึ่งที่เรียกว่า เช็คซัม (Checksum) ซึ่งเกิดจากการนำเอาชุดคำสั่งและข้อมูลที่อยู่ในโปรแกรมมาคำนวณ หรืออาจใช้ข้อมูลอื่นๆ ของไฟล์ ได้แก่ แอตริบิวต์ วันและเวลา เข้ามารวมในการคำนวณด้วย เนื่องจากทุกสิ่งทุกอย่าง ไม่ว่าจะเป็นคำสั่งหรือข้อมูลที่อยู่ในโปรแกรม จะถูกแทนด้วยรหัสเลขฐานสอง ดังนั้นจึงสามารถนำเอาตัวเลขเหล่านี้มาผ่านขั้นตอนการคำนวณทางคณิตศาสตร์ได้ ซึ่งวิธีการคำนวณเพื่อหาค่าเช็คซัมนี้มีหลายแบบ และมีระดับการตรวจสอบแตกต่างกันออกไป เมื่อตัวโปรแกรม ภายในเกิดการเปลี่ยนแปลง ไม่ว่าไวรัสนั้นจะใช้วิธีการแทรกหรือเขียนทับก็ตาม เลขที่ได้จากการคำนวณครั้งใหม่ จะเปลี่ยนไปจากที่คำนวณได้ก่อนหน้านี้ ข้อดีของการตรวจการเปลี่ยนแปลงก็คือ สามารถตรวจจับไวรัสใหม่ๆ ได้ และยังมีความสามารถในการตรวจจับไวรัสประเภทโพลีมอร์ฟิกไวรัสได้อีกด้วย แต่ก็ยังยากสำหรับสทีลต์ไวรัส ทั้งนี้ขึ้นอยู่กับความฉลาดของโปรแกรมตรวจหาไวรัสเองด้วยว่าจะสามารถถูกหลอกโดยไวรัสประเภทนี้ได้หรือไม่ และมีวิธีการตรวจการเปลี่ยนแปลงนี้จะตรวจจับไวรัสได้ก็ต่อเมื่อไวรัสได้เข้าไปติดอยู่ใน

เครื่องแล้วเท่านั้น และค่อนข้างเสี่ยงในกรณีที่เริ่มมีการคำนวณหาค่าเช็คซัมเป็นครั้งแรก เครื่องที่ใช้ต้องแน่ใจว่าบริสุทธิ์พอ คือต้องไม่มีโปรแกรมใดๆ ติดไวรัส มิฉะนั้นค่าที่หาได้จากการคำนวณที่รวมตัวไวรัสเข้าไปด้วย ซึ่งจะลำบากภายหลังในการที่จะตรวจหาไวรัสตัวนี้ต่อไป

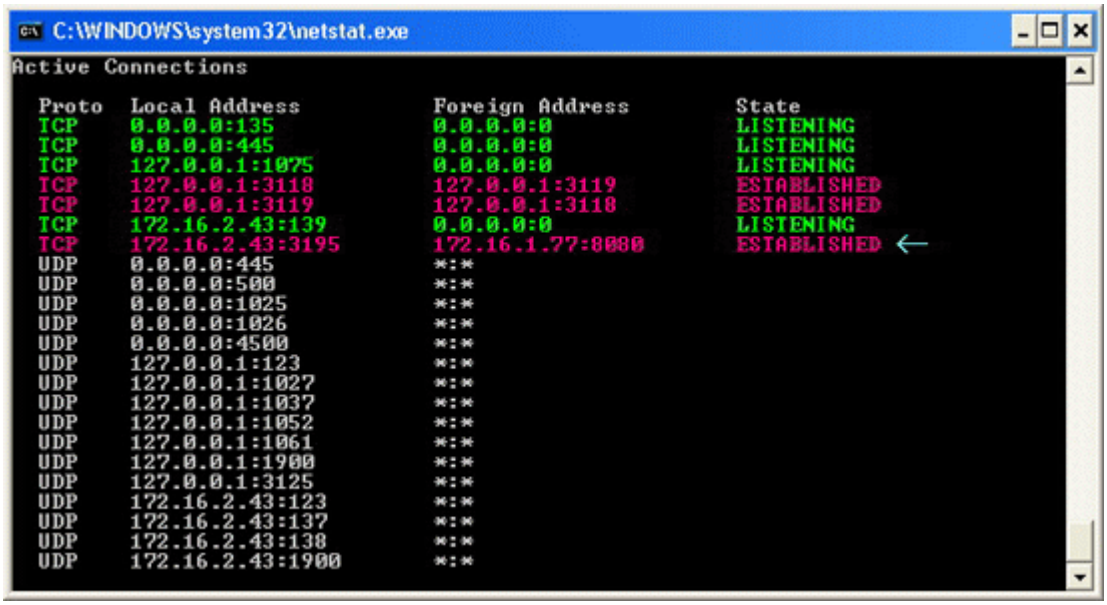
การเฝ้าดู เพื่อที่จะให้โปรแกรมตรวจจับไวรัสสามารถเฝ้าดูการทำงานของเครื่องได้ตลอดเวลานั้น จึงได้มีโปรแกรมตรวจจับไวรัสที่ถูกสร้างขึ้นมาเป็นโปรแกรมแบบเรซิเดนท์หรือ ดีไวซ์ไดรเวอร์ โดยเทคนิคของการเฝ้าดูนั้นอาจใช้วิธีการสแกนหรือตรวจการเปลี่ยนแปลงหรือสองแบบรวมกันก็ได้ การทำงานโดยทั่วไปก็คือ เมื่อซอฟต์แวร์ตรวจจับไวรัสที่ใช้วิธีนี้ถูกเรียกขึ้นมาทำงาน ก็จะเข้าไปตรวจในหน่วยความจำของเครื่องก่อน ว่ามีไวรัสติดอยู่หรือไม่โดยใช้ไวรัสซิกเนเจอร์ ที่มีอยู่ในฐานข้อมูล จากนั้นจึงค่อยนำตัวเองเข้าไปฝังอยู่ในหน่วยความจำ และต่อไปถ้ามีการเรียกโปรแกรมใดขึ้นมาใช้งาน โปรแกรมเฝ้าดูนี้ก็จะเข้าไปตรวจโปรแกรมนั้นก่อน โดยใช้เทคนิคการสแกนหรือตรวจการเปลี่ยนแปลงเพื่อหาไวรัส ถ้าไม่มีปัญหาก็จะอนุญาตให้โปรแกรมนั้นขึ้นมาทำงานได้ นอกจากนี้โปรแกรมตรวจจับไวรัสบางตัวยังสามารถตรวจสอบขณะที่มีการคัดลอกไฟล์ได้อีกด้วย

ข้อดีของวิธีนี้คือ เมื่อมีการเรียกโปรแกรมใดขึ้นมา โปรแกรมนั้นจะถูกตรวจสอบก่อนทุกครั้งโดยอัตโนมัติ ซึ่งถ้าเป็นการใช้สแกนเนอร์จะสามารถทราบได้ว่าโปรแกรมใดติดไวรัสอยู่ ก็ต่อเมื่อทำการเรียกสแกนเนอร์นั้นขึ้นมาทำงานก่อนเท่านั้น

ข้อเสียของโปรแกรมตรวจจับไวรัสแบบเฝ้าดูก็คือ จะมีเวลาที่เสียไปสำหรับการตรวจหาไวรัสก่อนทุกครั้ง และเนื่องจากเป็นโปรแกรมแบบเรซิเดนท์หรือดีไวซ์ไดรเวอร์ จึงจำเป็นจะต้องใช้หน่วยความจำส่วนหนึ่งของเครื่องตลอดเวลาเพื่อทำงาน ทำให้หน่วยความจำในเครื่องเหลือน้อยลง และเช่นเดียวกับสแกนเนอร์ก็คือ จำเป็นจะต้องมีการปรับปรุงฐานข้อมูลของไวรัสซิกเนเจอร์ให้ทันสมัยอยู่เสมอ

การใช้คำสั่ง netstat ตรวจสอบ ในปัจจุบันสปายแวร์ (Spyware) นั้นเป็นปัญหาใหญ่ปัญหาหนึ่งที่คุกคามผู้ใช้คอมพิวเตอร์ โดยระดับความร้ายแรงของปัญหานั้นอาจแค่ก่อให้เกิดความรำคาญจนถึงระดับทำให้เกิดความสูญเสียทรัพย์สินเงินทองหรือชื่อเสียงได้ และถึงแม้ว่าผู้ใช้จะป้องกันโดยติดตั้งโปรแกรมป้องกันสปายแวร์แล้วก็ตาม แต่ก็ยังมีโอกาสที่จะมีสปายแวร์หลุดลอดเข้ามาในเครื่องได้ การตรวจหาสปายแวร์นั้น นอกจากจะใช้โปรแกรมป้องกันสปายแวร์แล้ว ผู้ใช้ยังสามารถทำการตรวจสอบหาสปายแวร์ด้วยตนเองโดยใช้ยูทิลิตี้ netstat ซึ่งมีมาพร้อมกับระบบ Windows XP และ Windows 7 ล้ว

Netstat เป็นคำสั่งที่ใช้แสดงสถานะการเชื่อมต่อกับเครื่องคอมพิวเตอร์เครื่องอื่นๆ โดยที่สนใจจะเป็นการเชื่อมต่ออินเทอร์เน็ตผ่านโปรโตคอล TCP/IP



จากภาพคอลัมน์แรก (Proto) จะแสดงโปรโตคอลที่ใช้เชื่อมต่อ

คอลัมน์ที่สอง (Local Address) เป็น IP เครื่องผู้ใช้เอง

คอลัมน์ที่สาม (Foreign Address) เป็น IP เครื่องอื่นที่ติดต่อกับผู้ใช้

คอลัมป์ที่สี่ (State) สถานะการเชื่อมต่อ ซึ่งจะมีหลายๆสถานะ จะขอกล่าวแบบง่ายๆ มี 2 สถานะ

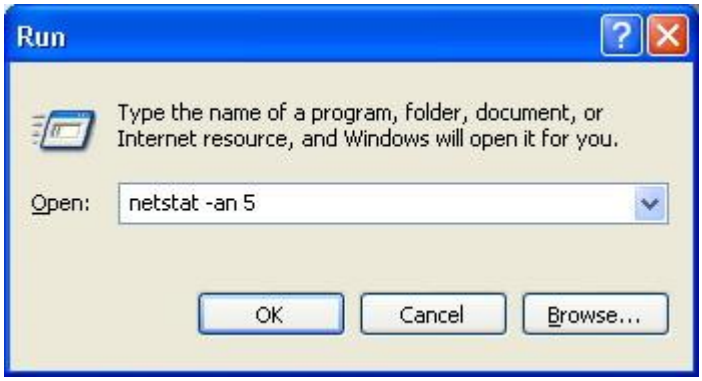
- นำสถานะ LISTENING เป็นสถานะที่เปิดรอไว้ คอยคนอื่นมาเชื่อมต่อ

- สถานะ ESTABLISHED เป็นสถานะที่กำลังเชื่อมต่ออยู่ ซึ่งสถานะนี้เองที่เราจะใช้ในการตรวจสอบโปรแกรมประเภท spyware โดยการดูว่ามีการเชื่อมต่อใดที่อยู่ในสถานะ ESTABLISHED และเชื่อมต่อไปยังคอมพิวเตอร์เครื่องที่เราไม่รู้จัก (Foreign Address แปลกๆ) หรือไม่

วิธีการตรวจสอบ มีดังนี้

1. เปิดหน้าต่างคอมมาดน์พร็อมพ์ โดยการคลิกที่ Start คลิก Run พิมพ์ cmd แล้วกด Enter (ใน Windows Vista นั้นให้คลิก All Programs คลิก Accessories คลิกขวา Command Prompt แล้วเลือก Run as Administrator ให้ใส่พาสเวิร์ดของ Adminsitartor เมื่อระบบถาม)

2. ในหน้าต่างคอมมาดน์พร็อมพิมพ์ netstat -nab แล้วกด Enter ซึ่งคำสั่งนี้จะแสดงชื่อโปรแกรมที่กำลังเชื่อมต่อกับอินเทอร์เน็ต โดยจะแสดงรายละเอียดของหมายเลขไอพีและพอร์ต



จากนั้นทำการตรวจสอบผลที่ได้ โดยดูว่าเครื่องคอมพิวเตอร์มีการเชื่อมต่อไปยังเครื่องแปลกๆ ที่ไม่รู้จักหรือไม่ ถ้ามีนั่นคือสัญญาณเตือนให้ทราบว่าเครื่องนี้กำลังโดนดูดข้อมูลออกไป ให้รีบหาโปรแกรมกำจัดสปายแวร์มาใช้เพื่อป้องกันข้อมูล และรักษาแบนด์วิธในการเชื่อมต่อเน็ตไม่ให้เสียเปล่าจากโปรแกรมเหล่านี้

เทคนิคการกำจัดไวรัสคอมพิวเตอร์และสปายแวร์

1. ใช้เครื่องมือในการกำจัดไวรัส Remove Tools

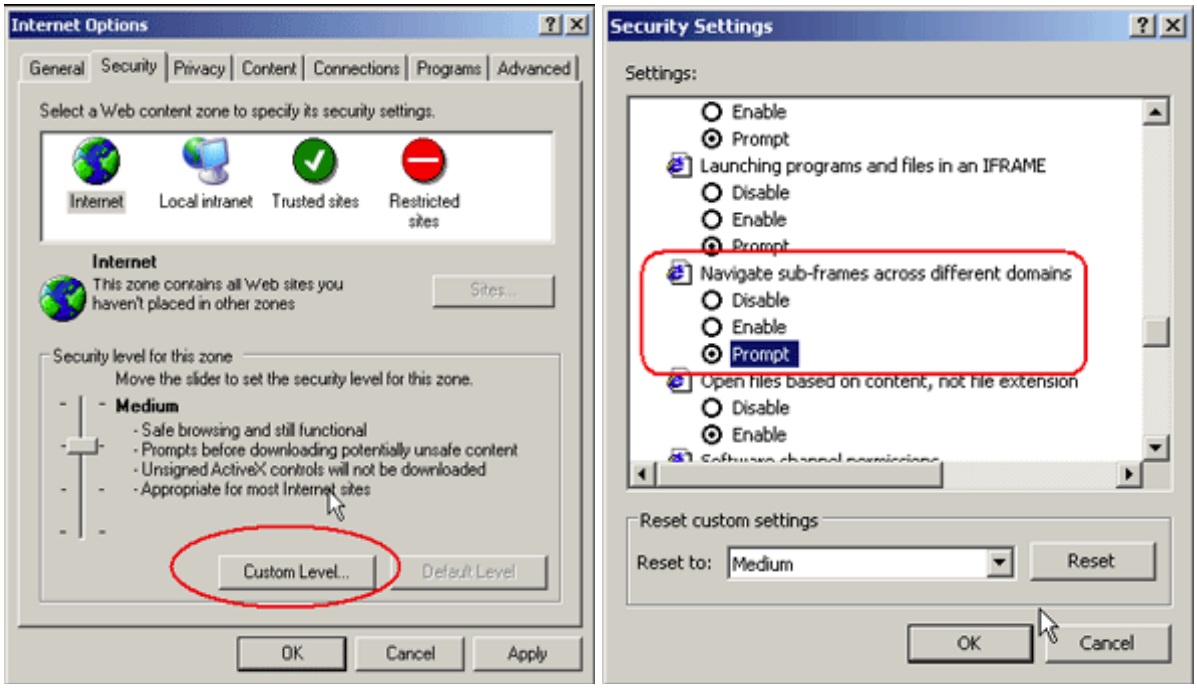
Remove Tools คือ เครื่องมือในการกำจัดไวรัสในรูปแบบตัวต่อตัว หมายความว่า ถ้าผู้ใช้ทราบว่าไวรัสที่ติดนั้นคืออะไร แต่โปรแกรมที่ใช้อยู่ไม่สามารถกำจัดได้ ดังนั้น เราอาจจำเป็นต้องดาวน์โหลด Remove Tools จากเว็บไซต์มาจัดการโดยเฉพาะ เช่น http://securityresponse.symantec.com/avcenter/tools.list.html

จุดแข็ง สามารถกำจัดไวรัสได้ด้วยโปรแกรมเฉพาะ และกำจัดได้หมด

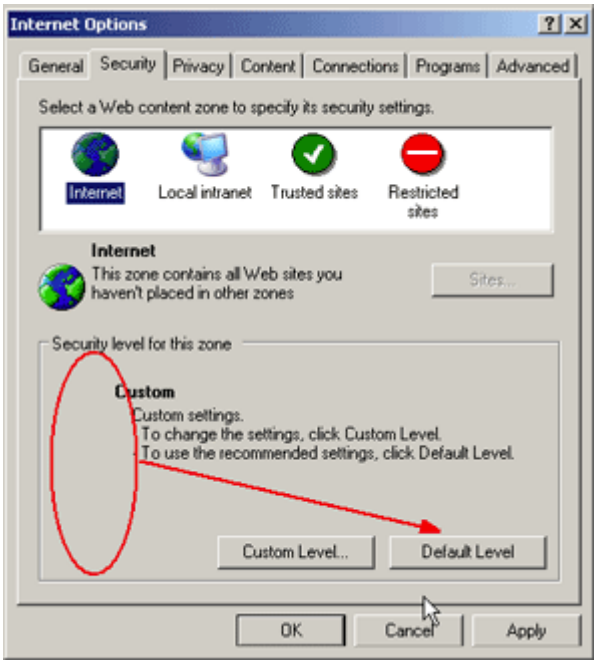
จุดอ่อน ไม่สามารถป้องกันไวรัสแบบ Real Time ได้ เพราะใช้สำหรับตรวจสอบไวรัสเป็นรายครั้ง ไม่มีการอัพเดทโปรแกรมผ่านทางอินเตอร์เน็ต ต้องเข้าไปเว็บไซต์นั้นๆ ใหม่ และ ดาวน์โหลดมาใหม่ การกำจัดไวรัสบางครั้งจำเป็นต้องเป็น Windows Save Mode เท่านั้น และกำจัดไวรัสได้เฉพาะบางตัว จึงจำเป็นต้องรู้ชื่อไวรัสก่อนเพื่อจะได้เลือก ดาวน์โหลดปรแกรมที่ถูกต้อง และสามารถกำจัดให้หมดสิ้นได้

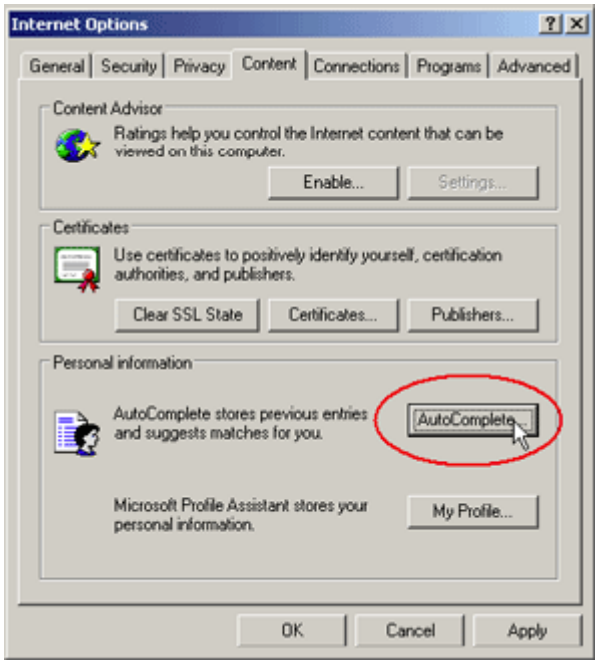
2. การตั้งค่าความปลอดภัยใน Internet Explorer

การตั้งค่าในบราวเซอร์ Internet Explorer เป็นสิ่งที่จำเป็นและมีความสำคัญ ปัญหาหลายๆ อย่างเกิดจากช่องโหว่เหล่านี้มากมายทีเดียว เพราะผู้เขียนโปรแกรมไวรัสและสปายแวร์มีความสามารถมากขึ้นจึงสามารถหารูโหว่เข้าโจมตีได้ง่ายขึ้น การปรับตั้งค่าบางส่วนทำได้ดังนี้ (ตัวอย่างนี้ใช้ IE 6.0 SP2)



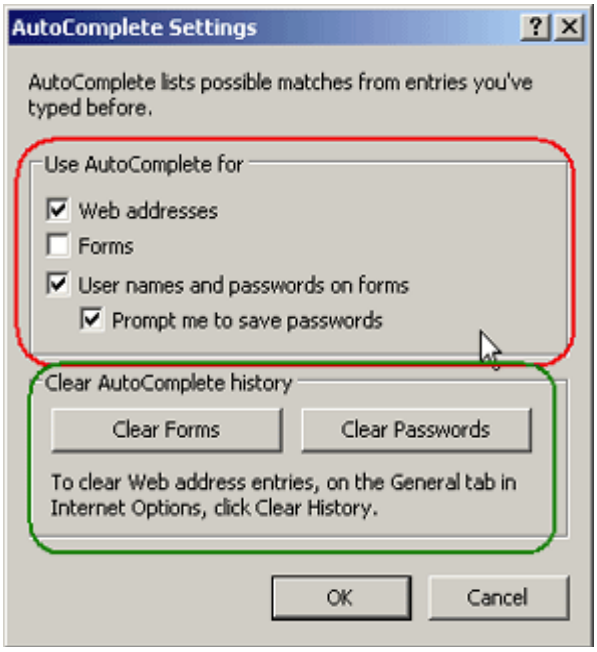
จากเมนูของ IE เลือก Tools --> Internet Options --> Security ค่าปกติของบราวเซอร์จะอยู่ที่ Medium ถ้าตั้งไว้เป็น High อาจจะเข้าชมบางเว็บไม่ได้เลย ให้คลิกที่ปุ่ม Custom Level เพื่อตั้งค่าดังรูปภาพ ให้เลื่อนรายละเอียดลงไปด้านล่างถึงหัวข้อ Navigate sub-frames across different domains ให้ตั้งค่าไว้ที่ Prompt แล้วคลิกปุ่ม OK เพื่อเก็บค่านี้ไว้

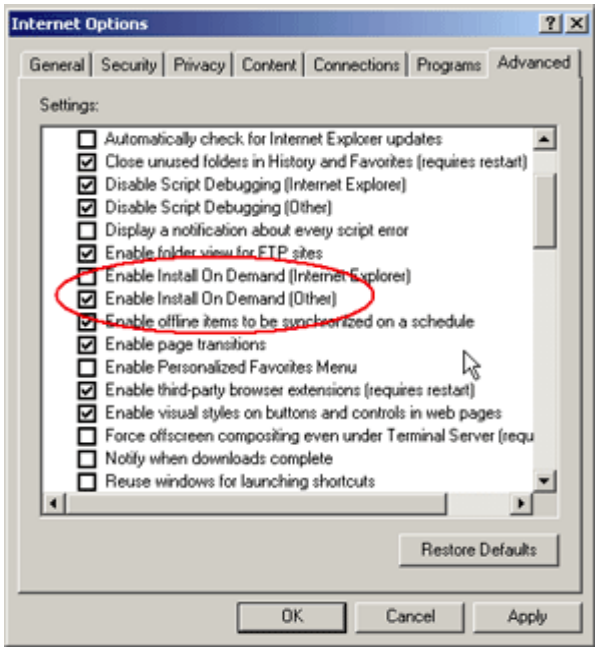




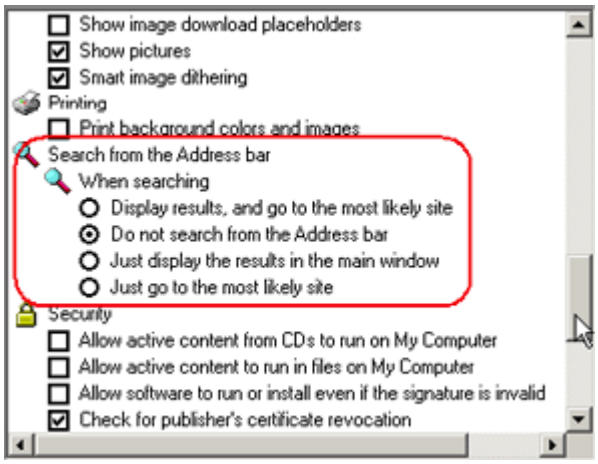
เมื่อตั้งค่าแล้วจะเห็นว่า สไลด์เลื่อนปรับค่า Security (ในวงกลม) หายไป สามารถเรียกกลับคืนด้วยคลิกที่ปุ่ม Default Level ต่อไปเราจะปรับตั้งค่าในส่วน Content ที่ AutoComplete... เพื่อกำหนดค่าการจดจำรหัสผ่านและประวัติการท่องเว็บต่างๆ ดังภาพถัดไป

การตั้งค่าให้จำ URL และรหัสผ่านต่างๆ





ถ้ายกเลิกการ Check box ต่อไปบราวเซอร์จะไม่จำ URL ที่เคยไปมาก่อน และรหัสผ่านต่างๆ ที่เคยกรอกไว้เช่น รหัสผ่านในการรับ - ส่งอีเมล์ผ่านหน้าเว็บ การกรอกข้อมูลในฟอร์ม เมื่อยกเลิกแล้วต้องการลบสิ่งที่โปรแกรมเคยบันทึกสามารถทำได้ด้วยการคลิกปุ่ม Clear Form และปุ่ม Clear Password



ในกรอบขวามือบนเป็นการคลิกไปที่แท็ป Advanced เพื่อกำหนดให้ยกเลิก (เอาเครื่องหมายถูกออกจากหัวข้อที่วงไว้) การติดตั้งสคริปต์หรือโปรแกรมตามความต้องการอื่น เช่น พวก Browser hijacker ไปเปลี่ยนค่าในบราวเซอร์

ในด้านซ้ายมือเป็นการตั้งค่าไม่ให้บราวเซอร์ไปค้นหาเว็บไซต์อื่นๆ ที่มีชื่อใกล้เคียงกัน แต่ให้แสดงเป็นหน้าว่างๆ แทน เพราะมีหนอนไวรัส หรือสปายแวร์บางตัว จะอาศัยช่องโหว่ของการป้อนข้อมูล URL ผิด ทำให้วิ่งตรงไปยังเว็บไซต์ที่โปรแกรมต้องการได้ จากนั้นก็จะพยายามติดตั้งหรือฝังตัวสคริปต์ลงในเครื่องเพื่อการรับส่งข้อมูลนั่นเอง

เพียงขั้นตอนง่ายๆ ก็จะทำให้การใช้งานอินเทอร์เน็ตมีความเสี่ยงลดน้อยลงได้และเมื่อใช้ร่วมกับโปรแกรมป้องกันอื่นๆ ก็จะช่วยให้มีความปลอดภัยมากยิ่งขึ้น

การป้องกันไวรัสคอมพิวเตอร์

การติดไวรัสคอมพิวเตอร์ได้มาจากหลายทางดังนี้

- ไวรัสจากอินเตอร์เน็ต
- ไวรัสยูเอสบีแฟลชไดร์ฟ
- ไวรัสจากการเชื่อมต่อเครือข่าย
- ติดตั้งซอฟต์แวร์ผิดลิขสิทธิ์ แล้วมีโปรแกรมประสงค์ร้ายแฝงมา
- ถูกหลอก หรือรู้เท่าไม่ถึงการณ์ โดยติดตั้งโปรแกรมที่ไม่รู้จัก หรือคลิกลิงค์ที่เชื่อมต่อกับเว็บไซต์ที่ติดไวรัส
- ติดไวรัสผ่านทางจดหมายอิเล็กทรอนิกส์ เนื่องจากตั้งรหัสผ่านที่สามารถเดาได้ง่าย หรือไวรัสใช้โปรแกรมสุ่มหารหัสผ่านเสี่ยงต่อการถูกแฮ็คจดหมายอิเล็กทรอนิกส์ หลักการทั่วไปของการป้องกันมีดังนี้

1. จำกัดสิทธิ์ของผู้ใช้ (Least user privilege) หมายถึงไม่ควรใช้ Admin account ในการใช้งานคอมพิวเตอร์ เนื่องจากสิทธิ์ Admin เป็นสิทธิสูงสุดของคอมพิวเตอร์ เมื่อถูกไวรัสจู่โจมทำให้ไวรัสนั้นมีสิทธิเทียบเท่า Admin ไปด้วย
2. update Web browser บ่อยๆ รวมถึง update plugin
3. update program สแกนไวรัสที่ติดตั้งบนเครื่องคอมพิวเตอร์ตามระยะเวลา
4. ติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้อง
5. ติดตั้งโปรแกรมป้องกันไวรัส สปายแวร์ มัลแวร์ โดยเฉพาะโปรแกรมป้องกันไวรัสเพียงอย่างใดอย่างหนึ่งเท่านั้น เพื่อป้องกันการทำงานช้าลงของเครื่องคอมพิวเตอร์
6. รหัสผ่านที่ใช้สำหรับเข้าใช้งานแต่ละโปรแกรมไม่ควรใช้รหัสเดียวกัน เพื่อป้องกันการถูกแฮ็ค
7. ควรติดตั้งเฉพาะโปรแกรมที่จำเป็นสำหรับการปฏิบัติงานเท่านั้น
8. เมื่อจะเข้าใช้เว็บไซต์ใดให้สังเกตชื่อเว็บไซต์ (URL) ว่าแปลกไปจากเดิมหรือไม่ เพราะอาจจะเข้าเว็บไซต์ที่เป็นไวรัสได้

วิธีการป้องกัน ไวรัสคอมพิวเตอร์

1. วิธีการที่ดีที่สุดในการป้องกันปัญหาไวรัสคอมพิวเตอร์ คือ ให้ติดตั้งโปรแกรมแอนตี้ไวรัสแล้วอัพเดทไวรัสอย่างสม่ำเสมอ และให้สแกนไวรัสเป็นประจำ โดยสแกนแบบ Full

- ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสมกับ OS ของเครื่อง
- สร้างแผ่น Emergency Disc หรือแผ่น boot CD/USB เพื่อใช้ในการกู้ระบบ
- อัพเดตข้อมูลไวรัสของโปรแกรมทุกวัน หรือทุกครั้งที่โปรแกรมแจ้งเตือนให้อัพเดต
- เปิดใช้งาน auto-protect ถ้าโปรแกรมสนับสนุน
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่าง ๆ

- ใช้โปรแกรมเพื่อตรวจหาไวรัสบนเครื่องคอมพิวเตอร์อย่างน้อย 1 ครั้ง ต่อสัปดาห์

2. ติดตั้งโปรแกรมอุดช่องโหว่ (patch) โดยการอัพเดตซอฟต์แวร์และโปรแกรมประยุกต์ต่างๆ ให้ใหม่อยู่เสมอ

- ระบบปฏิบัติการ (OS) Windows, โปรแกรม Internet Explorer (IE) และโปรแกรม Microsoft Office เป็นต้น

3. ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่างๆ เช่น แผ่นฟล็อปปี้ดิสก์ แผ่นซีดี แผ่นดีวีดี เทปแบ็กอัป หรือไม่ทราบแหล่งที่มา เป็นต้น

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif เป็นต้น รวมทั้งไฟล์ที่มีนามสกุลซ้อนกัน เช่น .jpg, .exe, .gif.scr, txt.exe เป็นต้น ให้ลบไฟล์นั้นทิ้งทันที

4. ใช้ความระมัดระวังในการเปิดอ่าน อี-เมล์

- อย่าเปิดไฟล์ที่แนบมากับ E-mail จนกว่าจะรู้ที่มา
- อย่าเปิดอ่านอี-เมล์ที่มี Subject ที่เป็นข้อความจูงใจ
- ลบอี-เมล์ที่ไม่ทราบแหล่งที่มาทิ้งทันที เพื่อตัดปัญหาทั้งปวง

5. ตระหนักถึงความเสี่ยงของไฟล์ที่ดาวน์โหลด หรือได้รับจากทางอินเตอร์เน็ต

- ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมที่ใช้สนทนา Social Network เช่น ICQ, MSN, skype, facebook, twitter เป็นต้น หรือการแลกเปลี่ยนไฟล์ โดยเฉพาะไฟล์ที่สามารถรันได้ เช่น ไฟล์ที่มีนามสกุล .exe, .pif, .com, .bat, .vbs เป็นต้นโดยไม่ได้ตรวจสอบแหล่งที่มาก่อน
- ไม่ควรเข้าเว็บไซต์ที่มากับอี-เมล์หรือโปรแกรมสนทนาต่างๆ รวมทั้งโฆษณาชวนเชื่อหรือหน้าเว็บที่ปรากฏขึ้นมาโดยไม่ตั้งใจ
- ไม่ดาวน์โหลดไฟล์ต่างๆ จากเว็บไซต์ที่ไม่มั่นใจ หรือไม่น่าเชื่อถือ
- ติดตามข่าวสารข้อมูลการแจ้งเตือนไวรัสจากแหล่งข้อมูลด้านความปลอดภัยอยู่เสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ถ้าต้องการแชร์ไฟล์ ควรแชร์แบบอ่านอย่างเดียว และตั้งรหัสผ่านด้วย

วิธีการป้องกันสปายแวร์

เพื่อจะป้องกันการติดตั้งสปายแวร์โดยไม่ได้ตั้งใจ แนะนำให้ปฏิบัติตามวิธีการ ดังนี้

1. ไม่คลิกลิ้งบนหน้าต่างเล็กๆ ที่ปรากฏขึ้นมาอัตโนมัติหรือโฆษณาที่ป๊อบอัพขึ้นมา เพราะป๊อบอัพเหล่านั้นมักจะมีสปายแวร์ฝังอยู่ การคลิกลิ้งเหล่านั้นจะทำให้สปายแวร์ถูกนำเข้ามาติดตั้งบนเครื่องได้ในทันที การปิดหน้าต่างป๊อบอัพเหล่านั้นควรคลิกที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar)

2. ควรเลือกที่คำตอบ "No" ทุกครั้งที่มีคำถามต่างๆ ถามขึ้นมาจากป๊อบอัพเหล่านั้นผู้ใช้ต้องระมัดระวังเป็นอย่างมากกับคำถามที่ปรากฏขึ้นมาเป็นไดอะล็อกบ็อกซ์ต่างๆ แม้ว่าไดอะล็อกบ๊อกซ์

เหล่านั้นจะเกิดขึ้นตอนกำลังรันโปรแกรม หรือโปรแกรมอื่นก็ตาม ควรปิดหน้าต่างป๊อบอัพเหล่านั้นด้วยวิธีคลิ้กที่ปุ่ม "X" บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ส

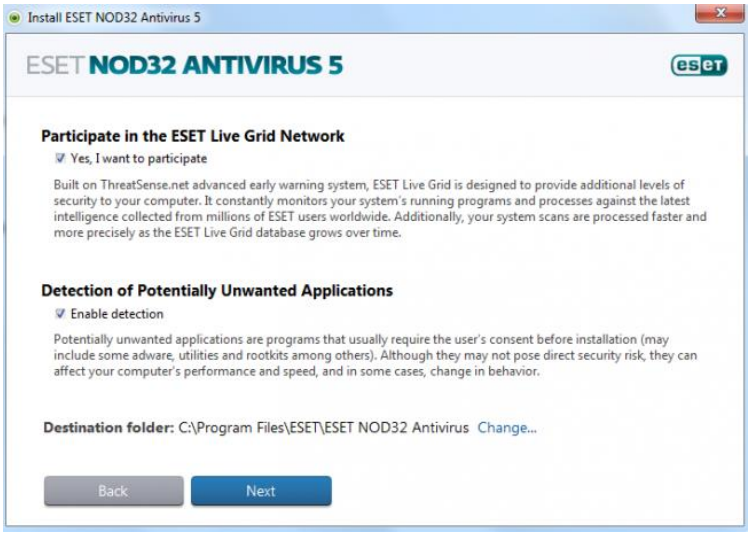
3. ควรระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่ให้ดาวน์โหลดฟรี เพราะมีหลายเว็บไซต์ที่หาแถบเครื่องมือหรือมีคุณสมบัติอื่นๆ ที่เหมาะสำหรับผู้ใช้ให้ปรับแต่งเองไว้ให้ดาวน์โหลดบนอินเทอร์เน็ต หากผู้ใช้ที่ต้องการใช้คุณสมบัติของเครื่องมือเหล่านี้ ควรจะดาวน์โหลดเครื่องมือเหล่านี้มาจากเว็บไซต์ที่น่าเชื่อถือ

4. ไม่ควรติดตามอีเมล์ลิ้งที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันสปายแวร์ ซอฟต์แวร์ป้องกันซึ่งลิ้งก์เหล่านั้นอาจจะเป็นการอนุญาตให้สปายแวร์เข้ามาติดตั้งในเครื่องของผู้ใช้โดยไม่รู้ตัว

การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ละการใช้งาน

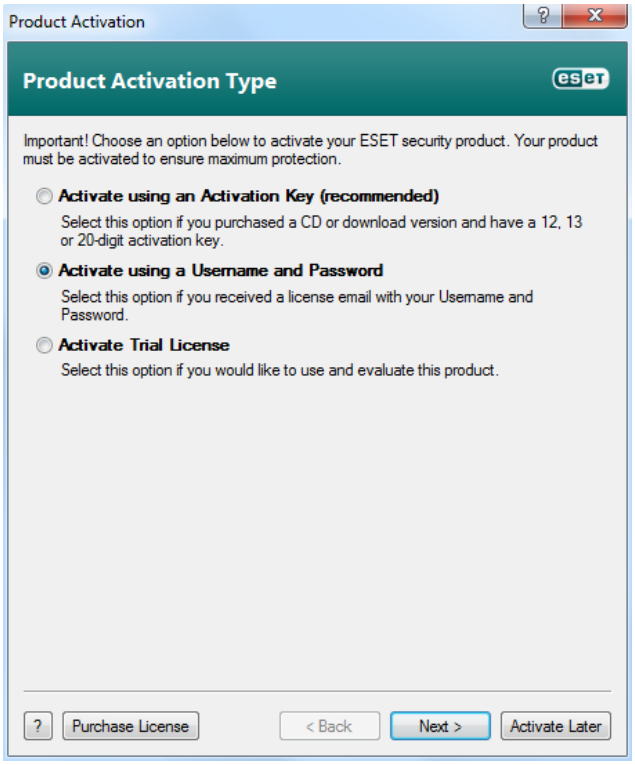
การติดตั้งโปรแกรม ESET NOD32 Antivirus สามารถดาวน์โหลดโปรแกรมได้จาก www.thaiware.com จากนั้นก็จะได้ไฟล์สำหรับติดตั้งมาเก็บไว้ในเครื่อง เมื่อคลิกที่ไฟล์นั้นก็จะมีหน้าต่างขึ้นมาดังนี้

หลังจากนั้นคลิกปุ่ม Install ก็จะมีหน้าให้อ่านเงื่อนไขการใช้งาน คลิก I Accept จากนั้นก็จะมีหน้าให้เลือกในการติดตั้ง ข้อแรกจะเป็นการยืนยันการเปิดฟังค์ชั่น Live Grid ข้อสองเป็นการแจ้งเตือนเวลาที่ผู้ใช้เปิดโปรแกรมที่ไม่รู้จัก แนะนำให้เลือกทั้งสองข้อ หลังจากนั้นคลิกที่ปุ่ม Next ได้

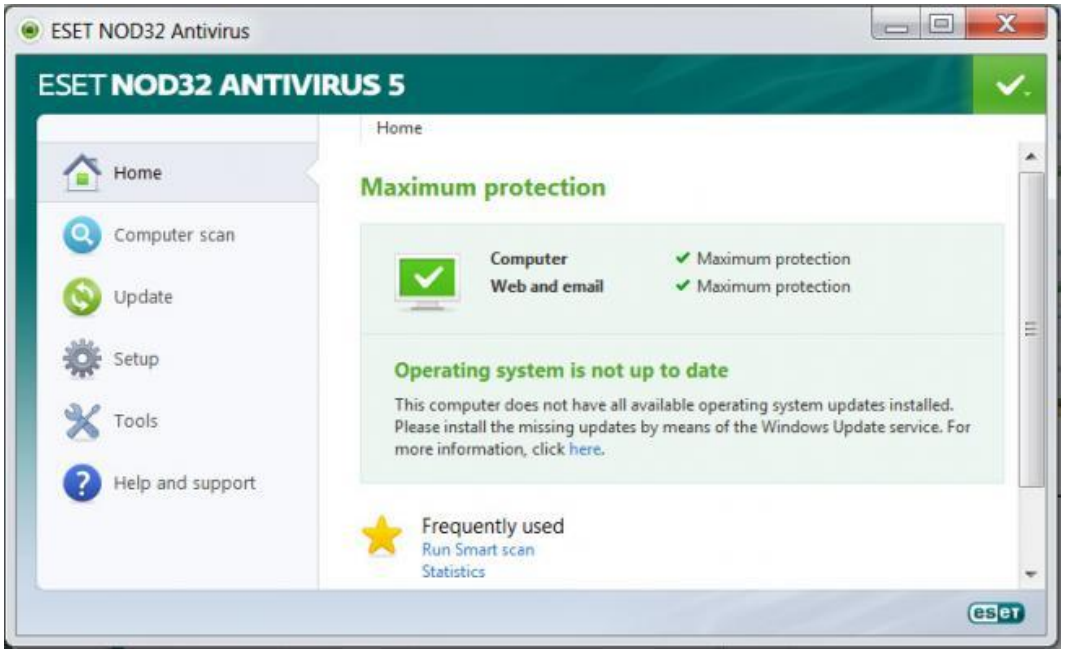


จากนั้นจะเป็นการติดตั้งโปรแกรมไปจนจบ ก็จะมีหน้าต่างขึ้นมาให้ Activate โปรแกรม ซึ่งจะทำได้ 3 วิธี โดยการใส่ Activation Key (ซึ่งต้องสั่งซื้อจากต่างประเทศ ระบบนี้ในไทยไม่มีขาย) วิธีที่ 2 คือ Activate โดยใช้ Username และ Password ซึ่งจะได้รับหลังจากนำ Product Code ไป

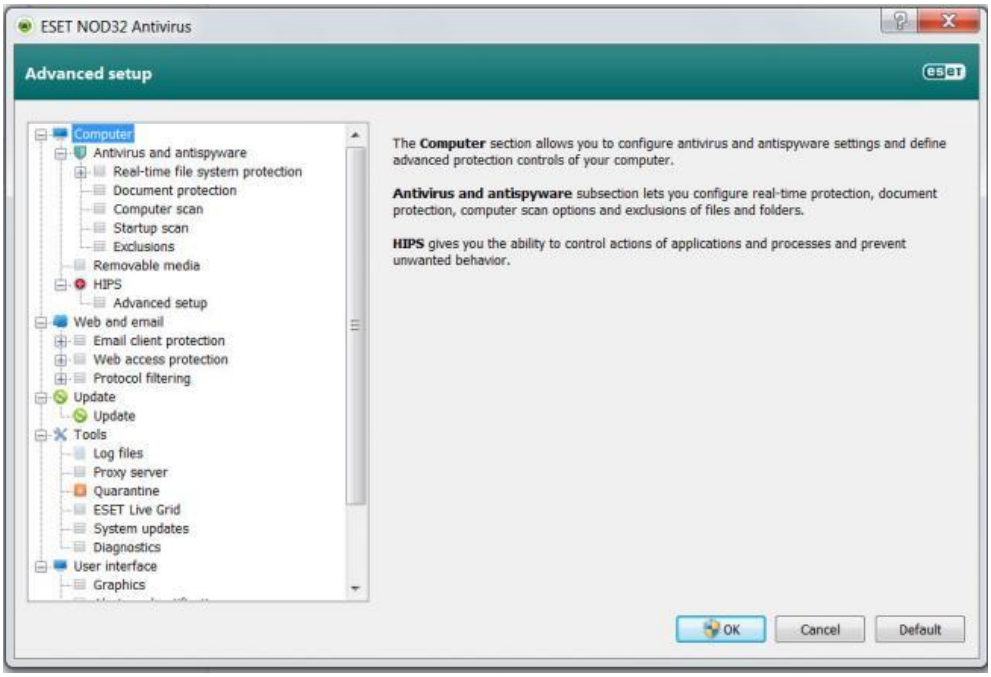
ลงทะเบียนที่ http://nod32th.com/register/index.php โดย Product Code นี้สามารถสั่งซื้อผ่านไทยแวร์ได้เลย (สั่งซื้อ Product Code) และวิธีสุดท้ายคือ Activate แบบทดลองใช้



การใช้งาน



ESET ยังคงรักษาคอนเซปส์การออกแบบ Dashboard สไตล์เรียบง่ายเอาไว้ เพื่อให้ผู้ใช้ทั่วไปสามารถใช้งานได้ไม่ยาก โดยฝั่งซ้ายจะมีคำสั่งในการใช้งาน และจะแจ้งสถานะของโปรแกรมให้ที่ทางฝั่งขวา แต่อย่างไรก็ดี พบว่าการปรับแต่งโปรแกรมในหน้าหลักนั้น มีตัวเลือกไม่ยืดหยุ่นเท่าที่ควร แนะนำว่าในการใช้งานครั้งแรก ควรเข้าไปปรับแต่งที่ Advance Setup ก่อน โดยเข้าไปที่เครื่องหมายถูกที่มุมขวาบน ซึ่งในนี้จะมีเมนูการปรับแต่งอยู่มากมายให้เลือก ก็เข้าไปเลือกให้เหมาะสมกับการใช้งานของตนเอง

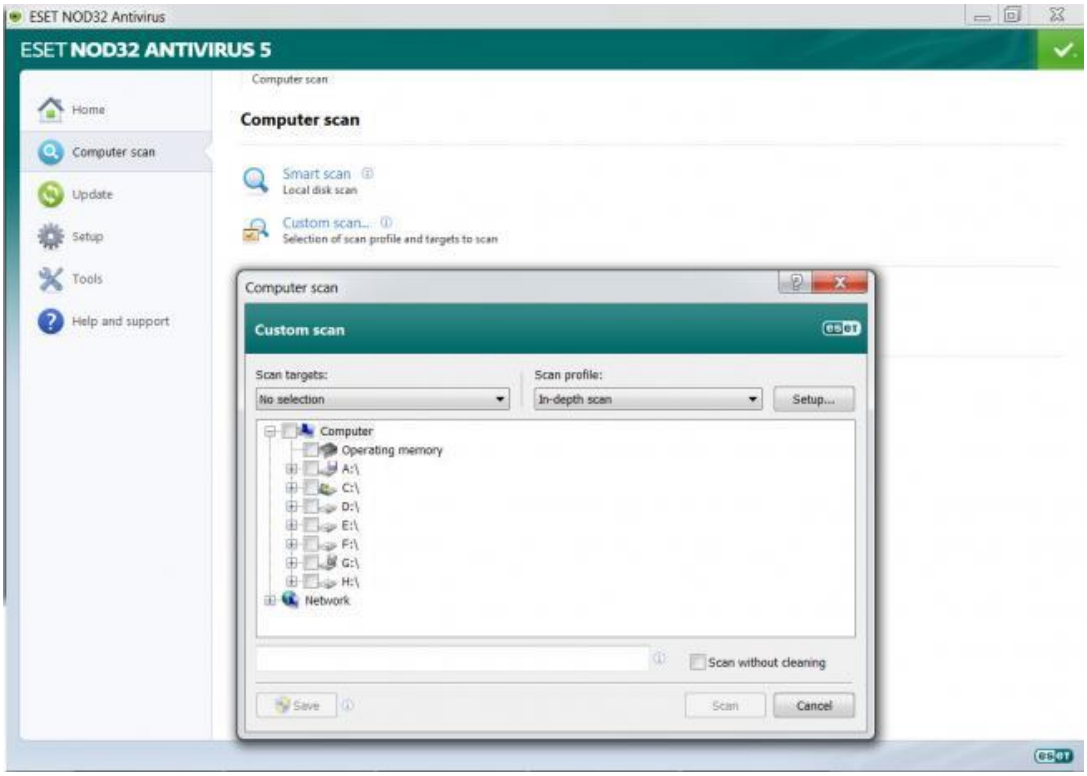


คุณสมบัติ

1. คุณสมบัติ Gamer mode ลดการใช้แรมและพื้นที่สำรองในการทำงานของโปรแกรมในขณะที่ผู้ใช้ดูภาพยนตร์หรือเล่นเกม โดยสามารถปรับให้ฟีเจอร์นี้เรียกใช้งานได้อัตโนมัติโดยเข้าไปที่ Setup -> Enter advanced setup เลือก User interface -> Gamer mode และติ้กในช่อง Enable Gamer Mode when running applications in full-screen mode automatically.

2. Live Grid รวบรวมข้อมูลไฟล์และลักษณะการทำงานของไวรัสจากผู้ใช้ Nod32 ทั่วโลกมาปรับปรุงฐานข้อมูลของโปรแกรมให้ทันสมัยอยู่เสมอ โดยอาศัยเทคโนโลยี Cloud

ขั้นตอนการสแกนไวรัส



Nod32 เวอร์ชั่นนี้ รองรับการสแกนและจัดการกับ Removeable Media โดยเมื่อต่อ Removeable Media จะมีการแจ้งเตือนให้สแกนทันที หรือสแกนภายหลัง (สามารถปรับแต่งค่าเริ่มต้นให้สแกนทันทีที่มีเชื่อมต่อ)

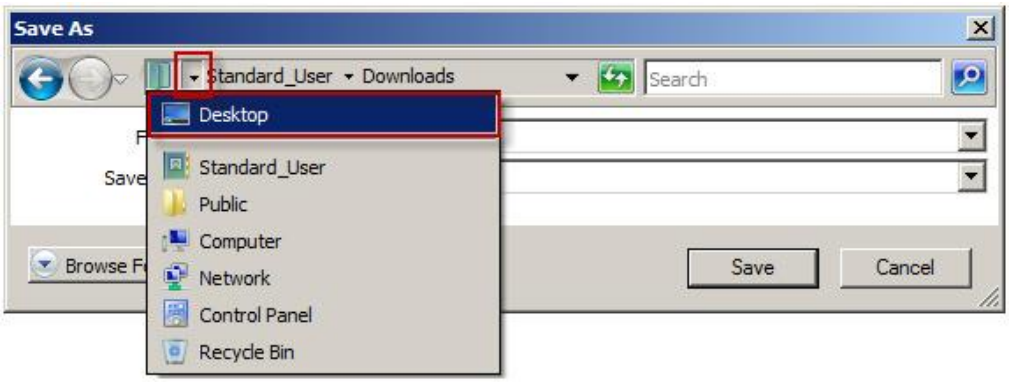
Nod32 รองรับการสแกนไดร์ฟหลักของเครื่องที่ติดตั้งและเครื่องอื่นบนเครือข่าย มีตัวเลือกในการสแกนให้ทั้งแบบ Smart Scan, In-Depth Scan และ Context Menu Scan. จากการทดสอบพบว่า Eset สามารถสแกนไฟล์ได้ค่อนข้างเร็ว โดยอยู่ที่ประมาณ 44.3 เมกกะไบต์ต่อวินาที การสแกนพื้นที่ 1 กิ๊กกะไบต์จะใช้เวลาประมาณ 23 วินาที (ทดสอบบนคอมพิวเตอร์ Windows 7 Home Premium Pentium Dual-Core T4200 (64 bit), แรม 3GB ฮาร์ดดิสก์ 210GB)

การติดตั้ง Kaspersky Anti-Virus 2011 ข้อแนะนำก่อนติดตั้งโปรแกรม ต้องแน่ใจว่าได้ uninstall โปรแกรมแอนตี้ไวรัสใดๆ ออกจากเครื่องเรียบร้อยแล้ว

เริ่มดาวน์โหลดโดยเลื่อนหน้าจอลงมาจนพบ Kaspersky Anti-Virus 2011 จากนั้นให้ใส่อีเมล์และกดปุ่ม Download

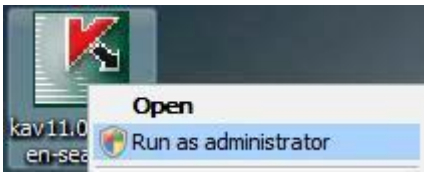
เมื่อคลิกดาวน์โหลด จะมีให้เลือก Run, Save และ Cancel ให้คุณเลือก Save

ต่อมาจะถามว่าต้องการให้นำไฟล์ไปไว้ที่ไหน ให้เลือกที่ **Desktop** และกดปุ่ม **Save**



กระบวนการดาวน์โหลดจะเริ่มขึ้น ความเร็วในการดาวน์โหลดขึ้นอยู่กับความเร็วในการเชื่อมต่ออินเตอร์เน็ท เมื่อดาวน์โหลดเสร็จแล้วให้กดปุ่ม **Close**

- ถ้าใช้ Windows XP ให้ดับเบิ้ลคลิกเพื่อติดตั้ง
- ถ้าใช้ Windows Vista หรือ Windows 7 ให้คลิกขวาที่ไฟล์ แล้วเลือก Run as administrator เมื่อมีข้อความขึ้นมาถามอีกครั้งให้คลิก Continue

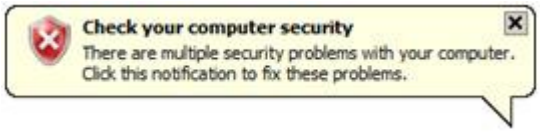


เมื่อจะติดตั้งอาจได้รับข้อความเตือน ให้คลิก **Run**

เมื่อตัวช่วยติดตั้งเปิดขึ้น ให้คลิก Next เพื่อเริ่มการติดตั้งแบบ Express

เมื่อเข้าสู่ข้อตกลงลิขสิทธิ์ และได้อ่านและยอมรับเงื่อนไขทั้งหมด ให้คลิกปุ่ม I agree ให้ติ๊กถูกหน้า I accept the terms of participation in Kaspersky Security Network และคลิกปุ่ม Install

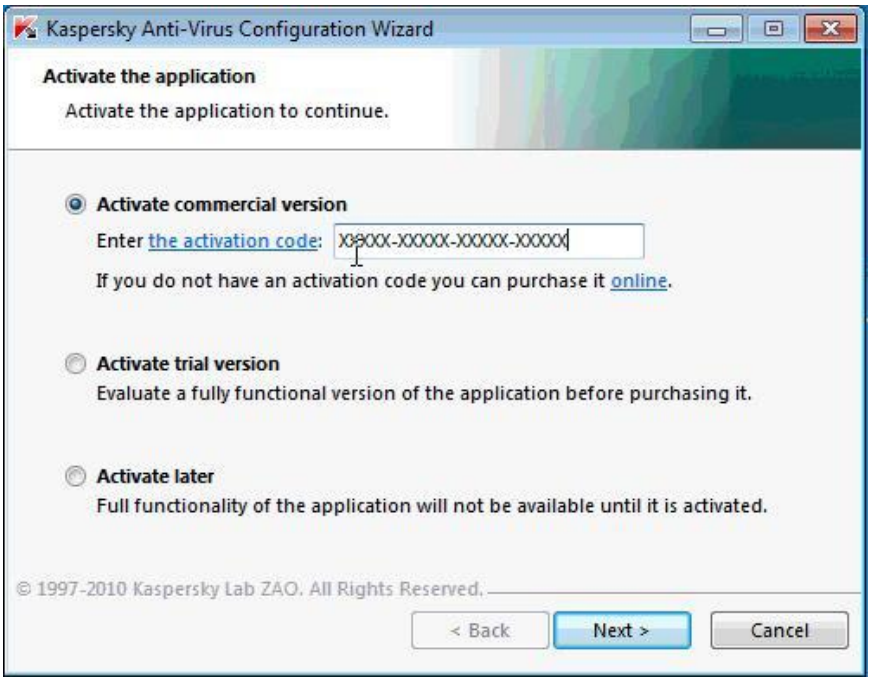
ข้อความเตือนจาก Windows Security Center ขณะทำการติดตั้งโปรแกรม ซึ่งเป็นเรื่องปกติและมันจะแก้ไขเองโดยอัตโนมัติเมื่อการติดตั้งเสร็จสิ้นแล้ว



การปรับแต่ง

มาถึงขั้นตอนนี้โปรแกรมจะให้คุณใส่ activation code ซึ่งมี 20 ตัวอักษร (XXXXX-XXXXX-XXXXX-XXXXX) ที่ได้รับทาง SMS ตัวช่วยเหลือจะช่วยให้ใส่ตัวอักษรเป็นตัวพิมพ์ใหญ่และมีขีดคั่นให้เอง ถ้าไม่ต้องการ activate ตัวช่วยเหลือจะค้นหา license ที่มีอยู่ในขณะนั้น หากต้องการ activate หลังจากติดตั้งโปรแกรมเสร็จแล้ว กรุณาดูขั้นตอนการ activate Kaspersky Anti-Virus 2011

ก่อนทำการ activate กรุณาเช็ควันและเวลาในเครื่องคอมพิวเตอร์ของให้ถูกต้อง



ให้รอขั้นตอนนี้สักครู่ หลังจาก activate แล้ว จะเห็นชนิดของ License และวันหมดอายุ จากนั้นคลิก Next เมื่อเสร็จสิ้นการติดตั้งและ activate ให้คลิก Finish เพื่อเริ่มการทำงาน Kaspersky Anti-Virus 2011

Kaspersky Anti-Virus 2011 จะเริ่มการอัพเดตฐานข้อมูลโดยอัตโนมัติ Kaspersky Anti-Virus 2011 จะมีฐานข้อมูลเป็นเวอร์ชั่นล่าสุด เมื่อการอัพเดตเสร็จสิ้น และข้อความจาก Windows Security Center จะหายไปเอง

ไวรัสคอมพิวเตอร์ในปัจจุบัน

1. ไวรัส Brontok

ลักษณะอาการ

- Menu Folder Option จะหายไป
- จะเกิดไฟล์ .exe ชื่อเหมือน Folder ในทุก Folder ที่เปิดเข้าไปดู
- มีหน้าเวปขึ้นมาเขียนว่า Brontok
- ไม่สามารถเรียกใช้ Registry Editor และFolder Option ได้

วิธีแก้ไข

1. หากมีคอมพิวเตอร์หลายเครื่องมีการแชร์ไดร์ฟ หรือแลนกันไว้ให้จัดการยกเลิกการแชร์ตัดการติดต่อกันเสียก่อน

2. เข้า Safe Mode (กด f8 รัวๆ ตอนรีบู๊ดเครื่อง) เลือกเข้าในฐานะของ Administrator

3. ไปที่ Run พิมพ์ msconfig กด OK เลือก Start up ยกเลิกเครื่องหมายหน้ารายการเหล่านี้ออกไป norBtok, smss

4. Restart เครื่องใหม่

5. โหลด File UnHookExec.inf จาก

http://securityresponse.symantec.com...UnHookExec.inf

6. เมื่อโหลดเสร็จให้ คลิกขวาที่ไฟล์ แล้วเลือก install

7. ไปที่ Run พิมพ์ regedit ไปที่ HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVe rsionPoliciesExplorer ลบค่า "NoFolderOptions" = "1

8. ไปที่%UserProfile%Local SettingsApplication Data ลบไฟล์ csrss.exe, inetinfo.exe, lsass.exe, services.exe, smss.exe, winlogon.exe ออกให้หมด

9. ไปที่ %UserProfile%Start MenuProgramsStartup ลบไฟล์ Empty.pif

10. ไปที่ %UserProfile%Templates ลบไฟล์ A.kotnorB.com

11. ไปที่ %Windir%inf ลบไฟล์ norBtok.exe

12. ไปที่%System% ลบไฟล์ 3D Animation.scr

2. ไวรัสคลิป VDO.EXE

เป็นไวรัสที่ไม่ได้สร้างความเสียหายร้ายแรงแก่ระบบเท่าใดแต่สร้างความรำคาญให้แก่ผู้ใช้ที่ติดไวรัสชนิดนี้มา โดยไวรัสชนิดนี้จะมีรูปร่างเหมือนโฟลเดอร์ที่อยู่ในวินโดว์สทั่วๆ ไป แต่จะมีนามสกุลเป็น .exe ทำให้เมื่อคลิกมันก็จะฝังตัวไว้ใน C:WINDOWSsystem32 โดยจะรันตัวมันเองขึ้นมาเรื่อยๆ และสร้างไฟล์ คลิป VDO.exe ขึ้นมาใหม่เรื่อยๆ แม้ว่าจะทำการลบไฟล์ คลิป VDO.exe แล้วก็ตาม

วิธีแก้ไขไวรัส

1. เข้า windows task manager โดยกด Ctrl + Alt + Del ไปที่แถบ processes หาไฟล์ที่ชื่อ soundmsg.exe จากนั้นก็จัดการ end progress โดยการคลิ้กขวาเลือก end process หรือกด delete แล้วตอบ yes ไป

2. ลบไฟล์ คลิปVDO.exe

3. ไปที่ C:windowssystem32 แล้วหาไฟล์ soundmsg.exe หรือ search หาไฟล์ soundmsg.exe

4. ไปที่ Start menu -> Run พิมพ์เข้า RegEdit เลือกที่ HK_Local_MachineSoftwareMicrosoftWindowsCu rrentVersionRun ลบค่า Registry ที่ชื่อ Virus test

5. ถ้าไวรัสติดที่ Handy drive ให้เข้า Save Mode ของ Windows แล้วเข้าไปลบไฟล์คลิป VDO.exe

3. Svchost.exe

เป็น Worm ชนิดหนึ่งที่สร้างชื่อเลียนแบบไฟล์ Svchost.exe ของระบบปฏิบัติการวินโดว์ส ซึ่งไฟล์ svchost.exe เป็นไฟล์ generic host process ใช้รัน กับ DLL ไฟล์เพื่อสร้าง Service ขึ้นมา เช่น EventSystem, Netman, NtmsSvc, RasMan โดยที่สามารถรันได้หลายๆ instance พร้อมกัน อีกชื่อหนึ่งที่ใช้คือ W32.CodeBlue ซึ่งส่งผลกระทบกับระบบปฏิบัติการวินโดว์สที่ใช้งานโปรแกรมประยุกต์ IIS

ขั้นตอนการทำงานของ W32.CodeBlue

1. เรียกใช้ไฟล์ Httpext.dll ในเครื่องผู้ถูกบุกรุกซึ่งอยู่ในโฟลเดอร์ C:Inetpubwwwrootscripts

2. ตัวหนอนจะเรียกใช้งานผ่านคำสั่ง HTTP GET

3. หลังจากนั้นตัวหนอนจะสร้างไฟล์ C:Svchost.exe และเรียกใช้งาน

4. C:Svchost.exe จะสร้างและแก้ไขส่วนต่างๆ ของระบบ W32.CodeBlue ดังนี้

- สร้างไฟล์ C:Svchost.exe และแก้ไข registry ดังนี้ HKEY_LOCAL_MACHINESoftwareMicrosoft WindowsCurrentVersionRun ซึ่งจะอนุญาตให้เรียกใช้งานตัวหนอนหลังจาก restart เครื่องทุกครั้ง

- สร้างไฟล์ชั่วคราวที่ C:d.vbs ซึ่งไฟล์นี้เป็นไฟล์ที่ถูกเรียกจากโปรแกรม C:WINNTsystem32Wscript.exe

- ไฟล์ d.vbs จะลบไฟล์ .ida, .idq และ .printer IIS service เพื่อไม่ให้มีการติดเชื้อจาก CodeRed

- ในช่วงเวลา 10 นาฬิกาและ 11 นาฬิกา ตัวหนอนจะส่ง mail ที่มีข้อมูลขนาดใหญ่ไปยังเว็บไซต์บริษัทในเมืองจีน

วิธีตรวจสอบ

- ใน Drive C หรือ D จะมี Folder ที่ชื่อ d และใน Folder ที่ชื่อ d นั้นจะมี Folder ต่างๆ เช่น c, cpu, n, w และอื่นๆ

- ไฟล์ Svchost.exe ของระบบจะอยู่ใน C:WINDOWSsystem32 เท่านั้น ไฟล์ที่เป็นไวรัสส่วนใหญ่จะอยู่ใน C:Svchost.exe หรือ C:WINDOWSSvchost.exe

วิธีแก้ไข

1. ไปที่ Start Menu เลือก Run พิมพ์ regedit คลิก OK ไปที่ HKEY_LOCAL_MACHINESoftwareMicrosoft WindowsCurrentVersionRun

2. ฝั่งขวาของข้อความจะแสดงค่า C:svchost.exe ให้ลบข้อความทางฝั่งขวามือและออกจากโปรแกรม

3. ค้นหาและลบไฟล์ C:svchost.exe และ C:d.vbs Flashy.exe

ลักษณะอาการ

- ไม่สามารถเรียกใช้ Task Manager, Registry Editor และ Folder Option ได้

- หากพยายามแก้ไขด้วยวิธีการทำ System Restore ถ้าเครื่องที่ได้ตั้งรหัสเอาไว้ Flashy.exe จะแก้รหัสทำให้ไม่สามารถ Login เข้าเครื่องนั้นได้อีกเลย

- Error นี้จะแสดงขึ้นมาทันทีเมื่อ ตรวจพบการใช้งาน Controller ของ Removeble Media ต่างๆ

- โดยปกติไม่มีอะไรเกิดขึ้น แต่เมื่อเสียบ Card Reader เข้าไปก็จะโชว์ Error ทันที เมื่อเสียบ Flash Drive เข้าไปหรือเสียบ Memory Card เข้าไปใน Card Reader แล้ว

- หากว่าใน Memory Card หรือ Flash Drive มี Aplication อยู่ (นามสกุล .exe) Flashy.exe จะปลอมชื่อตัวเองไปเป็นชื่อเดียวกัน Aplication นั้นๆ ทำให้เข้าใจว่า Aplication นั้นกำลังถูกเรียกใช้งานอยู่ตามปกติ Flashy.exe จะเขียนค่าลงใน Memory Card และทำให้ตัวเองมีหน้าตาเหมือน Folder และเมื่อเอาไปใช้ที่ เครื่องอื่นจะมองเห็นเป็น Folder ทำให้ผู้ใช้ ไม่ทันระวังตัวพอดับเบิ้ลคลิกไปก็เท่ากับเป็นการรัน Virus เข้าเครื่องในทันที

- Virus ตัวนี้ไม่แพร่กระจายในเครือข่าย (คือไม่ใช่ อยู่ๆ ก็ไปเขียนค่าหรือติดตั้งตัวเองในเครื่องอื่นๆ ในวง Lan ของเรา มันจะอยู่แต่เครื่องที่มันอยู่เท่านั้น แต่ใช้ Flash Drive เป็นพาหะแทน)

- อาการจะแสดงผลในทันทีโดยไม่รีรอ

วิธีแก้ไข

1. ให้ใส่รหัสผ่าน คือ hacked

2. เข้าไปที่ Task Manager เลือก Processes หาชื่อ Flashy.exe และ systemID.pif เลือก End Process

3. เนื่องจาก ไม่สามารถเข้าไปแก้ไขค่า Registry ใน Run > regedit ได้ จึงต้องสร้างไฟล์เพื่อปลดล็อค regedit โดยการสร้าง Notepad แล้วพิมพ์ดังนี้ โดย File สามารถใช้ปลดล็อคได้กับทุกกรณีที่มีการล็อค regedit ที่เกิดจากไวรัสตัวอื่นๆ เมื่อพิมพ์เสร็จก็ให้ save เป็นนามสกุล .inf หรือ

ดาวน์โหลดโดยคลิ๊กที่ Link http://securityresponse.symantec.com...UnHookExec.inf เมื่อสร้าง หรือ Download เสร็จ ให้คลิกขวาแล้วเลือก install

4. ไปที่ Run พิมพ์ regedit แล้วให้ลบไฟล์ใน regedit ดังนี้

- HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion PoliciesExplorer ลบ "NoFolderOptions" = "1“

- HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion ExplorerAdvanced ลบ "HideFileExt" = "1"

- HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersion ExplorerAdvanced ลบ "Hidden" = "2"

- HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices SharedAccess ลบ "Start" = "4"

- HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentV ersion Run ลบ Flashy.exe

5. ไปที่Start MenuProgramsStartup ลบ systemID.pif

6. ไปที่ Run พิมพ์ msconfig เลือก start up เอาเครื่องหมายถูกหน้า systemID ออก

7. ไปที่Run พิมพ์ regedit แล้วไปที่HKEY_LOCAL_MACHINE SOFTWAREMicrosoftWindows NTCurrentVersionWinlogon โดยแก้ค่า Registry ดังนี้ (ถ้าไม่มีก็คลิกขาวเลือก New เลือก String value) "AutoAdminLogon"="1" "DefaultUserName"=“ชื่อผู้ใช้" "DefaultPassword"hacked"

8. เปิด Show hidden File แล้วไปที่ C:WINDOWSsystem32 ลบ File ชื่อ Flashy.exe

9. หาแผ่น Hirens BootCD 8.1 โดยการโหลดจาก http://files.9down.com:8080/HBCD81%5...own.com%5D.rar เขียนลงแผ่น CD แล้วทำการ Boot เครื่องด้วย CD ให้เลือกหัวข้อ Password ข้อ 1. แล้วเลือก patition เลือก Account ที่จะล้าง Password และ ออกจากโปรแกรม

4. Toy.exe

ลักษณะอาการ

1. เมื่อเปิดเครื่องขึ้นมาหน้า Desktop จะมีภาษาจีนและภาษาอังกฤษขึ้นมา

2. ไม่สามารถเข้า Local Disk ต่างๆ ได้ตามปกติรวมถึง Flash Drive ด้วยโดยจะดับเบิ้ลคลิกเข้า Drive ต่างๆ โดยตรงไม่ได้ ต้องคลิกขวาแล้ว Open หรือ Explore เท่านั้น

วิธีแก้ไข

1. เข้าไปที่ C:Document and Setting ชื่อ User Start Menu Program Startup และ C:WINDOWSSYSTEM32 ลบไฟล์ที่ชื่อ mslogon

2. Restart เครื่อง

5. Windows Genuine

เนื่องจากบริษัท Microsoft ได้ตรวจสอบลิขสิทธิ์ Windows XP ทำให้ต้อง Format Harddisk ใหม่ทั้งหมด ผ่านทาง Windows Update ปัญหานี้เกิดจากตัวอัพเดตที่มีรหัส KB890859 ทำให้ user mode ของWindows เกิดปัญหา โดยเริ่มจาก Microsoft เข้ามาเตือนว่า Update พร้อมสำหรับโหลดแล้ว (สำหรับผู้ที่ตั้งเป็น Notify me but don't download) เมื่อการอัพเดตเสร็จสมบูรณ์ Product Key จะถูกส่งไปยัง Microsoft Server เพื่อดูว่าผิดลิขสิทธิ์หรือไม่ หากผิด เมื่อเครื่องคุณนั้นรีสตาร์ทแล้วจะไม่สามารถ Logon ได้จะมีหน้าจอสีฟ้า เกิดจากการแก้ไขไฟล์ในระดับ kernel ทำให้เกิด c000021a fatal error

วิธีแก้ไข

วิธีที่ 1 เข้า recovery console ของวินโดว์ส

1. Set Bios ให้เครื่องบูตจากซีดีรอม โดยใส่แผ่น setup ของ Windows XP เอาไว้

2. เมื่อเครื่องบูตจนถึงหน้าที่ให้เลือกเซ็ตอัพให้กด r เพื่อเข้าสู่ recovery console

3. เมื่อเข้าสู่ recovery console จะเป็นจอสีดำคล้าย DOS จะถามว่าต้องการทำงานกับไดรฟ์ไหน โดยจะมีรายการขึ้นมาให้กดตัวเลขเลือก เช่น [1]C:WINDOWS ถ้าจะทำงานกับไดรฟ์นี้ก็กด 1 แล้วกด enter

4. ให้ใส่ Password ลงไป ถ้าไม่มีก็กด enter ผ่านไป แล้วก็จะขึ้น C:WINDOWS>

5. ให้เข้าไปในโฟลเดอร์ชื่อ $NtUninstallKB890859$ โดยพิมพ์ cd$NtUninstallKB890859$ แล้วกด enter ที่หน้าจอจะขึ้น C:WINDOWS$NtUninstallKB890859$>

6. พิมพ์ dir แล้วกด enter จะมีรายชื่อไฟล์ขึ้นมาให้ copy ไฟล์ authz.dll, user32.dll, winsrv.dll, ntkrnlpa.exe, ntoskrnl.exe และ win32k.sys ไปไว้ที่ C:WINDOWSSYSTEM32

7. พิมพ์ copy authz.dll c:windowssystem32 แล้วกด enter จะถามว่าจะให้ overwrite ทับไฟล์ที่มีอยู่แล้วหรือไม่ ให้ตอบ yes โดยกด y ทำแบบนี้จนครบทุกไฟล์คือ พิมพ์ copy ชื่อไฟล์ c:windowssystem32 เมื่อทำครบหมดทุกไฟล์แล้วให้พิมพ์ exit แล้วกด enter เครื่องจะรีสตาร์ทเอง

วิธีที่ 2

1. เปิด Windows Task Manager

2. กด End process wgatray.exe ใน Task Manager

3. Restart Windows XP แล้วเข้า Safe Mode

4. ลบFile WgaTray.exe จาก c:WindowsSystem32

5. ลบFile WgaTray.exe จาก c:WindowsSystem32dllcache

6. ไปที่ Run พิมพ์ RegEdit

7. ไปที่ HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsN T CurrentVersionWinlogonNotify

8. ลบ folder ‘WgaLogon’ และทุก File

9. Reboot Windows XP.

6. ไวรัส Godzila

ลักษณะอาการ

1. เครื่องจะไม่สามารถ Double Click เปิดไดร์ฟต่างๆ ได้ แต่จะคลิกเมาส์ขวาเพื่อเปิดไดร์ฟโดยเลือกเมนู Open หรือ Explore

2. มีข้อความปรากฏบน Title Bar ของ Internet Explorer ว่า “Hacked By Godzilla”

วิธีการแก้ไข

1. Double Click ไอคอน My Computer ที่ Desktop เลือกเมนู Tools --> Folder Options

2. ปรากฏไดอะล็อก Folder Options คลิกแท็บ View

1) คลิกเลือก Show Hidden files and folders

2) เอาเครื่องหมาย/ในช่องสี่เหลี่ยมหน้า Hide extention... และ Hide protected operating system file ออก

3) คลิก OK

3. กดปุ่ม Ctrl + Alt + Delete ที่คีย์บอร์ด

4. ปรากฏไดอะล็อกบ็อก Windows Task Manager คลิกเลือกแท็บ Processes

1) คลิกเลือกเมนู Image Name (เพื่อ sort File)

2) คลิกเลือกไฟล์ wscript.exe

3) คลิกปุ่ม End Process

5. เปิดไดร์ฟ (โดยคลิกเม้าส์ขวาเลือก Explore ห้าม Double Click ไดร์ฟ) ทำการลบไฟล์ autorun.inf และ MS32DLL.dll.vbs ออก (โดยกด Shift+Delete) ทุกไดร์ฟที่มีอยู่ในเครื่องคอมพิวเตอร์ซึ่งรวมทั้ง Handy Drive ด้วย

6. เปิดโฟลเดอร์ C:WINDOWS เพื่อลบไฟล์ MS32DLL.dll.vbs ออก (โดยกด Shift+Delete)

7. ไปที่ปุ่ม Start --> Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่ง regedit กดปุ่ม OK ปรากฏไดอะล็อกบ็อก Registry Edit

8. คลิกเลือก HKEY_LOCAL_MACHINE --> Software --> Microsoft --> windows --> Current Version --> Run เพื่อลบไฟล์ MS32DLL (โดยการกดปุ่ม Delete ที่คีย์บอร์ด)

9. คลิกเลือก HKEY_CURRENT_USER --> Software --> Microsoft --> Internet Explorer --> Main เพื่อลบไฟล์ที่ Window Title “Hacked by Godzilla” ออก (โดยการกดปุ่ม Delete ที่คีย์บอร์ด)

10. คลิกปุ่ม Start --> Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่ง gpedit.msc กดปุ่ม OK ปรากฏไดอะล็อกบ็อก Group Policy

11. คลิกเลือก User Configuration --> Administrative Templates --> System --> Double Click ไฟล์ Turn Off Autoplay ปรากกฏไดอะล็อกบ็อก Turn Off Autoplay Properties

1) คลิกเลือก Enabled

2) คลิกเลือก All drives

3) คลิก OK เพื่อป้องกันการเปิดไดร์ฟอัตโนมัติในกรณีที่นำแผ่นซีดีหรือแฮนดี้ไดร์ฟมาใช้งานซึ่งเป็นช่องทางที่จะทำให้เกิดการติดไวรัสได้ง่ายขึ้น

12. Double Click ไอคอน Mycomputer ที่ Desktop เลือกเมนู Tools --> Folder Options

13. ปรากฏไดอะล็อก Folder Options คลิกแท็บ View

1) คลิก/ในช่องวงกลม เลือก Donot show hidden file and folders

2) คลิก OK แล้วลองรีสตาร์ทเครื่องดูว่ายังเป็นอยู่ไหม

7. ไวรัส AdobeR.exe Win32/RJump.A

ลักษณะอาการ เป็นไวรัสที่ติดจากแฮนดี้ไดร์ฟ ควรป้องกันไม่ให้แฮนดี้ไดร์ฟเปิดเองโดยอัตโนมัติ เพราะเวลาที่เสียบแฮนดี้ไดร์ฟเข้าเครื่องคอมพิวเตอร์ ก็จะเด้งขึ้นมาโดยอัตโนมัติ และถามว่าจะเปิดด้วยโปรแกรมอะไร หากในแฮนดี้ไดร์ฟนั้นมีไฟล์ Autorun.inf อยู่ มันก็จะเปิดตามคำสั่งที่อยู่ในไฟล์ Autorun.inf โดยอัตโนมัต ซึ่งแล้วแต่ไวรัสว่าจะเขียนคำสั่งให้รันตัวไหนขึ้นมาไฟล์ Autorun.inf สามารถเปิดอ่านได้โดยดับเบิ้ลคลิกได้เลยไม่เป็นอันตราย

วิธีการแก้ไข

วิธีปิดไม่ให้แฮนดี้ไดว์ฟเปิดเองอัตโนมัติ

1. Start ----> Run ----> gpedit.msc ----> Computer

2. Configuration ---> Administrative Templetes ----> system ---> ดูในช่องขวามือดับเบิ้ลคลิกคำว่า Turn Off Auto play เลือกเป็น Enabled ในช่อง Turn Off Auto playon = All drives กด OK แล้วเวลาเสียบแฮนดี้ไดร์ฟเข้า My computer เพื่อความปลอดภัยไม่ควรไปดับเบิ้ลคลิกแฮนดี้ไดร์ฟ ควรคลิกขวาดูว่ามีคำว่า Auto หรือ Auto run ไหม หากมีแสดงว่ามีไวรัส ให้เลือก Open แล้วไปลบไฟล์โดย ไปที่ My computer --> Tools --> Folder options --> View --> หัวข้อ Hiden files and folder ใต้นั้นให้ติ๊กเลือก Show hiden file and folder แล้วติ๊กถูกสองบรรทัดล่างออก แล้ว OK คลิกขวาที่แฮนดี้ไดร์ฟ เลือก Open แล้วลบไฟล์ Autorun.inf

Adober.exe msvcr71.dll ravmonlog สังเกตง่ายมันจะจางๆ หากลบไม่ได้แสดงว่าไวรัสทำงานอยู่ นั่นหมายความว่า หากเผลอดับเบิ้ลคลิกแฮนดี้ไดร์ฟ ให้กด Ctrl + Alt + Delete โปรแกรม Task Manager จะขึ้นมา และเลือกในแถบ Processes หาโปรแกรมที่ชื่อว่า AdobeR.exe หลังจากนั้นกด End Task แล้วกด OK แล้วก็ไปลบไฟล์ AdobeR.exe ใน C:WINDOWS แล้วก็ไปลบคำสั่งใน registry โดย Start ---> Run ---> regedit --> HKEY_LOCAL_MACHINE /Software /Microsoft /Windows / CurrentVersion/Run มองทางขวามือลบ DWORD ชื่อว่า RAVD แล้วก็ปิด

ไวรัสคอมพิวเตอร์กับการใช้งาน Flash drive

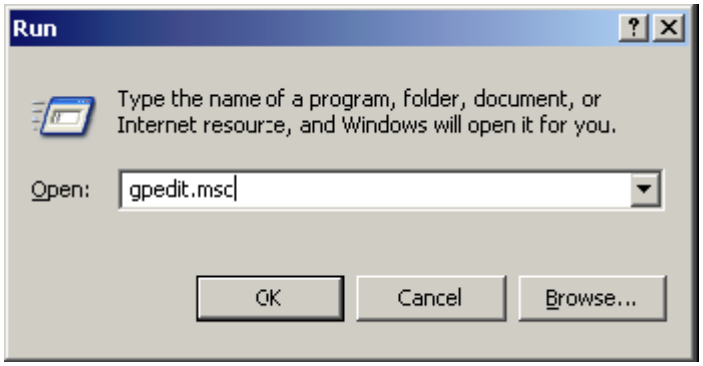
วิธีป้องกันคอมพิวเตอร์จาก Flash drive ที่ติดไวรัส

1. วิธีการปิดการทำงานอัตโนมัติของอุปกรณ์ USB Flash Disk

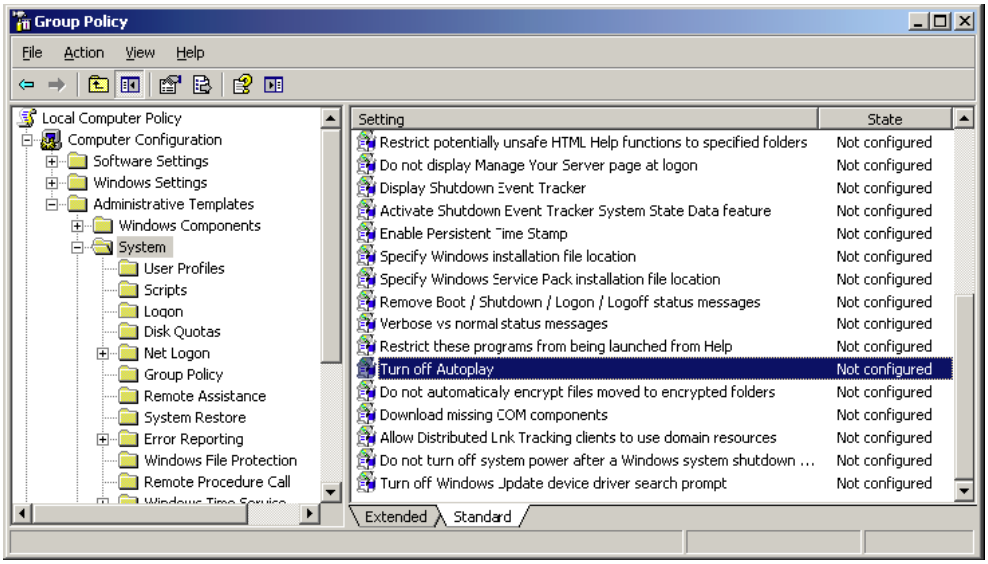
เครื่องคอมพิวเตอร์เกือบทั้ง หมดที่ใช้ระบบปฏิบัติการ Windows 98, ME, XP, 2000, 2003 หรือใหม่กว่า มักจะอนุญาตให้เรียกใช้โปรแกรมโดยอัตโนมัติเมื่อนำอุปกรณ์ USB Flash Disk มาต่อเชื่อมกับคอมพิวเตอร์ ซึ่งผลเสียที่ตามมาคือ การเรียกโปรแกรมที่อาจเป็นไวรัสให้ทำงานโดยไม่รู้ตัว วิธีที่ดีที่สุดและได้ผลตรงประเด็นคือ การปิดการทำงานอัตโนมัติดังกล่าวเสีย ซึ่งสามารถทำได้หลายวิธี ด้วยกันดังนี้

1.1 ปิดด้วย GPEDIT

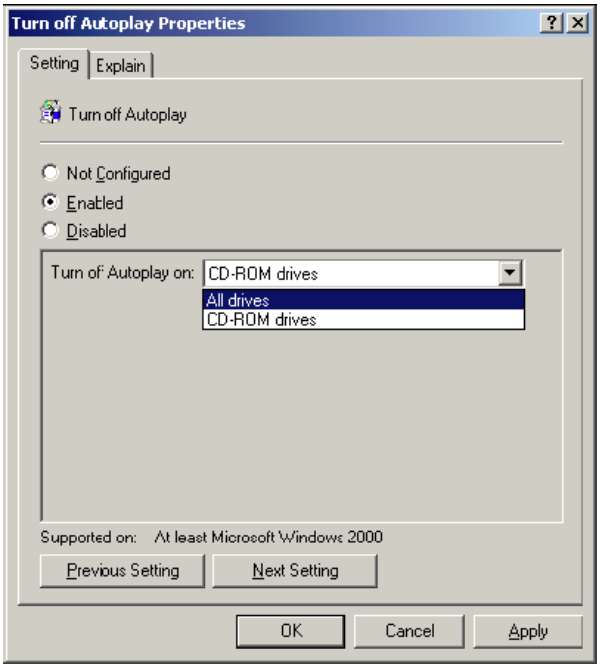
- คลิกที่ปุ่มเมนู Start -> Run
- พิมพ์คำสั่ง gpedit.msc



- ที่หน้าต่าง Group Policy สังเกตที่ด้านซ้าย แล้วเลือกไปที่เมนู Computer Configuration -> Administrative Templates -> System



• ดับเบิลคลิกที่ Turn off Autoplay เพื่อเข้าสู่หน้าต่าง Turn off Autoplay properties และเลือก Enable จากนั้น ในกรอบที่อยู่ด้านล่าง หัวข้อ Turn off Autoplay On: แล้วจึงเลือกเป็น All Drive



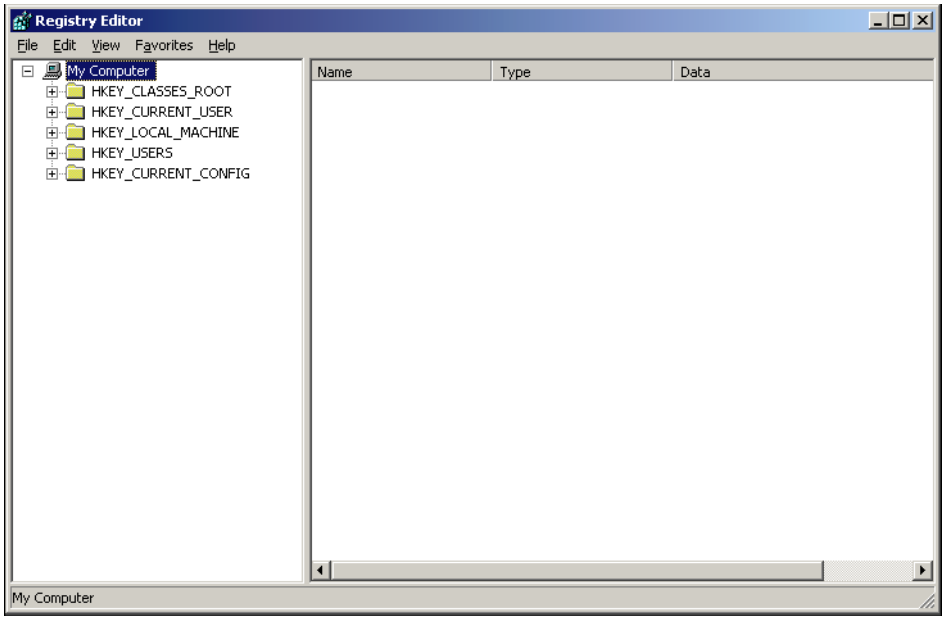
• จากนั้น คลิกปุ่ม OK แล้วปิดหน้าต่างของ Group Policy Editor

1.2. ปิดด้วย registry

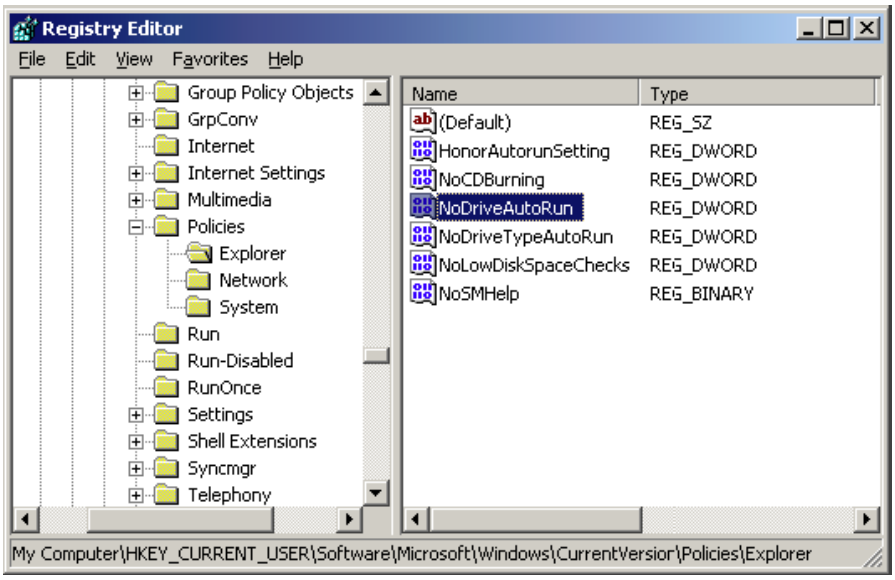
วิธีนี้ค่อนข้างยุ่งยากและมีความเสี่ยงหากเกิดความผิดพลาดในขั้นตอนการทำ จึงควรดำเนินขั้นตอนต่างๆ อย่างรอบคอบรัดกุม

• คลิกที่ ปุ่มเมนู Start -> Run

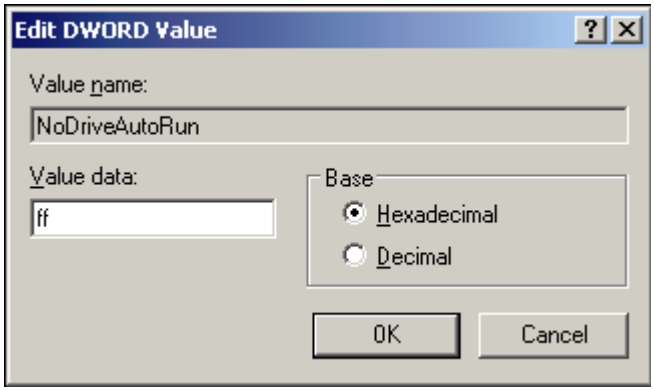
• พิมพ์คำสั่ง regedit จะปรากฏหน้าต่าง Registry Edit ดังรูป



HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer



• ดับเบิลคลิกที่ key “NoDriveAutoRun” เพื่อกรอกค่า ff (เลขฐานสิบหก)



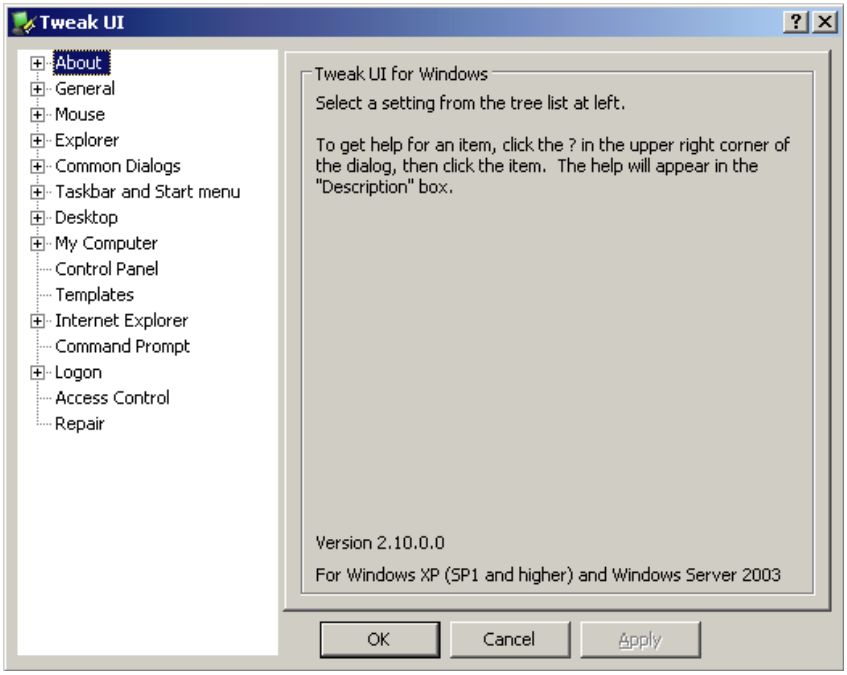
• คลิก OK และปิดหน้าต่างโปรแกรม Registry Editor จากนั้นจึงรีสตาร์ทวินโดว์สเพื่อทดลองผล

1.3 ปิดโดยใช้โปรแกรม TweakUI

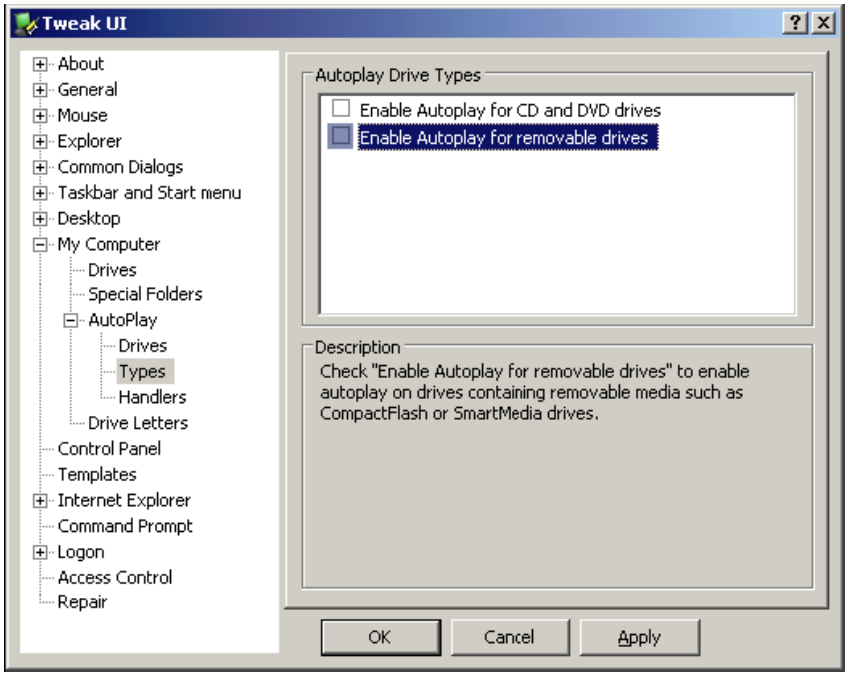
โปรแกรม TweakUI เป็นโปรแกรมที่ทางบริษัท Microsoft ได้เผยแพร่ให้สามารถ download ใช้งานได้ฟรี และใช้งานได้ไม่ยาก ทำความเข้าใจได้ง่ายกว่ามาก ตัว TweakUI เองได้รวมวิธีการปรับแต่ง Windows อย่างง่ายๆ ไว้มากมาย หนึ่งในนั้นคือ ความสามารถในการปิดการทำงานแบบอัตโนมัติเมื่อใส่แผ่นซีดีและอุปกรณ์ USB Flash Disk ด้วย ซึ่งการใช้โปรแกรม TweakUI จะช่วยลดขั้นตอนที่ยุ่งยากได้มากและมีความเสี่ยงต่อความผิดพลาดได้น้อยกว่าสองวิธีข้างต้น สำหรับขั้นตอนในการปิดการทำงานแบบอัตโนมัติ มีดังนี้

• คลิกที่เมนู Start -> Program -> Power Toys For Windows XP

• เลือก TweakUI จะปรากฏหน้าต่าง TweakUI ขึ้นมา



• ที่ panel ด้านซ้ายมือ เลือก My Computer-> AutoPlay-> Types ที่ด้านขวามือจะปรากฏกรอบ Autoplay Drive Types ให้คลิกซ้ำเพื่อไม่เลือก Enable Autoplay for CDand DVD Drives ถ้าไม่ต้องการให้แผ่น CD DVD ทำงานแบบอัตโนมัติเมื่อใส่แผ่น Enable Autoplay for removable drives ถ้าไม่ต้องการให้อุปกรณ์ USB Flash Diskทำงานโดยอัตโนมัติเมื่อใส่แผ่น



• จากนั้นกดปุ่ม OK เพื่อปิดหน้าต่างนี้

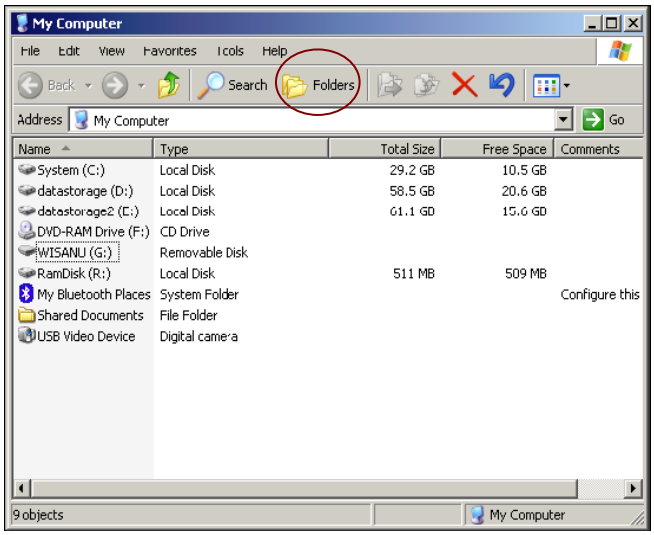
2. ห้ามดับเบิ้ลคลิก Flash Drive

ห้ามดับเบิ้ลคลิก Flash Drive เพื่อเปิดดูข้อมูล หรือดับเบิ้ลคลิกไฟล์แปลกๆ หรือโฟลเดอร์ที่อยู่ๆ ก็ปรากฏให้เห็น เช่น Folder.exe หรือไฟล์ที่ชื่อเหมือนโฟล์เดอร์ที่มีอยู่แล้วตามด้วย .exe วิธีเปิดให้คลิกขวา Open หรือ Explorer จะปลอดภัยมากกว่า

วิธีการเปิด flash drive ด้วย explorer ให้ปลอดภัย

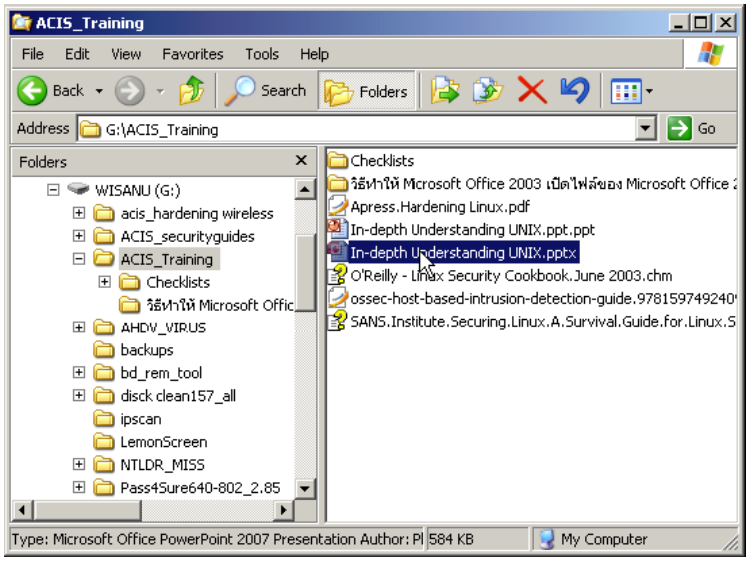
ในบางครั้ง หากมีความจำเป็นจะต้องใช้งาน USB Flash Disk ของคนอื่นกับเครื่องคอมพิวเตอร์ของเรา และไม่สามารถที่ตรวจจับไวรัสที่อาจมีอยู่ในอุปกรณ์ USB Flash Disk ด้วยโปรแกรมใดๆ ได้ ยังมีอีกวิธีหนึ่งที่จะสามารถเลี่ยงการติดไวรัสจากอุปกรณ์ USB Flash Disk ที่ไม่น่าไว้วางใจนั้นได้ ดังนี้

1. เมื่อต่อเชื่อมอุปกรณ์ USB Flash Disk กับเครื่องคอมพิวเตอร์แล้ว ให้ดับเบิ้ลคลิกที่ My Computer



2. คลิกที่ปุ่ม Folder ที่อยู่ด้านบน จะปรากฏ panel ด้านซ้ายมือขึ้นมา

3. ที่ panel ด้านซ้ายมือจะแสดงชื่อไดร์ฟ และ folder ย่อยๆ ลงไปตามลำดับ และด้านขวามือจะแสดง folder ย่อย ที่อยู่ภายใต้ไดร์ฟและ folder ที่เราเลือกด้านซ้ายมือ



4. ให้ใช้วิธีการเลือก ไดร์ฟหรือ folder ย่อยที่ด้านซ้ายมือ แทนการดับเบิ้ลคลิกที่ไดร์ฟหรือ folderที่ panel ด้านขวามือ โดยจะดับเบิลคลิกใน panel ด้านขวามือก็ต่อเมื่อพบไฟล์ที่ต้องการแล้วจริงๆ ซึ่งวิธีนี้จะเลี่ยงการเผลอดับเบิลคลิกเพื่อเรียกให้ไวรัสทำงานโดยไม่ได้ตั้งใจได้

วิธีการตรวจจับไวรัสก่อนการใช้งาน

1. ตรวจจับไวรัสด้วยโปรแกรมป้องกัน autorun.inf

อีกสิ่งหนึ่งนอกเหนือจากที่กล่าวมาในข้างต้น หากจำเป็นต้องเชื่อมต่ออุปกรณ์ USB FlashDisk แล้วผู้ใช้ควรติดตั้งโปรแกรมที่ทำหน้าที่ตรวจจับไวรัสหรือเตือนกรณีที่มีไวรัสฝังตัวอยู่ในอุปกรณ์ โปรแกรมตัวหนึ่งที่ขอแนะนำคือ USB 1.3 ซึ่งคอยทำหน้าที่ตรวจหาไฟล์ที่ชื่อ autorun.inf ที่ไวรัสส่วนใหญ่นิยมฝังตัวไฟล์นี้ไว้เพื่อให้ผู้ใช้เรียกไวรัสโดยไม่รู้ตัว โปรแกรม USB เป็นโปรแกรมที่ใช้งานง่าย ไม่รบกวนผู้ใช้ สามารถหา download ได้ที่ www.sputnik70.narod.ru ส่วนวิธีการใช้งานง่ายๆ มีดังนี้

1. เมื่อ download ไฟล์มาแล้ว ให้คลาย zip ไฟล์ เก็บไว้ใน folder ชื่อ USB เช่น C:\USB

2. เรียกใช้ไฟล์ชื่อ USB.exe จะปรากฏไอคอนที่ system tray

3. คลิกเมาส์ปุ่มขวาที่ไอคอน เลือกเมนู Setting-> Autostart เพื่อให้โปรแกรมทำงานทันทีที่เปิดเครื่องคอมพิวเตอร์

4. คลิกเมาส์ปุ่มขวาอีกครั้ง ที่ไอคอนเดิม เลือกเมนู Action-> Disable Autorun for all system driveเพื่อให้โปรแกรมยกเลิกการทำงานแบบอัตโนมัติทั้งหมดของทั้ง USB Flash Drive และ CD/DVD Drive

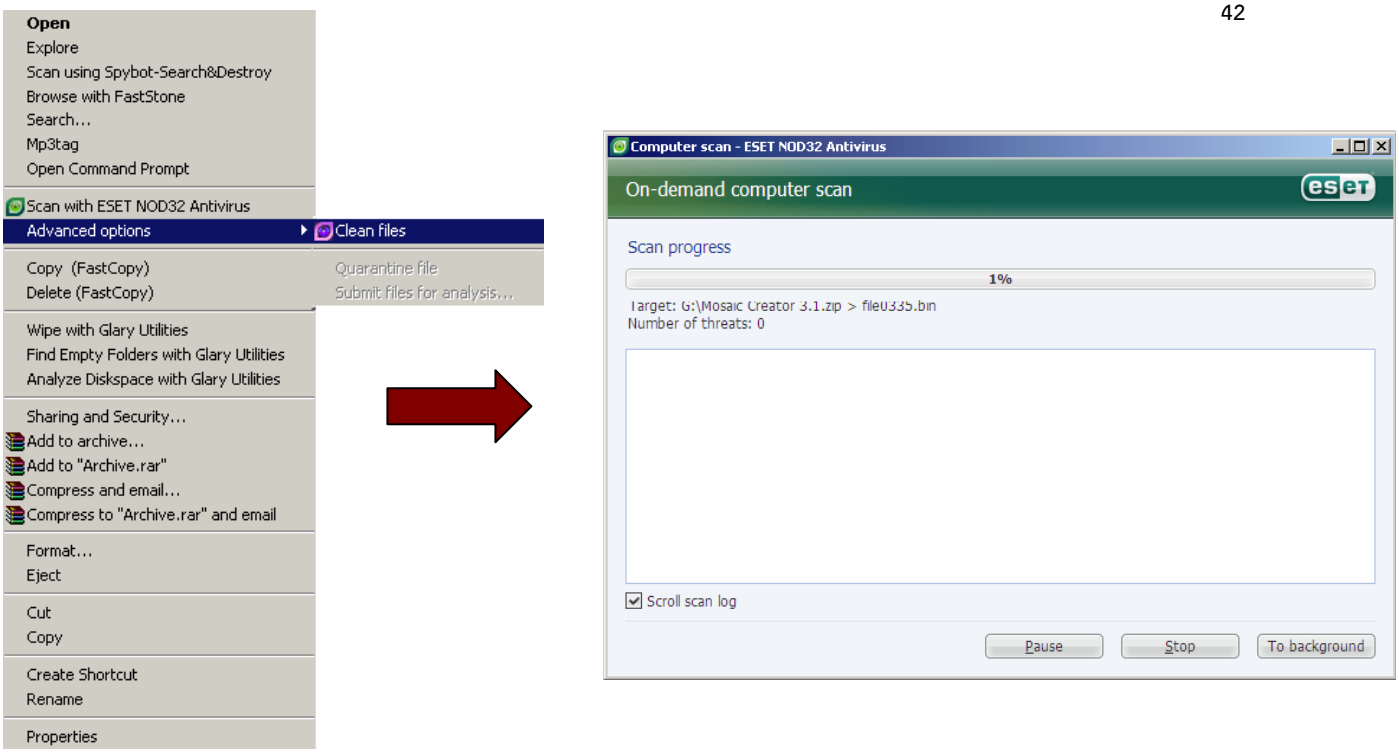
2. ตรวจจับไวรัสที่แฝงมากับอุปกรณ์ USB Flash Disk ด้วยโปรแกรมตรวจจับไวรัส

การป้องกันด้วยวิธีปิดการทำงานอัตโนมัติด้วยวิธีต่างๆ ที่กล่าวมาข้างต้น ก็เป็นขั้น ตอนที่ช่วยเสริมไม่ให้ไวรัสเข้ามาก่อความเสียหายให้แก่ระบบของเรา แต่ถ้าการแพร่ระบาดของไวรัสและความซับซ้อนมากขึ้นยังมีอยู่อย่างต่อเนื่อง ผู้ใช้ก็จำเป็นจะต้องพึ่งพาเครื่องมืออย่างโปรแกรมตรวจจับและป้องกันไวรัสเข้ามาช่วยเหลือ เพื่อเพิ่มความรัดกุมให้กับการป้องกันตัวจากภัยของไวรัส การใช้งานโปรแกรมตรวจจับไวรัสเพื่อตรวจหาไวรัสที่แฝงตัวมากับอุปกรณ์ USB Flash Disk นั้น มีขั้นตอนและวิธีการที่แตกต่างกันไปตามแต่ผู้ผลิตจะกำหนด ดังนั้น จึงขอยกตัวอย่างโปรแกรมที่ได้รับความนิยมตัวหนึ่ง นั่นคือ NOD32 โดยขั้นตอนการใช้งานก็ไม่ยุ่งยากนัก คือ

1. เมื่อเชื่อมต่ออุปกรณ์ USB Flash Disk เข้ากับคอมพิวเตอร์แล้ว ให้ดับเบิลคลิกที่ My Computer

2. คลิกเมาส์ปุ่มขวาเพื่อเลือกเมนู Advanced options->Clean Files

3. จากนั้น จะปรากฏหน้าต่าง ของโปรแกรม NOD32 และจะตรวจจับไวรัสโดยอัตโนมัติ



วิธีการใช้ Flash drive อย่างปลอดภัย

1. ให้คิดเสมอว่า Flash Drive ไม่ว่าจะของใครก็ตามไม่ปลอดภัย และอาจแพร่กระจายไวรัสมาสู่เราได้ทุกเมื่อ

2. หมั่น update โปรแกรมตรวจจับไวรัสให้ทันสมัยเสมอ รองรับไวรัสใหม่ๆ ที่แพร่ระบาดอยู่ในปัจุบัน

3. พยายามไม่อนุญาตให้ผู้อื่นเข้ามาใช้เครื่องคอมพิวเตอร์ของเราโดยไม่ที่เราไม่ได้รับรู้ และต้องบังคับให้ผู้ที่จะเข้ามาใช้เครื่องคอมพิวเตอร์ของเราร่วมกับอุปกรณ์ USB Flash Disk ต้อง scan virus ด้วยโปรแกรมตรวจจับไวรัสก่อนเสมอ

4. หมั่น scan virus ของเครื่องเราเองเป็นประจำ เพื่อให้มั่นใจว่าเครื่องของเราก็จะไม่เป็นแหล่งแพร่ระบาดของไวรัสไปสู่ภายนอกเช่นกัน

5. หมั่น สังเกตความเปลี่ยนแปลงและจดบันทึกความผิดปกติใดๆ ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ของเรา เพราะหากเป็นอาการของไวรัส จะได้สามารถนำข้อมูลที่จดบันทึกไปเป็นเบาะแสในการระวังและป้องกันปัญหาที่เกิดจากไวรัสได้ในคราวต่อๆ ไป

6. ควรจดจำและปฏิบัติตามวิธีหลีกเลี่ยงไวรัสที่เกิดจาก USB Flash Disk จนเป็นนิสัย เพราะจะช่วยให้เครื่องคอมพิวเตอร์ปราศจากไวรัส และลดการแพร่ระบาดของไวรัสในวงกว้างได้อีกด้วย

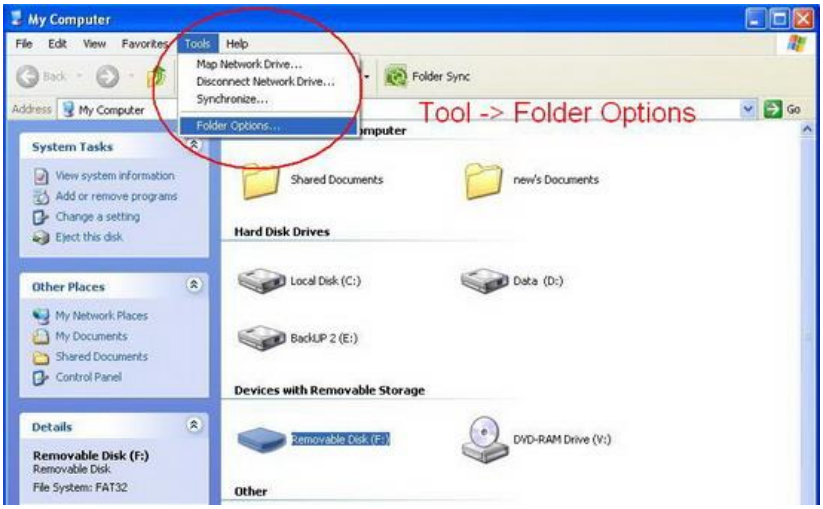
7. ติดตามข่าวสารการแพร่ระบาดของไวรัสอย่างต่อเนื่อง เพื่อที่จะได้รู้เท่าทันปัญหาไวรัสก่อนปัญหาจะมาถึง

วิธีการกู้คืนข้อมูลที่สูญหายจาก Flash drive

1. ก่อนเสียบ Card Reader หรือ Flash Drive ให้กดปุ่ม Shift ค้างไว้ แล้วค่อยเสียบ Flash Drive เข้า เพื่อป้องกันไม่ให้ Auto Run ทำงาน

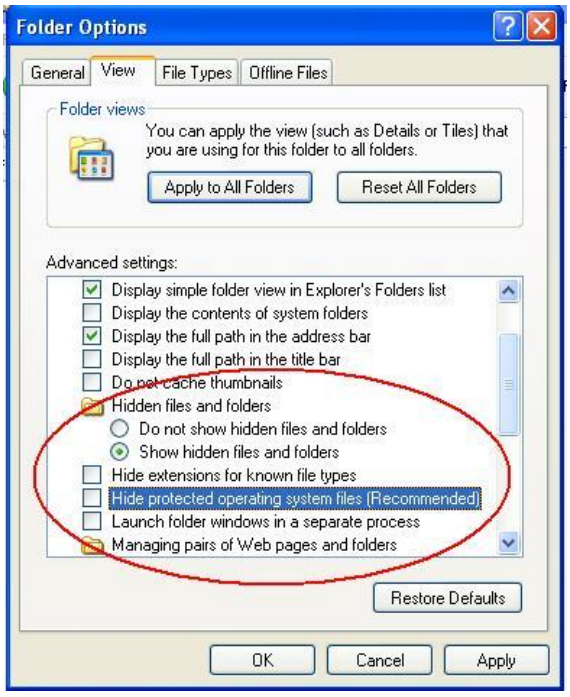
2. ที่ My Computer คลิ๊กขวา เลือก Drive ที่ต่อเข้าคอมพิวเตอร์

3.ไปที่เมนู Tools เลือก Folder Option



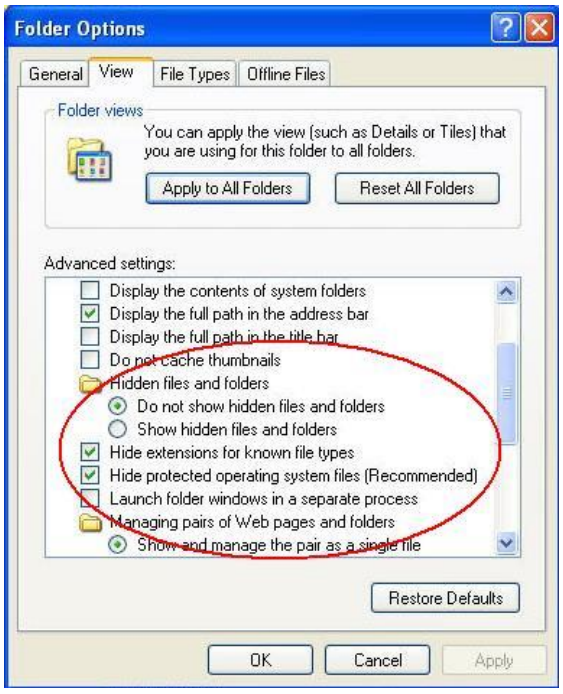
4. เลือก Tab หัวข้อ View

5. เลือก Show hidden files and folders ปลด Hide extensions for known file types ออก ปลด Hide protected operating system files ออก (มีแจ้งเตือน ให้ตอบ Yes) จากนั้น กด Apply และ กด OK



5. เข้าไปดูใน Flash Drive Folder ต่าง ๆจะกลับมาแล้ว จากนั้น ก็ลบไฟล์ที่เป็น ShortCut นามสกุล exe ที่เป็นไฟล์ไวรัส รวมทั้งไฟล์ autorun.inf ทิ้งให้หมด

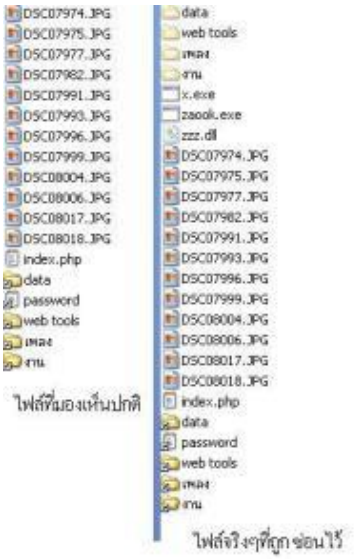
6. หลังจากนั้น ก็ให้ Hidden files and folder ตามเดิม



ไวรัสคอมพิวเตอร์ที่ติดจาก Flash Drive

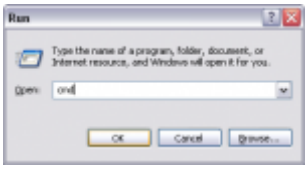
ไวรัส shortcut

หลายคนคงเคยเจอกับปัญหาแบบนี้ที่อยู่ๆ folder ใน Flash Drive หายไปหมด แต่ไฟล์อื่นๆ อยู่ไวรัสตัวนี้มีชื่อว่า “ไวรัส ซ่อนไฟล์ ให้เป็น system และสร้าง shortcut” มีชื่อที่แตกต่างกันหลายชื่อเช่น VBS Worm, VBSRunauto, VBS/Yuyun A หรือ malware DR/Agent.JP.4, TOEUW.EXE Virus/Malware อาการของไวรัสตัวนี้ติดง่ายๆ เพียงแค่เอา Flash Drive ไปเสียบเครื่องที่ติดไวรัสอยู่แล้ว และเมื่อเปิด Flash Drive ก็จะติดทันที โดยอาการที่ติดเป็นดังนี้



ไวรัสจะซ่อน folder ไว้แล้วสร้าง shortcut ชื่อเดียวกันกับ folder นั้นๆ ขึ้นมา ภาพซ้ายเป็นมุมมองปกติ ภาพขวาเป็นมุมมองแสดง folder จริงๆ ที่ถูกซ่อนไว้ พอไปคลิกที่ folder นั้นก็จะเป็นการรันไฟล์ไวรัสที่ลิ้งค์ไปให้ทำงานแสดงถึง shortcut ไปที่ไฟล์ไวรัส เมื่อคลิกรันไปแล้ว ไวรัสก็จะทำงาน ถ้าเครื่องที่มี anti virus ก็ pop up ขึ้นมาเตือน ส่วนเครื่องที่ไม่มีหรือมีแต่ไม่ update จะติดไวรัสนั้น วิธีแก้ไขเบื้องต้นสำหรับ folder ที่ถูกซ่อนไว้ ดังนี้

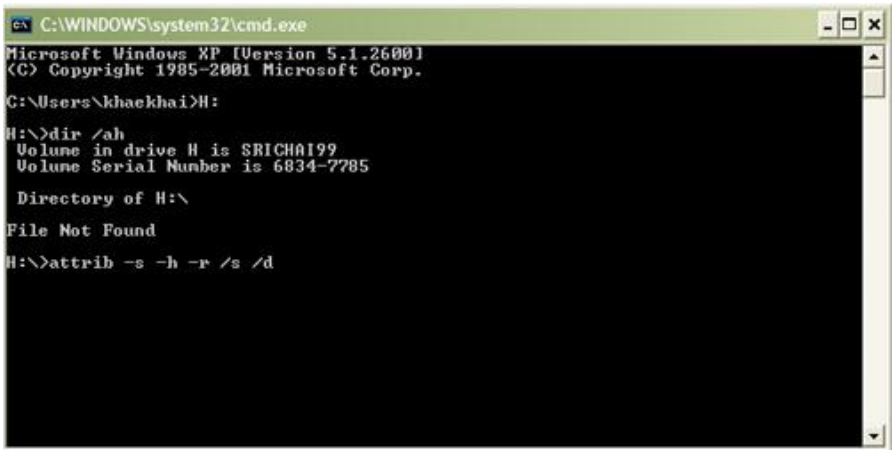
1. หลังจากเสียบ flashdrive แล้ว เปิด My Computer ดูว่า flashdrive ของเราอยู่ใน Drive อะไร เช่น F:, G:, H: ให้จำไว้แล้วปิดหน้าต่างนี้ไป ขั้นตอนต่อไป ไปที่ Start-> เลือก Run แล้วพิมพ์ว่า cmd



จะได้หน้าต่างสีดำๆ ขึ้น มาเรียกว่า command prompt ดังในรูป

2. หลังจากนั้นตามที่จำว่า Flash drive อยู่ เช่น D: E: F: ถ้าอยู่ drive H: ก็จะขึ้นดังนี้ H:\> แล้ว ให้พิมพ์คำสั่ง dir ซึ่งย่อมาจาก directory หมายถึง แสดง file และ folder ที่ยู่ใน drive H โดยพิมพ์คำสั่ง dir /ah มี /ah หมายถึง ให้แสดงเฉพาะ file และ folder ที่ถูกซ่อนอยู่ (hidden) ซึ่งทีนี้จะเห็นแล้วว่า folder ไม่ได้หายไปไหน ยังอยู่ครบเพียงแต่ถูกซ่อนไว้ และทำให้สถานะเป็น system file ต่อไปเป็นการทำให้กลับมาโดยพิมพ์ต่อใน command prompt ให้พิมพ์ว่า attrib -s -h -r /s /d ดังภาพ

แล้วพิมพ์คำสั่งในการลบ Folder ที่ซ่อนอยู่ (ไวรัส) ดังนี้ H:\>attrib -s -h -r /s /d



ความหมายของคำสั่ง attrib มาจากคำว่า Attribute แปลว่าคุณลักษณะ เป็นคำสั่งจัดการกับลักษณะหรือประเภทไฟล์ ต่อมา -s -h -r เป็นการระบุประเภทของไฟล์นั้นๆ โดย R (Read-Only) H (Hidden File) S (System File) ส่วน /s /d หมายถึงทุก file และทุกๆ folder รวมถึง sub folder คือ folder ย่อยๆ พิมพ์ attrib -s -h -r /s /d แล้ว Enter หลังจาก enter จะมีการทำงานของคำสั่งให้รอสักครู่ แล้วมาดูผลการทำงานโดยใช้คำสั่งเดิม คือ dir /ah ผลที่ได้หากไม่มี file หรือ folder ที่ถูกซ่อนไว้ถือว่าการทำงานสำเร็จ คราวนี้ไปดูใน Flash drive จะปรากฏว่า folder ต่างๆ ได้กลับมา

การแก้ไขโดยการใช้โปรแกรม SPKAutorunKiller

ดาวน์โหลดโปรแกรม SPKAutorunKiller 2.4 เมื่อดาวน์โหลดเสร็จสิ้น

1. ดับเบิลคลิกที่ไฟล์ SPKAutokillerV2.4.exe -----> Run -----> Install เพื่อติดตั้งโปรแกรม

2. หากติดตั้งโปรแกรมแล้วเครื่องเตือนว่ามี error บางอย่างและไม่มีสัญลักษณ์ SPK ขึ้นที่มุมล่างขวา ให้ติดตั้งปรแกรม DOTNET ซึ่งเป็นตัวเสริมเพิ่มและดิบเบิลคลิกที่ไอคอน Spk ที่หน้าจออีกครั้ง โปรแกรมจะถูกติดตั้งไว้ในเครื่อง และลบไวรัสโดยอัตโนมัติเมื่อมีการเสียบแฮนดี้ไดร์ฟ หรือสื่อบันทึกข้อมูลแบบพกพา

หมายเหตุ เมื่อแฮนดี้ไดร์ฟติดไวรัสนี้แล้ว ห้ามคลิกเพื่อเปิดไฟล์หรือดับเบิ้ลคลิกไฟล์ที่กลายเป็น shortcut เด็ดขาด ไม่เช่นนั้น เครื่อง คอมพิวเตอร์นั้นจะกลายเป็นแหล่งแพร่ไวรัสทันที กรณีเครื่องคอมพิวเตอร์เครื่องนั้นเป็นตัวแพร่เชื้อไวรัส Shotcut ไปแล้วให้ใช้โปรแกรม ComboFix จัดการไวรัสในเครื่อง

****การใช้งาน ComboFix แนะนำให้ใช้งานบน SeftMode เพื่อให้ได้ผลที่แน่นอนกว่า แต่ตัว ComboFix อาจจะมีปัญหากับการจัดการไวรัสที่แผงตัวเข้าสู่ระบบ Windows หรือไฟล์ System ดังนั้นก่อนการใช้งาน ComboFix แนะนำให้ Backup ข้อมูลที่สำคัญก่อน เพราะถ้าไวรัสติดไฟล์ระบบแล้ว หากComboFIx ทำงาน ก็อาจจะลบไฟล์ระบบนั้นทิ้งทันที จึงทำให้ WIndows อาจจะล่มได้

เอกสารอ้างอิง

_____. 2555. คู่มือการจัดการความรู้เรื่อง ไวรัสคอมพิวเตอร์และสปายแวร์. สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย

สัญญา คล่องในวัย. 2543. **ไวรัสคอมพิวเตอร์.** NECTECH Technical Journal ปีที่ 1 (ฉบับที่6): หน้า 237-242

NECTEC. 2555. **วิธีการป้องกัน ไวรัสคอมพิวเตอร์**. แหล่งที่มา : http://www.ops.go.th/ictc/index.php/ictc-km/it-update/antivirus-update/52-virus-protect, 20 กรกฎาคม 2556