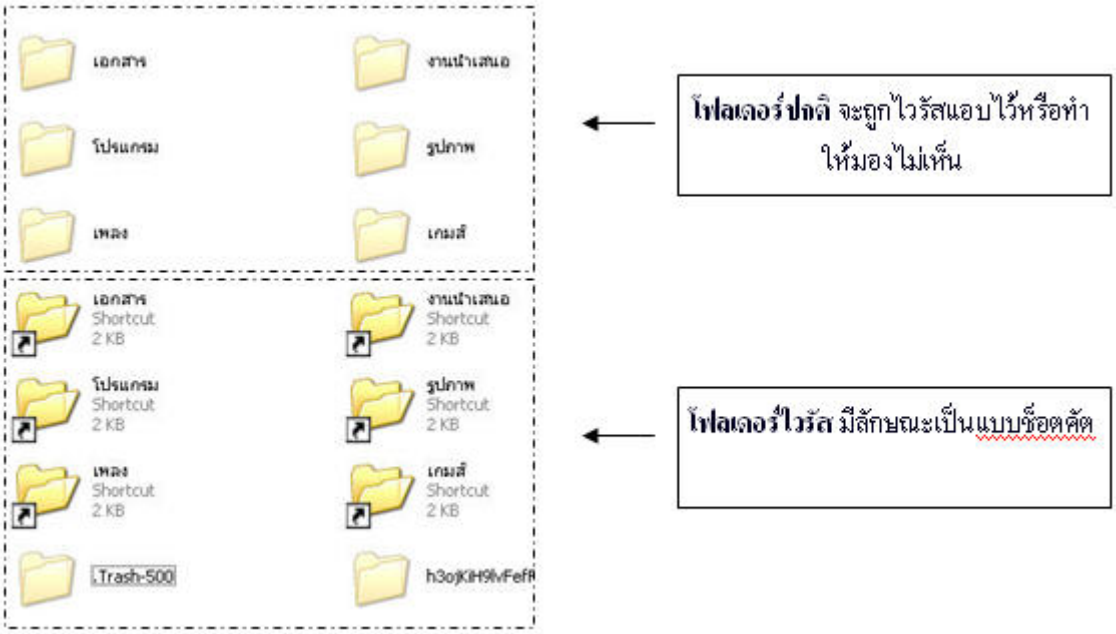
แก้ปัญหา ไวรัสซ่อน Folder แล้วสร้าง shortcut ใน Flash Drive

หลายคนคงเคยเจอกับปัญหาแบบนี้ ที่อยู่ดีๆ folder ใน Flash Drive หายไปหมด!! แต่ไฟล์อื่นๆดันอยู่ครบ หรือ ทุกอย่างปกติ แต่ไอ้เจ้า folder ที่ใช้เก็บข้อมูลต่างๆ ดันกลายเป็น .exe หมดเลย!! แล้วก็จะมีคำถามตามมาว่า “ทำไงดีงานอยู่ในนั้นหมดเลย ตาย...ล่ะทีนี้” ถ้าท่านที่เจอปัญหาแบบนี้ ให้ทำใจ..... ใจเย็นๆ ข้อมูลยังอยู่ เพียงแค่มีไวรัสบางตัวเอามันไปซ่อนไว้ และเราจะพาท่านเอามันกลับมา

เริ่มแรกมารู้จักก่อนว่ามันคืออะไรและติดมาได้ยังไง

ไวรัสตัวนี้มีชื่อว่า “ไวรัส ซ่อนไฟล์ ให้เป็น system และสร้าง shortcut” แต่มีชื่อที่แตกต่างกันหลายชื่อเช่น VBS Worm,VBSRunauto,VBS/Yuyun A หรือ malware DR/Agent.JP.4, TOEUW.EXE Virus/Malware

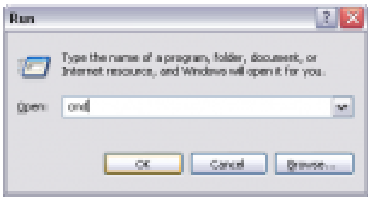
อาการของ ไวรัสตัวนี้ติดง่ายๆ เพียงแค่ท่านเอา Flash Drive ไปเสียบเครื่องที่ติดไวรัสอยู่แล้ว และเมื่อท่านเปิด Flash Drive ก็จะติดทันที โดยอาการที่ติดจะเป็นดังนี้



ดัง ที่เห็นในภาพไวรัสจะซ่อน folder ไว้แล้ว สร้าง shortcut ชื่อเดียวกันกับ folder นั้นๆขึ้นมา เปรียบเทียบได้จากภาพ ซ้ายและขวา ในภาพซ้ายเป็นมุมมองปกติ ภาพขวาเป็นมุมมองแสดง folder จริงๆของเราที่ถูกซ่อนไว้พอไปคลิกที่ folder นั้นก็จะเป็นการรัน ไฟล์ไวรัส ที่ลิ้งค์ไปให้ทำงาน ดังในรูปนี้แสดงถึงว่า shortcut ไปที่ไฟล์ไวรัส พอ เราคลิกรันไปแล้ว ไวรัสก็จะทำงาน ถ้าเครื่องที่มี anti virusก็ pop up ขึ้นมาเตือน ส่วนเครื่องที่ไม่มีหรือมีแต่ไม่ update ก็ติดแน่ๆ

วิธีแก้เบื้องต้นสำหรับ flash drive ที่โดนมาจากที่อื่นคือ folder ถูกซ่อนไว้หาไม่เจอ แต่คอมพิวเตอร์ไม่ได้ติดไวรัสตัวนี้ไปด้วย

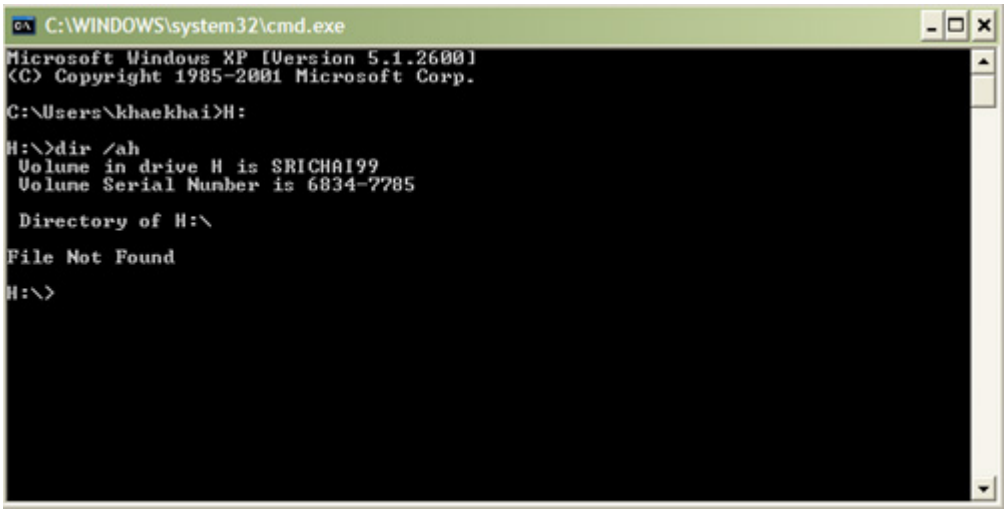
1. หลังจากเสียบ flashdriveแล้ว เปิด My Computer ดูว่า flashdriveของเราอยู่ใน Drive อะไร เช่น F: , G: , H: ให้จำไว้แล้วปิดหน้าต่างนี้ไป ขั้นตอนต่อไป ไปที่ Start->เลือก Run แล้วพิมพ์ว่า cmd



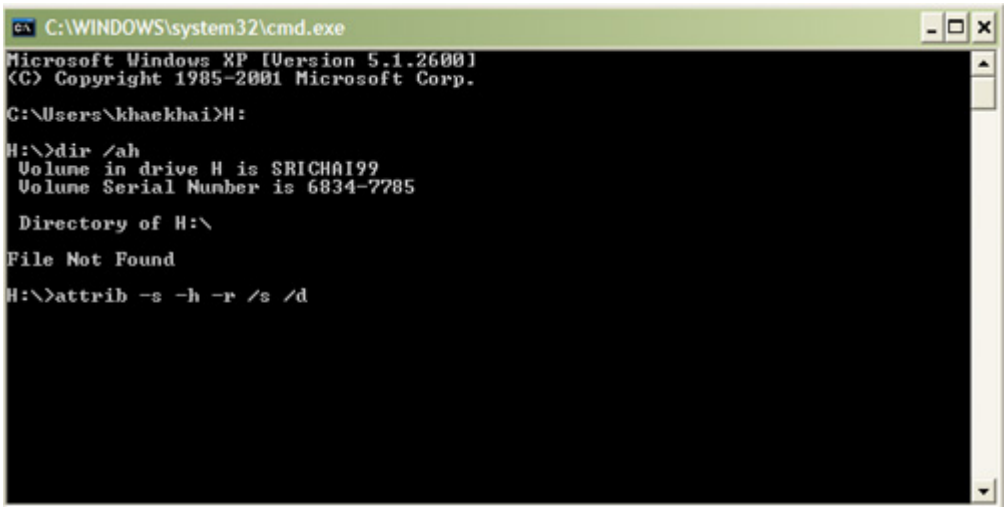
จะได้หน้าต่างสีดำๆขึ้น มาเรียกว่า command prompt ดังในรูป

2. หลังจากนั้นตามที่ให้จำว่า Flash drive เราอยู่ drive ไหน ได้แล้วให้พิมพ์ drive นั้น ลงไปเช่น D: E: F: แล้วแต่เครื่องพอพิมพ์ drive ลงไป เช่นถ้าอยู่ drive H: ก็จะขึ้นดังนี้ H:\>

แล้ว ให้พิมพ์คำสั่ง dirซึ่งย่อมาจาก directory หมายถึง แสดง file และ folder ที่อยู่ใน drive H โดยพิมพ์คำสั่ง dir /ah มี /ah เพิ่มขึ้นมาหมายถึง ให้แสดงเฉพาะ file และ folder ที่ถูกซ่อนอยู่ (hidden) ซึ่งทีนี้เราก็จะเห็นแล้วว่า folder เก็บงานเราไม่ได้หายไปไหน ยังอยู่ครบเพียงแต่ถูกซ่อนไว้ และ ทำให้สถานะเป็น system file ต่อไปเป็นการทำให้กลับมา
โดยพิมพ์ต่อใน command prompt เลย ให้พิมพ์ว่า attrib -s -h -r /s /d ดังในรูป



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



ความหมายของคำสั่ง attribมาจากคำว่า Attribute แปลว่าคุณลักษณะ เป็นคำสั่งจัดการกับลักษณะหรือประเภทไฟล์
ต่อมา -s -h -r เป็นการระบุประเภทของไฟล์ นั้นๆ โดย R(Read-Only) H(Hidden File) S(System File) ส่วน /s /d
หมายถึงทุก file และ ทุกๆ folder รวมถึง sub folder คือ folder ย่อยๆนั้นเอง พอทราบความหมายแล้วมาดูผลการทำงานกัน
พิมพ์ attrib -s -h -r /s /d แล้ว Enter หลังจาก enter จะมีการทำงานของคำสั่งให้รอสักครู่
แล้วมาดูผลการทำงานกันโดยใช้คำสั่งเดิม คือ dir /ah ผลที่ได้หากไม่มี file หรือ folder ที่ถูกซ่อนไว้ถือว่าการทำงานสำเร็จ
คราวนี้ไปดูใน Flash drive กันว่าเป็นยังไงบ้าง ผลที่ได้คือได้ folder ต่างๆ กลับมา

การแก้ไขโดยการปรแกรม SPKAutorunKiller

ดาวน์โหลดโปรแกรม SPKAutorunKiller 2.4

เมื่อดาวน์โหลดเสร็จสิ้น

1. ดับเบิลคลิกที่ไฟล์ SPKAutokillerV2.4.exe -----> Run -----> Install เพื่อติดตั้งโปรแกรม
2. หากติดตั้งโปรแกรมแล้วเครื่องเตือนว่ามีerror บางอย่างและไม่มีสัญลักษณ์ SPK ขึ้นที่มุมล่างขวา ให้ติดตั้งปรแกรม DOTNET ซึ่งเป็นตัวเสริมเพิ่มและดิบเบิลคลิกที่ไอค่อน Spkที่หน้าจออีกครั้ง โปรแกรมจะถูกติดตั้งไว้ในเครื่อง และทำการลบไวรัสโดยอัตโนมัติเมื่อมีการเสียบแฮนดี้ไดร์ฟ หรือสื่อบันทึกข้อมูลแบบพกพา

หมายเหตุ เมื่อแฮนดี้ไดร์ฟ ติดไวรัสนี้แล้ว **อย่า!!!!!** คลิกเพื่อเปิดไฟล์หรือดับเบิ้ลคลิกไฟล์ที่กลายเป็น shortcut เด็ดขาด

ไม่เช่นนั้น เครื่อง คอมพิวเตอร์เครื่องนั้นจะกลายเป็นแหล่งแพร่ไวรัสทันที
กรณีเครื่องคอมพิวเตอร์เครื่องนั้นเป็นตัวแพร่เชื้อไวรัส Shotcut ไปแล้ว
ให้ใช้โปรแกรม ComboFix จัดการไวรัสในเครื่อง

****การใช้งาน ComboFixแนะนำให้ใช้งานบน SeftModeนะครับ เพื่อให้ได้ผลที่แน่นอนกว่า แต่ตัว ComboFixอาจจะมีปัญหากับการจัดการไวรัสที่แผงตัวเข้าสู่ระบบ Windows หรือไฟล์ System ดังนั้นก่อนการใช้งาน ComboFixแนะนำให้ Backup ข้อมูลที่สำคัญก่อนนะครับ เพราะถ้าไวรัสติดไฟล์ระบบแล้ว หากComboFIxทำงาน ก็อาจจะลบไฟล์ระบบนั้นทิ้งทันที จึงทำให้ WIndows อาจจะล่มได้