แก้ปัญหา ไวรัสซ่อน Folder แล้วสร้าง shortcut ใน FlashDrive

หลายคนคงเคยเจอกับปัญหา folder ใน Flash Drive หายไปหมด แต่ไฟล์อื่นๆอยู่ครบ หรือ ทุกไฟล์อยู่ปกติ แต่ folder ที่ใช้เก็บข้อมูลต่างๆ กลายเป็น .exe ทั้งหมด ถ้าเจอปัญหาแบบนี้ ให้รู้ว่า ข้อมูลยังอยู่ เพียงแต่มีไวรัสบางตัวซ่อนfolderไว้ เริ่มต้นมารู้จักก่อนว่ามันคืออะไรและติดมาได้อย่างไร

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

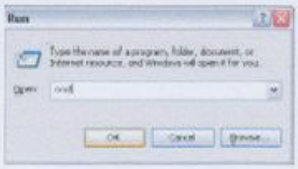
โฟลเดอร์ปกติ จะถูกไวรัสแอบไว้หรือทำให้มองไม่เห็น

โฟลเดอร์ไวรัส มีลักษณะเป็นแบบช็อตคัต

ดังที่เห็นในภาพไวรัสจะซ่อน folder ไว้แล้ว สร้าง shortcut ชื่อเดียวกันกับ folder นั้นๆขึ้นมา เปรียบเทียบได้จากภาพซ้ายและขวา ในภาพซ้ายเป็นมุมมองปกติ ภาพขวาเป็นมุมมองแสดง folder จริงๆของเราที่ถูกซ่อนไว้พอไปคลิกที่ folder นั้นก็จะเป็นการรัน ไฟล์ไวรัส ที่ลิ้งค์ไปให้ทำงาน ดังในรูปนี้แสดงถึงว่า shortcut ไปที่ไฟล์ไวรัส พอ เราคลิกรันไปแล้ว ไวรัสก็จะทำงาน ถ้าเครื่องที่มี anti virus จะมี pop up ขึ้นมาเตือน ส่วนเครื่องที่ไม่มีหรือมีแต่ไม่ได้ update จะติดไวรัสแน่นอน วิธีแก้ไขเบื้องต้นสำหรับ flash drive ที่ติดไวรัสมาจากที่อื่นคือ folder ถูกซ่อนไว้หาไม่เจอ แต่คอมพิวเตอร์ไม่ได้ติดไวรัสตัวนี้ไปด้วย

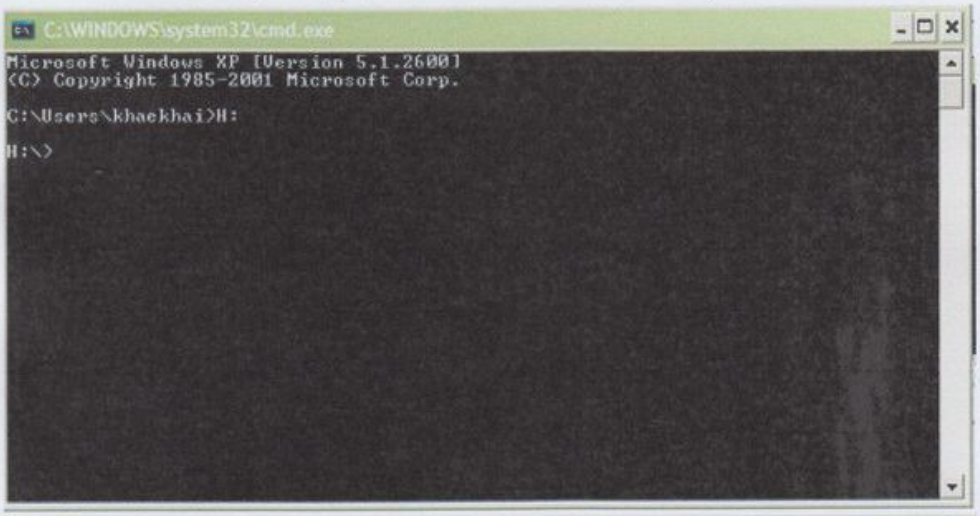
1. หลังจากเสียบ flash drive แล้วให้ เปิด My Computer เพื่อดูว่า flash drive ของเราอยู่ใน Drive อะไร เช่น F: , G: , H: ให้จำไว้แล้ว

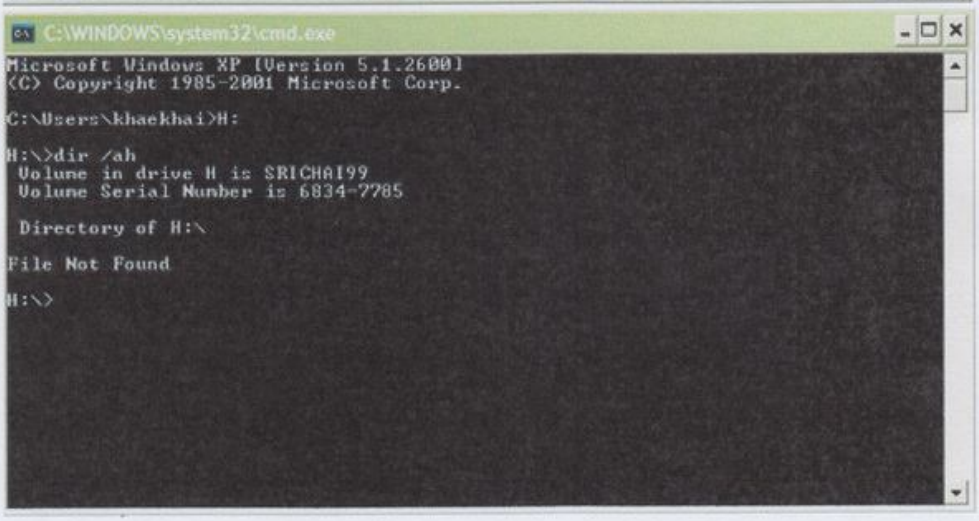
ปิดหน้าต่างนี้ไป ขั้นตอนต่อไป ให้ไปที่ Start-> เลือก Run แล้วพิมพ์ว่า cmd



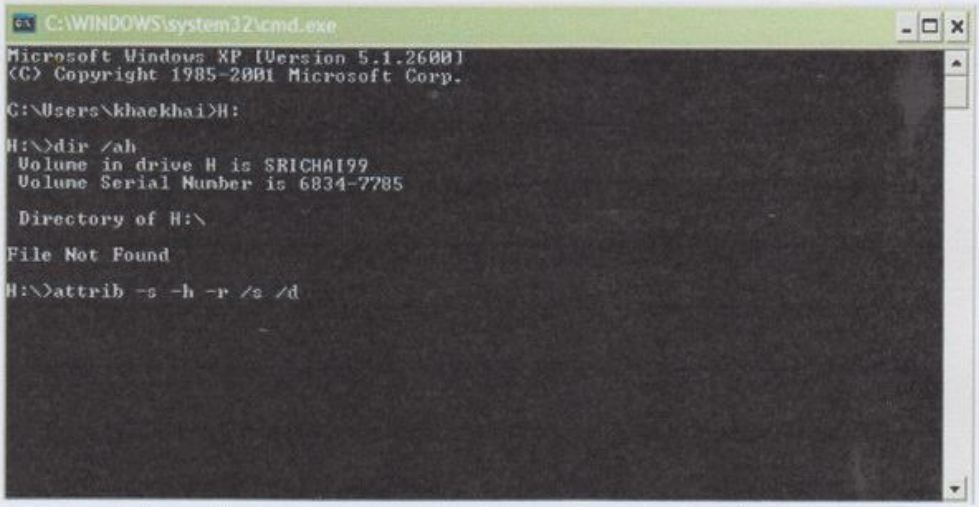
จะได้หน้าต่างสีดำขึ้นมาเรียกว่า command prompt ดังในรูป

2.หลังจากนั้นตามที่ให้จำว่า Flash drive เราอยู่ drive ไหน แล้วให้พิมพ์ drive นั้น ลงไปเช่น D: E: F: แล้วแต่เครื่องพอพิมพ์ drive ลงไป เช่นถ้าอยู่ drive H: ก็จะขึ้นดังนี้ H:\>แล้ว ให้พิมพ์คำสั่ง dir ซึ่งย่อมาจาก 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 ต่อไปเป็นการทำให้ folder กลับมา
โดยพิมพ์ต่อใน command prompt ว่า attrib -s -h -r /s /d ดังในรูป





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



ความหมายของคำสั่ง attrib มาจากคำว่า 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 แล้วมาดูผลการทำงาน โดยใช้คำสั่งเดิม คือ dir /ah ผลที่ได้หากไม่มี file หรือ folder ที่ถูกซ่อนไว้ถือว่าการทำงานสำเร็จ คราวนี้ไปดูใน Flash drive จะได้ folder ต่างๆ กลับมา

การแก้ไขโดยการใช้โปรแกรม SPKAutorunKiller

ดาวน์โหลดโปรแกรม **SPKAutorunKiller 2.4**

เมื่อดาวน์โหลดเสร็จสิ้น

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

2. หากติดตั้งโปรแกรมแล้วเครื่องเตือนว่ามีerror บางอย่างและไม่มีสัญลักษณ์ SPK ขึ้นที่มุมล่างขวา ให้ติดตั้งโปรแกรม DOTNET ซึ่งเป็นตัวเสริมเพิ่มและดิบเบิลคลิกที่ไอค่อน Spk ที่หน้าจออีกครั้ง โปรแกรมจะถูกติดตั้งไว้ในเครื่อง และทำการลบไวรัสโดยอัตโนมัติ เมื่อมีการเสียบแฮนดี้ไดร์ฟ หรือสื่อบันทึกข้อมูลแบบพกพา

หมายเหตุ เมื่อ falsh drive ติดไวรัสนี้แล้ว ห้าม คลิกเพื่อเปิดไฟล์หรือดับเบิ้ลคลิกไฟล์ที่กลายเป็น shortcut เด็ดขาด ไม่เช่นนั้น เครื่องคอมพิวเตอร์เครื่องนั้นจะกลายเป็นแหล่งแพร่ไวรัสทันที

กรณีเครื่องคอมพิวเตอร์เครื่องนั้นเป็นตัวแพร่เชื้อไวรัส Shotcut ไปแล้ว
ให้ใช้โปรแกรม ComboFix จัดการไวรัสในเครื่อง
****การใช้งาน ComboFix แนะนำให้ใช้งานบน SeftMode เพื่อให้ได้ผลที่แน่นอนกว่า แต่ตัว ComboFix อาจจะมีปัญหากับการจัดการไวรัสที่แผงตัวเข้าสู่ระบบ Windows หรือไฟล์ System ดังนั้นก่อนการใช้งาน ComboFix แนะนำให้ Backup ข้อมูลที่สำคัญก่อน เพราะถ้าไวรัสติดไฟล์ระบบแล้ว หากComboFIx ทำงานก็อาจจะลบไฟล์ระบบนั้นทิ้งทันที จึงทำให้ Windows อาจจะล่มได้

ที่มา http://www.singburi.go.th/sara/shortcut%20virus.html