แก้ปัญหา ไวรัสซ่อน Folder แล้วสร้าง shortcut ใน FlashDrive

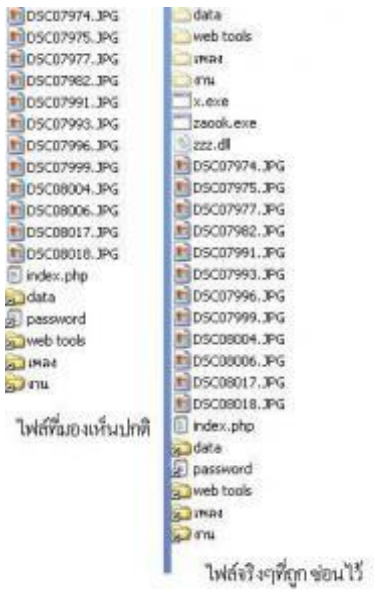
Posted by crupan

หลายคนคงเคยเจอกับปัญหาแบบนี้ ที่อยู่ดีๆ folder ใน Flash Drive หายไปหมด!! แต่ไฟล์อื่นๆดันอยู่ครบ หรือ ทุกอย่างปกติ แต่ไอ้เจ้า folder ที่ใช้เก็บข้อมูลต่างๆ ดันกลายเป็น .exe หมดเลย!! แล้วก็จะมีคำถามตามมาว่า “ทำไงดีเนี้ย งานอยู่ในนั้นหมดเลย ตาย...ล่ะทีนี้” ถ้าท่านที่เจอปัญหาแบบนี้นะครับ ให้ทำใจ..... ใจเย็นๆครับ ข้อมูลยังอยู่ครับ เพียงแค่มีไวรัสบางตัวเอามันไปซ่อนไว้ครับ และผมจะพาเอามากลับมา

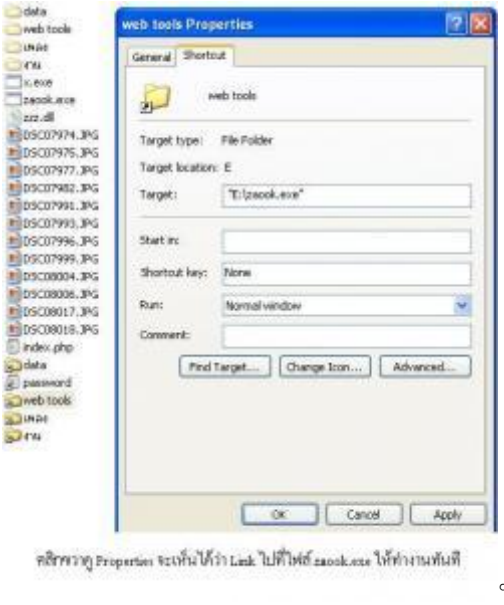
เริ่มแรกมารู้จักก่อนว่ามันคืออะไรและติดมาได้ยังไง

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

อาการของมัน ไวรัสตัวนี้ติดง่ายๆเลยครับ เพียงแค่ท่านเอา Flash Drive ไปเสียบเครื่องที่ติดไวรัสอยู่แล้ว และเมื่อท่านเปิด Flash Drive ก็จะติดทันที โดยอาการที่ติดจะเป็นแบบนี้ครับ



ดัง ที่เห็นในภาพนะครับไวรัสจะซ่อน folder ไว้แล้ว สร้าง shortcut ชื่อเดียวกันกับ folder นั้นๆขึ้นมา เปรียบเทียบได้จากภาพ ซ้ายและขวา ในภาพซ้ายเป็นมุมมองปกติ ภาพขวาเป็นมุมมองแสดง folder จริงๆของเราที่ถูกซ่อนไว้พอไปคลิกที่ folder นั้นก็จะเป็นการรัน ไฟล์ไวรัส ที่ลิ้งค์ไปให้ทำงาน ดังในรูปนี้แสดงถึงว่า shortcut ไปที่ไฟล์ไวรัส

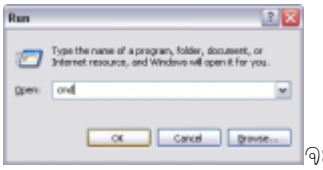


พอ เราคลิกรันไปแล้ว ไวรัสก็จะทำงาน ถ้าเครื่องที่มี anti virus ก็ pop up ขึ้นมาเตือนแน่นอนครับ ส่วนเครื่องที่ไม่มีหรือมีแต่ไม่ update ก็ติดแน่ๆครับ

วิธีแก้เบื้องต้นก่อนนะครับ

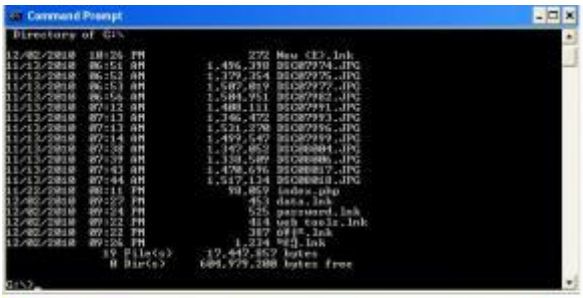
สำหรับ flash drive ที่โดนมาจากที่อื่นคือ folder ถูกซ่อนไว้หาไม่เจอ เอากลับมาไม่ได้นะครับ แต่คอมพิวเตอร์ไม่ได้ติดไวรัสตัวนี้ไปด้วย

1. หลังจากเสียบ flashdrive แล้วไปที่ Start-> เลือก Run แล้วพิมพ์ว่า cmd



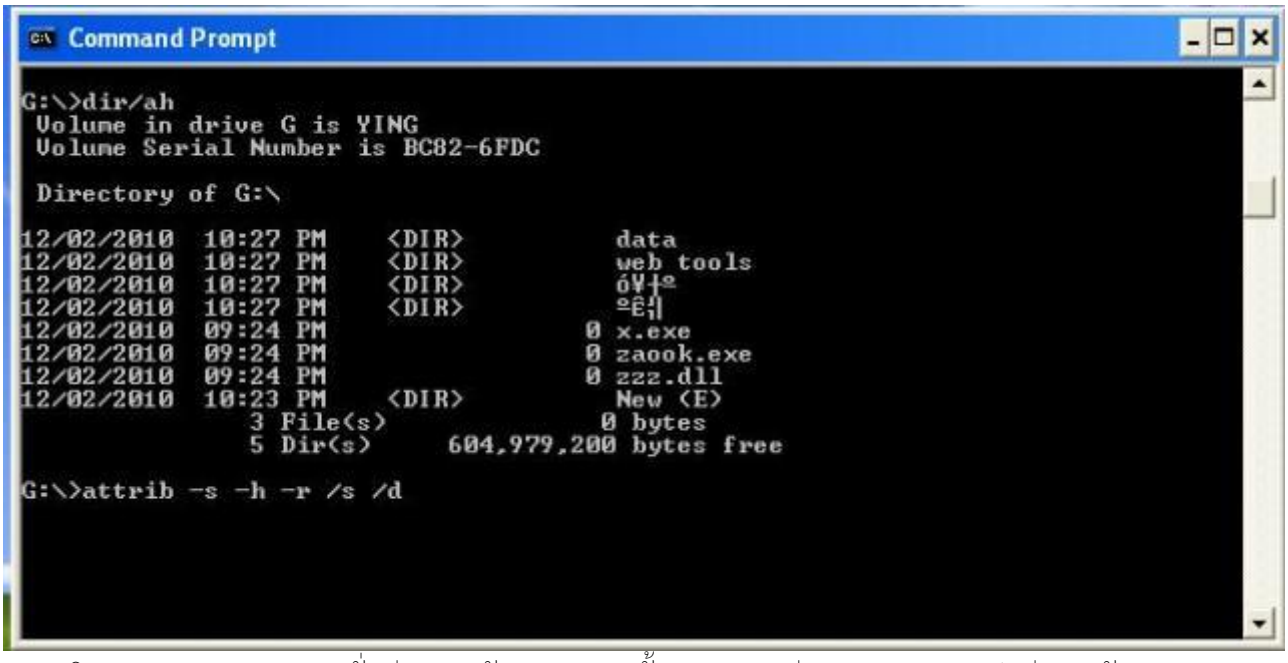
จะได้หน้าต่างสีดำๆขึ้นมาเรียกว่า command prompt ดังในรูป

2. หลังจากนั้นไปสำรวจว่า Flash drive เราอยู่ drive ไหน ของผมอยู่ใน Drive G นะครับ ได้แล้วให้พิมพ์ drive นั้น ลงไปเลยเช่น D: E: F: แล้วแต่คนนะครับ พอพิมพ์ drive ลงไป จะขึ้นแบบนี้ครับ G:\>



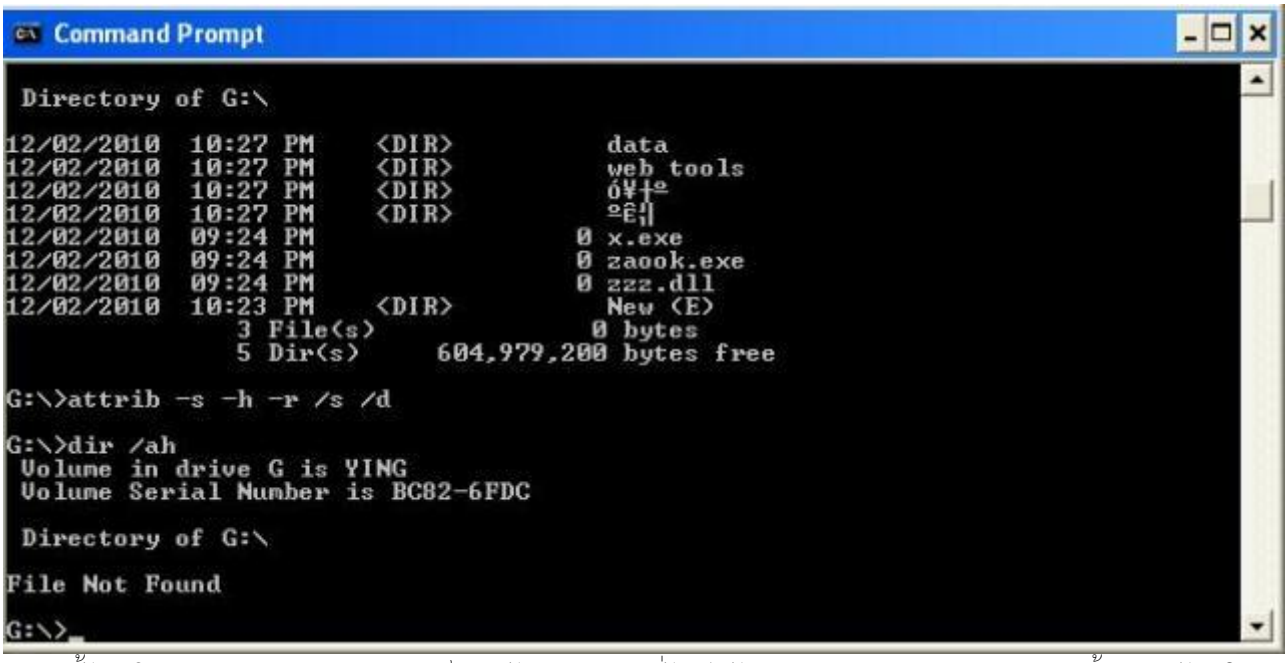
แล้ว ให้พิมพ์คำสั่งตามนี้ครับ dir แล้ว enter จะได้ผลตามรูปด้านบนนะครับ คือคำสั่ง dir ย่อมาจาก directory หมายถึง แสดง file และ folder อยู่อยู่ใน drive G ส่วนรูปล่าง คำสั่ง dir /ah ก็คล้ายๆกันแต่ต่างกันตรงมี /ah เพิ่มขึ้นมาโดยหมายถึง ให้แสดงเฉพาะ file และ folder ที่ถูกซ่อนอยู่ (hidden) ซึ่งทีนี้เราก็จะเห็นแล้วว่า folder เก็บงานเราไม่ได้หายไปไหน ยังอยู่ครบเพียงแต่ถูกซ่อนไว้ และ ทำให้สถานะเป็น system file ต่อไป เป็นการทำให้กลับมา

โดยพิมพ์ต่อใน command prompt เลย ให้พิมพ์ว่า attrib -s -h -r /s /d ดังในรูป

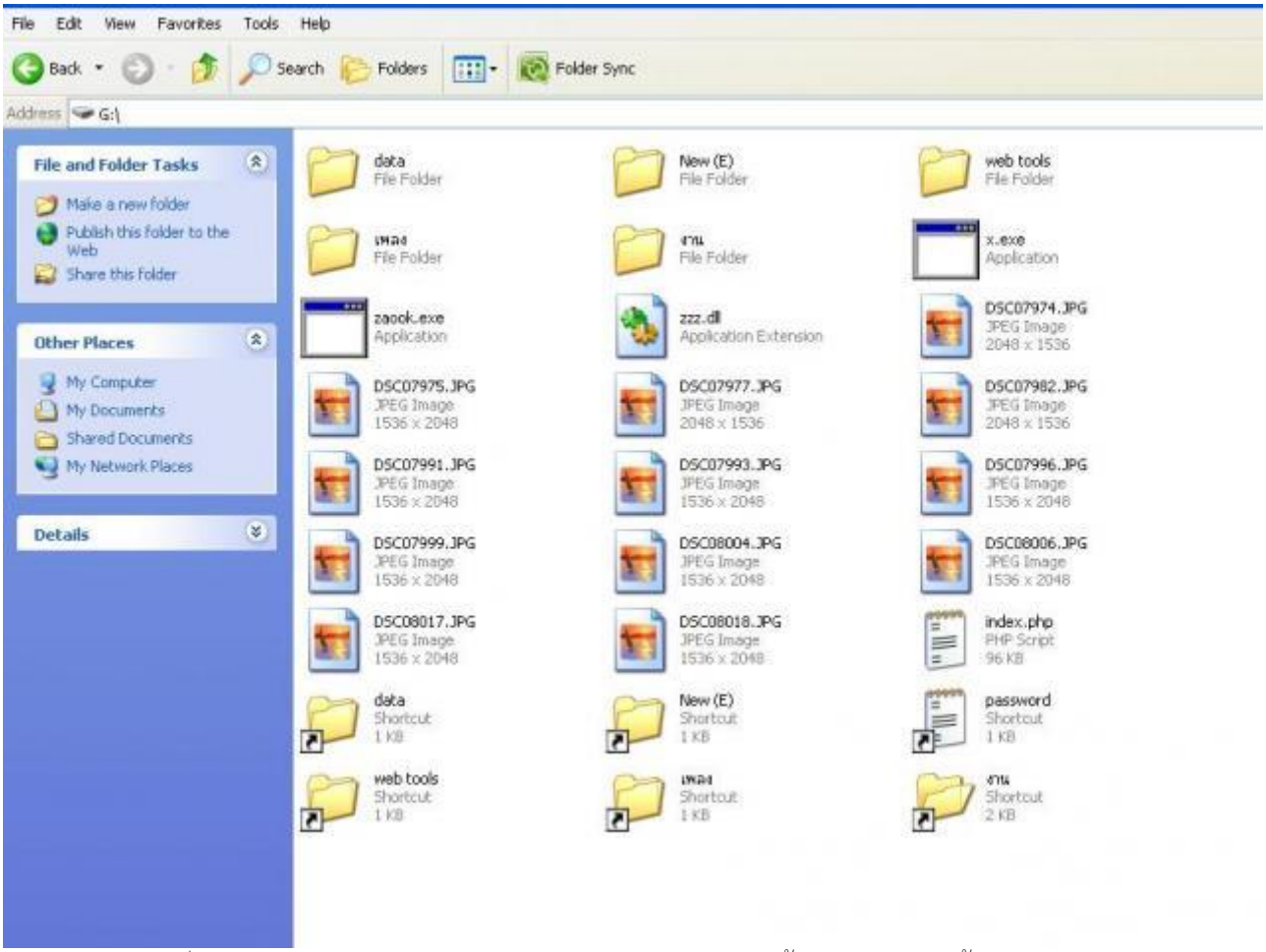


ขอ อธิบายความหมายของคำสั่งก่อนนครับ attrib นั้นมาจากคำว่า Attribute แปลว่าคุณลักษณะ เป็นคำสั่งจัดการกับลักษณะหรือประเภทไฟล์ต่อมา -s -h -r เป็นการระบุประเภทของไฟล์ นั้นๆ โดย R(Read-Only) H(Hidden File) S(System File) ส่วน /s /d หมายถึงทุก file และ ทุกๆ folder รวมถึง sub folder คือ folder ย่อยๆนั้นเอง พอทราบความหมายแล้วมาดูผลการทำงานกัน พิมพ์ attrib -s -h -r /s /d แล้ว Enter ได้เลยครับหลังจาก enter จะมีการทำงานแว็บหนึ่ง

มาดูผลการทำงานกันโดยใช้คำสั่งเดิม คือ dir /ah ผลที่ได้คือไม่มี file หรือ folder ที่ถูก ซ่อนไว้เลยดังในภาพ



คราวนี้ไปดูใน Flash drive กันว่าเป็นยังไงบ้าง ผลที่ได้คือได้ folder ต่างๆกลับมารวมทั้งเจอ ไฟล์เจ้าปัญหา คือไฟล์ไวรัส ดังในรูป



ต่อไปก็ลบไฟล์ที่เป็น shortcut ไฟล์ไวรัส รวมถึง autorun.inf ทิ้งให้หมด แค่นี้ก็หมดปัญหาครับ

สรุปง่ายๆ สำหรับ flash drive ที่เกิดปัญหา Folder ถูกซ่อนแล้วสร้าง shortcut ปลอมขึ้นมา ดังนี้

1. เสียบ flash drive แล้วดูว่าอยู่ drive ไหน

2. ไปที่ start->run พิมพ์ cmd

3. พิมพ์คำสั่งใน cmd เป็นชื่อ drive ของ flash drive เราเช่น E: หรือ F: แล้ว enter ทั้งนี้ขึ้นอยู่กับ drive ของเรา

4. พิมพ์ attrib -s -h -r /s /d แล้ว กด enter

5. ไปลบไฟล์ shortcut ไฟล์ ไวรัสที่เป็น exe ที่เราไม่รู้จัก รวมทั้ง autorun.inf ก็เรียบร้อยครับ ส่วนสำหรับเครื่องที่ติดไวรัสตัวนี้จะมาเขียนวิธีแก้อีกครั้งนะครับ

จงพยายาม อย่ากลัวมัน

สู้สู้...ไอ้มดแดง