

แก้ปัญหา ไวรัสซ่อน Folder แล้วสร้าง shortcut ใน FlashDrive

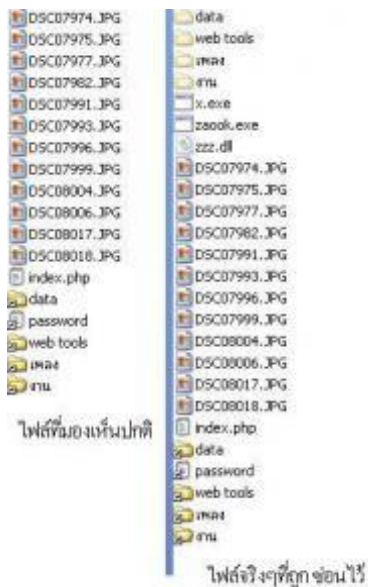
Posted by [crupan](#)

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

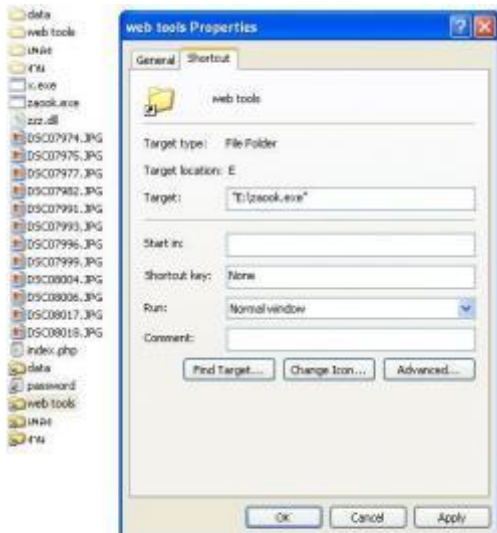
เริ่มแรกมารู้จักก่อนว่ามันคืออะไรและติดตามได้ยังไง

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

อาการของมัน ไวรัสตัวนี้ติดง่ายเลยครับ เพียงแค่ท่านเอา Flash Drive ไปเสียบเครื่องที่ติดไวรัสอยู่แล้ว และเมื่อท่านเปิด Flash Drive ก็จะมีติดทันที โดยอาการที่ติดจะเป็นแบบนี้ครับ



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



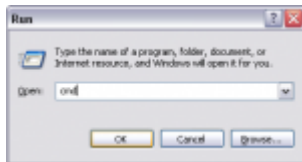
คลิกขวาที่ Properties จะเห็นได้ว่า Link ไปที่ไฟล์ zook.exe ให้ทำงานทันที

พอเราคลิกรันไปแล้ว 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:\>

```

C:\>dir
Directory of C:\
12/02/2010  10:26 AM                272  New CEO.Ink
12/02/2010  06:51 AM             1,496,380  01C07974..JPG
12/02/2010  06:52 AM             1,379,254  01C07975..JPG
12/02/2010  06:53 AM             1,507,819  01C07977..JPG
12/02/2010  06:55 AM             1,504,951  01C07982..JPG
12/02/2010  07:12 AM             1,400,111  01C07991..JPG
12/02/2010  07:13 AM             1,346,472  01C07993..JPG
12/02/2010  07:43 AM             1,521,278  01C07995..JPG
12/02/2010  07:54 AM             1,499,547  01C07999..JPG
12/02/2010  07:58 AM             1,547,852  01C08004..JPG
12/02/2010  07:59 AM             1,330,507  01C08006..JPG
12/02/2010  07:53 AM             1,478,616  01C08012..JPG
12/02/2010  07:44 AM             1,517,134  01C08015..JPG
12/02/2010  08:11 PM                90,859  Index.php
12/02/2010  09:22 PM                453  data.lnk
12/02/2010  09:24 PM                520  password.lnk
12/02/2010  09:22 PM                414  web tools.lnk
12/02/2010  09:22 PM                387  off.s.lnk
12/02/2010  09:24 PM                1,234  web.lnk
0 File(s)              17,442,859 bytes free
0 Dir(s)                604,779,200 bytes free
C:\>

```

```

C:\>dir /ah
Volume in drive G is YING
Volume Serial Number is BC82-6FDC

Directory of G:\

12/02/2010  10:27 PM    <DIR>          data
12/02/2010  10:27 PM    <DIR>          web tools
12/02/2010  10:27 PM    <DIR>          off
12/02/2010  10:27 PM    <DIR>          web
12/02/2010  09:24 PM          0 x.exe
12/02/2010  09:24 PM          0 zaook.exe
12/02/2010  09:24 PM          0 zzz.dll
12/02/2010  10:23 PM    <DIR>          New (E)
3 File(s)              0 bytes
5 Dir(s)                604,779,200 bytes free
C:\>

```

แล้ว ให้พิมพ์คำสั่งตามนี้ครับ dir แล้ว enter จะ

ได้ผลตามรูปด้านบนนะครับ คือคำสั่ง dir ย่อมาจาก directory หมายถึง แสดง file และ folder อยู่อยู่ใน drive G ส่วนรูปล่าง คำสั่ง dir /ah ก็คล้ายๆกันแต่ต่างกันตรงมี /ah เพิ่มขึ้นมาโดย หมายถึง ให้แสดงเฉพาะ file และ folder ที่ถูกซ่อนอยู่ (hidden) ซึ่งที่นี่เราก็จะเห็นแล้วว่า folder เกือบงานเราไม่ได้หาอยู่ไหน ยิ่งอยู่ครบเพียงแต่ถูกซ่อนไว้ และ ทำให้สถานะเป็น system file ต่อไป เป็นการทำให้กลับมามี

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

```

G:\>dir/ah
Volume in drive G is YING
Volume Serial Number is BC82-6FDC

Directory of G:\

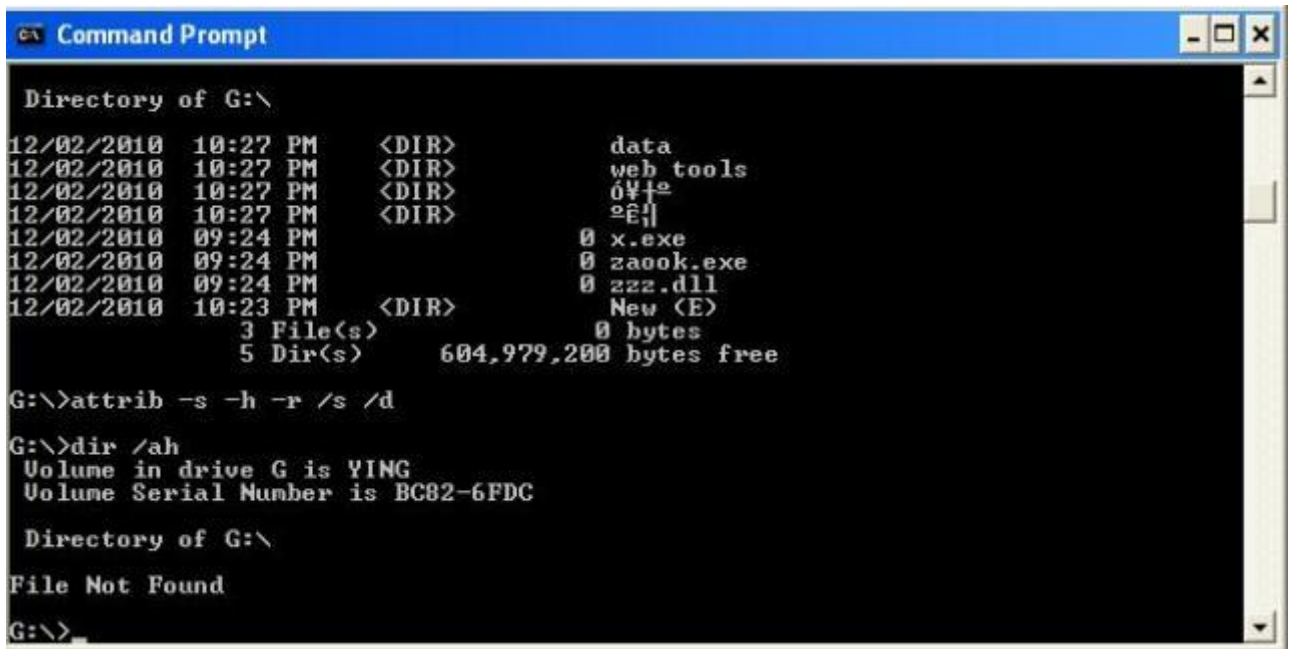
12/02/2010  10:27 PM    <DIR>          data
12/02/2010  10:27 PM    <DIR>          web tools
12/02/2010  10:27 PM    <DIR>          off
12/02/2010  10:27 PM    <DIR>          web
12/02/2010  09:24 PM          0 x.exe
12/02/2010  09:24 PM          0 zaook.exe
12/02/2010  09:24 PM          0 zzz.dll
12/02/2010  10:23 PM    <DIR>          New (E)
3 File(s)              0 bytes
5 Dir(s)                604,779,200 bytes free

G:\>attrib -s -h -r /s /d

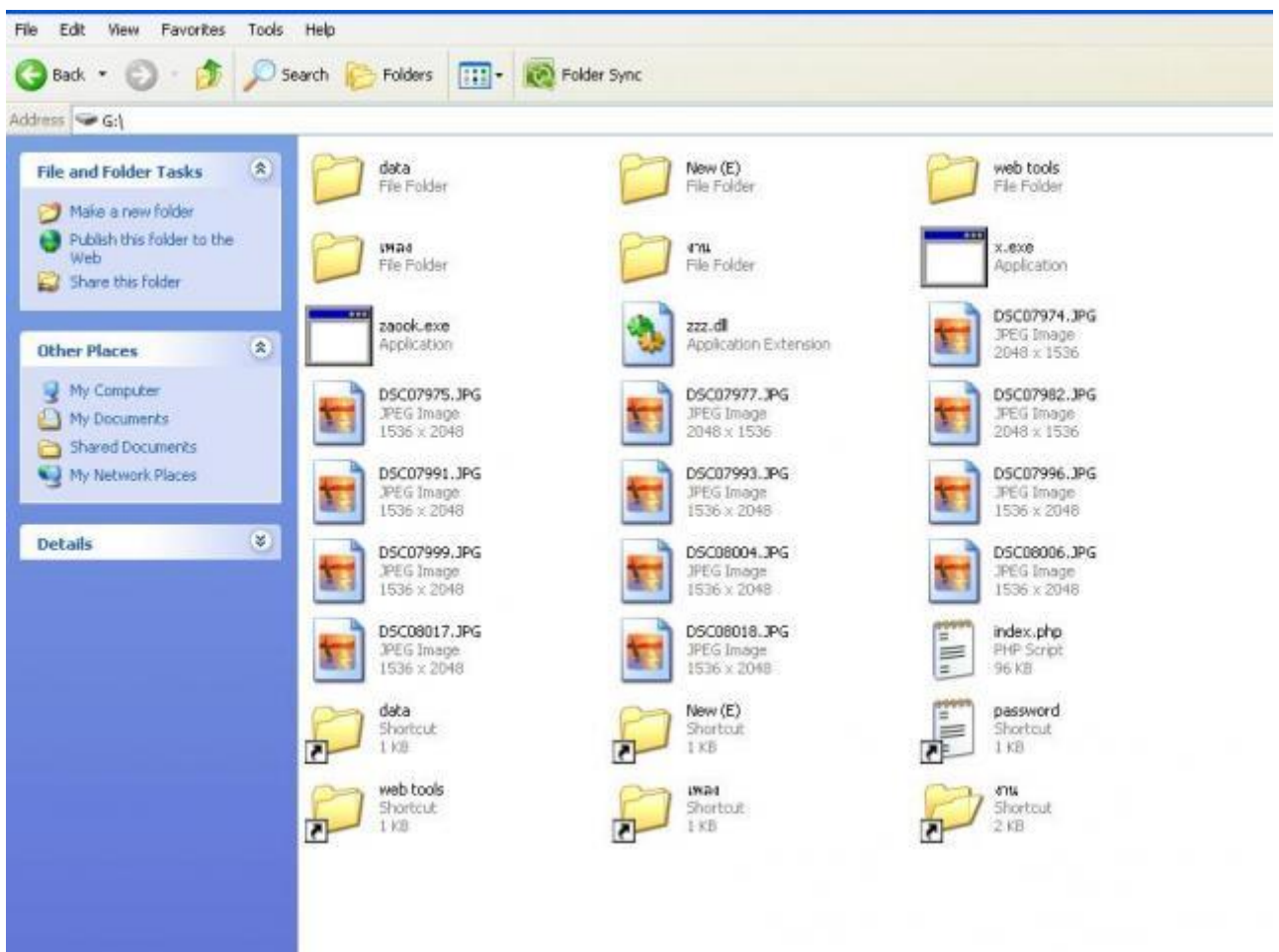
```

ขอ อธิบายความหมายของคำสั่งก่อนนะครับ 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 ย่อยๆนั่นเอง 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 ต่างๆกลับมาพร้อมทั้งเจอ ไฟล์เจ้าปัญหา คือไฟล์ไวรัส ดังในรูป



ต่อไปก็ลบไฟล์ที่เป็น shortcut ไฟล์ไวรัส รวมถึง autorun.inf ทิ้งให้หมด แต่เนี่ยก็หมดปัญหาครับ

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 อย่างกล้ามัน

สู้สู้...ไ้หมดแดง