การระบาดของไวรัสคอมพิวเตอร์ในปัจจุบันนั้น ช่องทางหนึ่งที่ถือได้ว่าเป็นช่องทางระบาดมาก ที่สุดอันหนึ่งคือ ระบาดผ่านทาง เนื่องจากในปัจจุบันสื่อเก็บข้อมูลแบบ USB Flash Drive นั้น เป็นที่นิยมใช้งานกันอย่างกว้างขวาง เพราะราคาถูกและการใช้งานก็สะดวก

ในปัจจุบันการระบาดของไวรัสคอมพิวเตอร์หลายตัวในช่วงที่ผ่านมา เช่น Hacked by Gozilla, Hack by 8Bits, หรือ Gernerin.e เป็นต้น จะแพร่ระบาดโดยการสำเนาตัวเองไปยังทุกๆ ไดรฟ์ บนเครื่องที่ติดไวรัส รวมถึงสื่อแบบพกพา เช่น floppy disk และ flash drive เป็นต้น ดังนั้นเมื่อใครก็ตามทำการต่อ flash drive กับคอมพิวเตอร์ และถ้าเครื่องคอมพิวเตอร์ได้ทำการ เปิด Autoplay บนไดร์ฟ USB ไว้ ระบบก็จะทำการเอ็กซีคิวท์ไฟล์ไวรัสทันที และคอมพิวเตอร์ เครื่อง นั้น ก็จะติดไวรัสในทันทีเช่นกัน

การป้องกันไวรัสจากแฟลชไดร์ฟ

VB Script นั้นจะใช้เซอร์วิส Windows Script Host ในการรันไฟล์ VB Script ดังนั้นการที่ จะ ป้องกันไม่ให้ไฟล์ VB Script ทำการรันได้นั้น จึงเป็นวิธีการป้องกันไวรัสประเภท VB Script หรือไวรัสตะกูล Hack by xxx ที่ได้ผลดี เนื่องจากว่าไฟล์ไวรัสไม่สามารถ ที่จะทำการ รันได้ จึงไม่สมารถที่จะติดในเครื่องคอมพิวเตอร์ได้นั้นเอง วิธีการปิดการให้บริการ Windows Script Host นั้นทำได้โดยการแก้ไข Registry ตามวิธีการด้านล่าง

วิธีการปิดให้บริการ Windows Script Host

- เปิดหน้าต่างคอมมานด์พร็อมท์โดยดำเนินการตามข้อใดข้อหนึ่ง ดังนี้
    - คลิก Start คลิก All Programsคลิก Accessories คลิก Command Prompt
    - คลิก Start คลิก Run พิมพ์ cmd ในกล่อง Open เสร็จคลิก OK

- พิมพ์คำสั่งตามบรรทัดด้านล่าง (รูปที่ ๑) เสร็จแล้วกด Enter ระบบจะแจ้งว่า "The Operation Completed Successfully"(รูปที่ ๒)

  reg add "HKLMSoftwareMicrosoftWindows Script HostSettings" /v Enabled /t REG_DWORD /d 0x00000000

รูปที่ ๑ Disable wscript

รูปที่ ๒ Disable Successfully

- ปิด command prompt โดยการพิมพ์ exit แล้วกด Enter

วิธีการเปิดให้บริการ Windows Script Host

ในกรณีที่ต้องการเปิดใช้งาน Windows Script Host ในดำเนินการตามขั้นตอนดังนี้

- เปิดหน้าต่างคอมมานด์พร็อมท์โดยดำเนินการตามข้อใดข้อหนึ่ง ดังนี้
  - คลิก Start คลิก All Programsคลิก Accessories คลิก Command Prompt
  - คลิก Start คลิก Run พิมพ์ cmd ในกล่อง Open เสร็จคลิก OK
- พิมพ์คำสั่งตามบรรทัดด้านล่าง (รูปที่ ๓) เสร็จแล้วกด Enter จะแจ้งว่า "Values Enabled Exists, Overwrite (Y/N)?" ให้พิมพ์ Y แล้วกด Enter (รูปที่ ๔) ระบบจะแจ้งว่า "The Operation Completed Successfully"(รูปที่ ๔)

  reg add "HKLMSoftwareMicrosoftWindows Script HostSettings" /v Enabled /t REG_DWORD /d 0x00000001

รูปที่ ๓ Enable wscript

รูปที่ ๔ Enable Successfully

ข้อแนะนำเพิ่มเติม

- หาก Flash drive มีสวิตซ์สำหรับป้องกันการเขียนข้อมูลลง Flash drive ให้เลือกไปที่ตำแหน่ง Lock เพื่อป้องกันการเขียนข้อมูลลง Flash drive
- ให้ตรวจสอบในโครงสร้างนอกสุดของ Flash drive ว่ามีไฟล์ Autorun.inf หรือไฟล์ประเภท VB Script (ไฟล์นามสกุล .vbs) หากแน่ใจว่าไม่ใช่ไฟล์ของตนเองให้ทำการลบไฟล์ดังกล่าวทิ้ง
- ในการใช้งานประจำวันหรืองานทั่วไป ควรจะล็อกออนเข้าใช้งานเครื่องด้วยผู้ใช้แบบจำกัดสิทธิ์ (Limited user account)

หมายเหตุ:

- วิธีการนี้ไม่ใช่การทดแทนโปรแกรมป้องกันไวรัส ขอแนะนำให้ทำการติดตั้งโปรแกรมป้องกันไวรัสและทำการอัพเดทอย่างสม่ำเสมอ
- วิธีการนี้สามารถป้องกันการรันไฟล์ประเภท VB Script เท่านั้น โดยสามารถป้องกันได้ทั้งการรันแบบโดยอัตโนมัติและแบบรันด้วยตนเอง
- วิธีการนี้เป็นวิธีการป้องกันไม่ให้เครื่องคอมพิวเตอร์ติดไวรัสประเภท VB Script เท่านั้น ไม่ใช่วิธีการแก้ไขสำหรับเครื่องที่ติดไวรัสแล้ว
- วิธีการนี้ไม่ใช่วิธีป้องกันไม่ให้ Flash drive ไม่ติดไวรัสประเภท VB Script
- วิธีการนี้ต้องใช้สิทธิ์ระดับ Administrator ในการรันคำสั่ง

แหล่งที่มา : http://www.truechonburi.com

เผยแพร่โดย : กลุ่มงานเทคโนโลยีสารสนเทศเพื่อการจัดการสำนักงาน