วิธีการจัดการ Hacked by godzilla

ปัญหา

เนื่องจากการใช้งานคอมพิวเตอร์เข้ามามีบทบาทในชีวิตประจำวันเพิ่มมากขึ้น ทั้งอำนวยความสะดวก สร้างความบันเทิง และอื่น ๆ แต่การทำงานกับคอมพิวเตอร์ก็หนีไม่พ้นผู้ประสงค์ร้ายที่ชอบสร้างสิ่งเข้ามาก่อกวนการทำงานของเครื่องคอมพิวเตอร์ ตัวอย่างเช่น ไวรัสคอมพิวเตอร์ เป็นต้น Hacked by Godzilla เป็นไวรัสตัวใหม่ที่กำลังระบาดอยู่ จัดเป็น spyware ที่ก่อกวนการทำงานมากกว่าจะทำลายข้อมูล โดยจะเป็นการติดผ่าน Handy Drive และ Floppy Disk เท่านั้น

วิเคราะห์

ลักษณะอาการเมื่อเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ติดไวรัส Hacked by godzilla

1. เครื่องจะไม่สามารถ Double Click เปิดไดร์ฟต่าง ๆ ได้ แต่จะคลิกเมาส์ขวาเพื่อเปิดไดร์ฟโดยเลือกเมนู Open หรือ Explore
2. มีข้อความปรากฏบน Title Bar ของ Internet Explorer ว่า “Hacked by godzilla”

วิธีแก้ปัญหา

1. Double Click ไอคอน My Computer ที่ Desktop เลือกเมนู Tools --> Folder Options
2. ปรากฏไดอะล็อก Folder Options คลิกแท็บ View
   2.1 คลิกเลือก Show Hidden files and folders
   2.2 เอาเครื่องหมาย / ในช่องสี่เหลี่ยมหน้า Hide extention… และ Hide protected operating system file ออก
   2.3 คลิก OK
3. กดปุ่ม Ctrl+Alt+Delete ที่คีย์บอร์ด
4. ปรากฏไดอะล็อกบ็อก Windows Task Manager คลิกเลือกแท็บ Processes
   4.1 คลิกเลือกเมนู Image Name (เพื่อ sort File)
   4.2 คลิกเลือกไฟล์ wscript.exe (ทีละตัว)
   4.3 คลิกปุ่ม End Process
5. เปิดไดร์ฟ (โดยคลิกเม้าส์ขวาเลือก Explore ห้าม Double Click ไดร์ฟ) ทำการลบไฟล์ autorun.inf และ MS32DLL.dll.vbs ออก (โดยกด Shift + Delete) ทุกไดร์ฟที่มีอยู่ในเครื่องคอมพิวเตอร์ซึ่งรวมทั้ง Handy Drive และ Floppy disk ด้วย

6. เปิดโฟลเดอร์ C:\WINDOWS เพื่อลบไฟล์ MS32DLL.dll.vbs ออก (โดยกด Shift + Delete)
7. ไปที่ปุ่ม Start --> Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่ง regedit กดปุ่ม OK ปรากฏไดอะล็อกบ็อก Registry Edit
8. คลิกเลือก HKEY_LOCAL_MACHINE --> Software --> Current Version --> Run เพื่อลบไฟล์ MS32DLL (โดยการกดปุ่ม Delete ที่คีย์บอร์ด)
9. คลิกเลือก HKEY_CURRENT_USER --> Software --> Microsoft --> Internet Explorer --> Main เพื่อลบไฟล์ที่ Window Title “Hacked by Godzilla” ออก (โดยการกดปุ่ม Delete ที่คีย์บอร์ด)
10. คลิกปุ่ม Start --> Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่ง gpedit.msc กดปุ่ม OK ปรากฏไดอะล็อกบ็อก Group Policy
11. คลิกเลือก User Configuration --> Administrative Templates --> System --> Double Click ไฟล์ Turn Off Autoplay ปรากกฏไดอะล็อกบ็อก Turn Off Autoplay Properties
    11.1 คลิกเลือก Enabled
    11.2 คลิกเลือก All drives
    11.3 คลิก OK
    เพื่อป้องกันการเปิดไดร์ฟอัตโนมัติในกรณีที่นำแผ่นซีดี หรือ Handy Drive มาใช้งานซึ่งเป็นช่องทางที่จะทำให้เกิดการติดไวรัสได้ง่ายขึ้น
12. คลิกปุ่ม Start --> Run ปรากฏไดอะล็อกบ็อก Run พิมพ์คำสั่ง msconfig กดปุ่ม OK ปรากฏไดอะล็อกบ็อก System Configuration Utility คลิกแท็บ Startup
    12.1 เอาเครื่องหมาย / ในช่องสี่เหลี่ยมหน้าไฟล์ MS32DLL ออก
    12.2 คลิกปุ่ม Apply
    12.3 คลิกปุ่ม OK (หรือ Close)
    จะปรากฏไดอะล็อกบ็อก System Configuration เลือก Exit Without Restart
13. Double Click ไอคอน My Computer ที่ Desktop เลือกเมนู Tools --> Folder Options
14. ปรากฏไดอะล็อก Folder Options คลิกแท็บ View
    14.1 คลิก / ในช่องสี่เหลี่ยมหน้า Hide extention… และ Hide protected operating system file
    14.2 คลิก OK
15. Click เม้าส์ขวาที่ไอคอน Recycle bin เพื่อเรียก Shortcut Menu เลือกคำสั่ง Empty Recycle bin เพื่อยืนยันการลบไฟล์ไวรัสออกจากเครื่องคอมพิวเตอร์อีกครั้ง

ตรวจสอบการแก้ปัญหา

เมื่อทำการแก้ไขครบตามวิธีการทั้งหมดเรียบร้อยแล้ว สามารถตรวจสอบว่าไวรัสได้ถูกกำจัดแล้วหรือไม่ ได้ดังนี้

1. สามารถ Double Click เปิดไดร์ฟต่าง ๆ ได้ที่มีได้
2. เมื่อเปิดหน้าต่าง Internet Explorer แล้ว Title bar ของ IE จะต้องไม่มีคำว่า “Hacked by godzilla”
3. เมื่อเสียบ Handy Drive จะต้องไม่ Autorun

ข้อเสนอแนะ

1. ควรจะแน่ใจว่าเลือกไฟล์หรือ register ที่ต้องการจะลบได้ถูกต้องเพราะหากลบผิดอาจทำให้ระบบปฏิบัติการเสียหายได้
2. เมื่อนำ Handy Drive มาเสียบใหม่ควรจะตรวจสอบไฟล์ภายในเสียก่อนว่าเป็นไฟล์ไวรัสหรือไม่