

## เรื่องง่ายๆที่ใครๆ(คง)รู้แล้ว

นำเสนอเมื่อ : 25 ม.ค. 2552

วันนี้ ไปอ่านเจอบทความ **"ป้องกันภัยจากอุปกรณ์เอสบี"** ใน นสพ.ไทยโพสต์ ฉบับวันอาทิตย์ที่ 27 เมษายน 2551 มีเทคนิคที่น่าสนใจ ซึ่งก็เคยใช้อยู่ แต่บางจุดบางประเด็นก็ฟังจะทราบ เลยคิดว่า น่าจะนำมาเผยแพร่ต่อและลองหาคำพามาประกอบบทความเพื่อให้เข้าใจมากยิ่งขึ้น เพื่อเป็นประโยชน์แก่ผู้ใช้คอมพิวเตอร์ทั่วไป

โดย ที่ในชีวิตประจำวันบางคนก็คงเจอพิษสงอันร้ายกาจของไวรัสมาแล้วบ้าง เช่น เสียบยูเอสบีแฟลชเมมโมรี่จากเครื่องพีซีที่หนึ่ง (ในห้องเรียน) แล้วเอาไปเสียบเปิดที่คอมพิวเตอร์ที่บ้านหรือที่ทำงาน ปรากฏว่า เจอไวรัสคอมพิวเตอร์เล่นงานซะแล้ว (เจอบยเลย...) เลยอยากนำมา เตือนไว้ ว่า จริงๆ มันก็พอมีทางป้องกันได้ ถ้าเราเอาใจใส่เล็กน้อยและทำให้เป็นนิสัย ก็จะไม่ค่อยมีปัญหาอะไรทั้งปวง

### **ประเด็นแรก ทำไมเราจึงติดไวรัสคอมพิวเตอร์ได้จากอุปกรณ์เอสบีได้**



บทความที่ ผู้เขียน ว่า มันคืออาการคล้ายโรคในคน คือ อาการ **"สำล่อน"** ของอุปกรณ์ที่ผู้ใช้มักจะนำเจ้าพวกนี้ไปจิ้มกับเครื่องคอมพิวเตอร์มากหน้า หลายตา บางตัวรู้จัก บางตัวไม่รู้จัก และส่วนใหญ่ดำเนินการด้วยความไม่ระวัง ซึ่งสิ่งที่ไม่พึงประสงค์ที่ตามมาจากพฤติกรรมดังกล่าวก็คือ **"การติดเชื้อไวรัสคอมพิวเตอร์"**



ต้อง ยอมรับว่า การแพร่หลายของอุปกรณ์ดังกล่าวนี้เอง ทำให้กลุ่มมิจฉาชีพใช้ประโยชน์จากจุดอ่อนของแฟลชเมมโมรี่ที่มีอยู่ส่งไวรัส เข้าแทรกแซง เพื่อแพร่กระจายไวรัสไปยังที่ต่างๆ จนในที่สุดถึงขั้นขณะนี้เจ้าแฟลชเมมโมรี่ได้กลายเป็นพาหะอันดับหนึ่ง ที่นำ เชื้อไวรัสไประบาดทำลายระบบคอมพิวเตอร์มากที่สุด โดยหากใส่ยูเอสบีแฟลชคอมพิวเตอร์หรือตัวอื่นๆ รอยละ 90 ของคนเหล่านี้ จะต้องมีประสบการณ์ที่แฟลชไดรฟ์ของตัวเองนำไวรัสที่ไม่พึงประสงค์แฝงตัวเข้ามา มาติดในเครื่องที่ใช้ด้วย ทั้งนี้ ในปัจจุบันไวรัสที่มากพร้อมอุปกรณ์เชื่อมต่อยูเอสบี มักจะเป็นไวรัสที่โปรแกรมจัดการไวรัสตรวจสอบไม่พบ (อัน นี้แล้วแต่ความเก่งของโปรแกรมป้องกันไวรัสครับ ถ้าเป็นโปรแกรมแท้ๆ และผู้ใช้งานมันดูแล้วพอเหตุให้โปรแกรมทันสมัยอยู่ตลอดเวลาพอจะตรวจเจอ ไวรัสเหล่านี้ได้) และเมื่อไวรัสเข้ามาติดในเครื่องแล้ว นอกจากทำลายระบบปฏิบัติการของเครื่องให้อยู่เปรี๊ยะเสียแล้ว บางครั้งมัน ยังเข้ามาควบคุมเครื่องเรา (บีตเน็ต) และถูกนำไปใช้ในทางที่มีขอบข่ายอื่น ตามบัญชีของผู้ที่เขียนไวรัสเหล่านี้ขึ้นมา

ดังนั้น เพื่อเป็นการป้องกันไม่ให้เครื่องคอมพิวเตอร์ จะต้องเผชิญกับความเสียหายที่มากพร้อมกับอุปกรณ์เอสบีเหล่านี้ก็อีก จึงจะขอแนะนำวิธีการป้องกันดังกล่าว โดยที่ไม่ต้องพึ่งโปรแกรมฆ่าไวรัสเสียเวลา เพียงแค่ใส่ใจและระมัด ระวังมันซักนิด เครื่องของคุณก็จะห่างไกลจากไวรัสที่แสนจะอันตราย ที่จะทำให้อุปกรณ์เสียเวลาและเสียเงินไปโดยเหตุที่ไม่ควรจะเสีย



ก่อนอื่นต้องเข้าใจกันก่อนว่า โดยปกติไวรัสที่มาพร้อมกับอุปกรณ์เอสบีและแฟลชเมมโมรี่นั้น ไม่สามารถที่รันโปรแกรมได้ด้วยตัวเอง ขณะเสียบแฟลชไดรฟ์กับเครื่องคอมพิวเตอร์ แต่สาเหตุที่ติดก็เพราะ ความอัจฉริยะของวินโดวส์ที่รองรับระบบ Plug and Play ซึ่งพร้อมที่ทำการ Autorun ทุกอุปกรณ์ที่เข้ามาติดต่อตัวเครื่องคอมพิวเตอร์ ซึ่งตัวนี้เป็นจุดอ่อนที่ผู้เขียนไวรัสส่วนใหญ่นำมาใช้เป็นตัวเปิดโปรแกรม นั่นก็คือไฟล์ที่ชื่อว่า Autorun.inf

ดังนั้น เพียงแค่เสียบอุปกรณ์เข้าไปและเครื่องทำการ Autorun อุปกรณ์ก็ติดไวรัสแล้ว และวิธีอีกประการหนึ่งที่ทำให้เราติดไวรัสก็คือ การดับเบิลคลิกไปที่โฟลเดอร์ไวรัส ซึ่งพักหลังๆ จะเห็นว่ามีผู้พัฒนาไวรัสแบบยกมาขึ้น (พวกนี้เก่งครับ แต่ทำเรื่องไร้สาระซะมาก) โดยสั่งการให้ไวรัสทำการกอบปีตัวเองเป็น โฟลด์หรือโฟลเดอร์งานของเรา และทดลองเราให้ดับเบิลคลิกที่งานชิ้นนั้น ซึ่งหากคลิกไปแล้วเจ้าไวรัสตัวร้ายก็จะมุ่งเข้ามาในระบบคอมพิวเตอร์ของเรา ทันที



### **ประเด็นที่สอง แล้วจะป้องกันไวรัสจากอุปกรณ์เหล่านี้ อย่างไร**

เมื่อ ทุราบถึงปัญหาแล้วก็จะพบว่าเจ้า Autorun เป็นตัวต้นเหตุของเรื่องทั้งหมด ซึ่งสามารถชี้ขาดชะตาของเครื่องคอมพิวเตอร์ของเราได้เลย ซึ่งหากเปรียบ Autorun เป็นนายคนเราก็ต้องสั่งการให้นายคนคนนั้น จะทำอะไรการสร้งทุกสิ่งทุกอย่าง ก่อนที่จะปล่อยให้ลงแปลงปลอมเขาสูเมืองของเรา นั่นก็หมายถึงผู้ใช้หรือเจ้าเมืองจะต้องทำการหยุดการ Autoplay การทำงานของ Autorun ก่อน ทั้งนี้เพื่อป้องกันไม่ให้ปลอมแปลงที่อาจจะแฝงเข้ามา สำหรับวิธีการหยุด Auto play ก็เริ่มจาก



1.ไปที่ Start > Run แล้วพิมพ์ว่า gpedit.msc กด OK ก็จะได้หน้าต่าง Group Policy ขึ้นมา



2.จากหน้าต่าง Group Policy ก็ให้เข้าไปตามเส้นทางนี้ User Configuration > Administrative Templates > System

3.จากนั้นจะปรากฏข้อความที่หน้าต่าง ให้เราเลือกดับเบิลคลิกคำว่า Turn off Autoplay และ



4.ในหน้าต่างให้ติดตั้งนี้

4.1 ตรง Option Button เลือกเป็น Enable

4.2 ใน list Box ให้เลือกเป็น All Drive เสร็จแล้วกด Apply และ OK

เท่า นี้ก็สามารถหยุดการรันคำสั่งเรียกไวรัสได้แล้ว แต่ถึงขั้นนี้แล้วยังฟังซะล้าใจ เพราะหากไวรัสมันยังอยู่ในอุปกรณ์มันก็ยังเป็นอันตรายอยู่ โดยไฟล์ของไวรัสเหล่านี้มันมักจะซ่อนอยู่ โดยปกติจะมองไม่เห็น แต่หากอยากให้เห็นก็ต้องแก้ไขตามนี้ คือ



1.ไปที่ start > Control Panel > Folder Option,> View

(แล้วแต่ระบบของ System ครับ อาจมีความแตกต่างกันบ้าง - ผู้เขียน)

2.ที่หัวข้อ Hidden Files and Folders ให้เลือกเป็น "show all hidden files and folders"

3.ติ๊กถูกที่ "Display the contents of system Folders"

4.ติ๊กเอาเครื่องหมายถูกตรง "Hide extensions for know file types" ออก

5.ติ๊กเอาเครื่องหมายถูกตรง "Hide protected operating system files (Recommended)" ออก

(ขอ นี้ ต้องระวังสำหรับผู้ใช้งานที่ไม่ชำนาญ เพราะ อาจมีการเผลอไปเปิด Folder ที่เป็นโปรแกรม หรือ ระบบปฏิบัติการ แล้ว เผลอหรือมั่วย้ายไฟล์หรือลบไฟล์เกี่ยวกับการทำงานของเครื่องคอมพิวเตอร์ ทำให้เกิดความเสียหายต่อโปรแกรมหรือระบบปฏิบัติการได้ จึงไม่แนะนำสำหรับเครื่องคอมพิวเตอร์ที่มีคนที่ใช้งานหลายคน - ผู้เขียน)

แต่ นี้เราก็สามารถหาตัวเจ้าไวรัสที่ซ่อนอยู่ ซึ่งการตรวจพบก็ง่ายมากเพียงไปที่อุปกรณ์ที่เราจะเลือก จากนั้นแค่เพียงคลิกขวาและเลือก Explore

แทนที่จะดับเบิลคลิกที่ไดรฟ์ ซึ่งวิธีการนี้เป็นที่ autorun ที่ดับเบิลคลิกได้ จากนั้นก็จะเห็นไฟล์และโฟลเดอร์ต่างๆ ซึ่งหากเลือกดูในมุมมอง details พบว่า เจ้าตัวที่จางๆ มีสถานะเป็น applicationก็จัดการลบได้เลย โดยการกด Shift+Delete แทนที่ก็เรียบร้อยแล้ว



อย่างไรก็ดีหากลบหมดแล้ว เพื่อความสบายใจจะฟอร์แมตตัวแฟลชไดรฟ์ใหม่ก็ไม่มี ไรว่า และคราวหลังหากต้องนำอุปกรณ์ต่อเชื่อมแบบยูเอสบีมาใช้ก็ขอแค่อย่าลืมดับเบิลคลิกและให้หน้าต่างคลิกขวา เลือก Explore แทนวิธีการนี้จะปลอดภัยกว่า ซึ่งหากปฏิบัติตามขั้นตอนที่ใหม่นี้ เชื่อว่าจะช่วยสร้างภูมิคุ้มกันให้กับคอมพิวเตอร์ของคุณเป็นอย่างดี

---

อ้างอิงจาก นสพ.ไทยโพสต์ 27 เมษายน 2551 คอลัมน์ ไอที

