เรื่องง่ายๆที่ใครๆ(คง)รู้แล้ว

นำเสนอเมื่อ : 25 ม.ค. 2552

วันนี้ ไปอ่านเจอบทความ **"ป้องกันภัยจากอุปกรณ์ยูเอสบี"** ใน นสพ.ไทยโพสต์ ฉบับวันอาทิตย์ที่ 27 เมษายน 2551 มีเทคนิคที่น่าสนใจ ซึ่งก็เคยใช้อยู่แต่บางจุดบางประเด็นก็พึ่งจะทราบ เลยคิดว่า นาจะนำมาเผยแพรต่อและลองหาภาพมาประกอบบทความเพื่อให้เขาใจง่ายยิ่งขึ้น เพื่อเป็นประโยชน์แก่ผู้ที่ใช้คอมพิวเตอร์ทั่วไป

โดย ที่ในชีวิตประจำวันบางคนก็คงเจอพิษสงอันร้ายกาจของไวรัสมาแล้วบ้าง เช่น เสียบยูเอสบีแฟลชเมมโมรี่จากเครื่องพีซีที่หนึ่ง (ในห้องเรียน) แล้วเอาไปเสียบเปิดที่คอมพิวเตอร์ที่บ้านหรือที่ทำงาน ปรากฏว่า เจอไวรัสคอมพิวเตอร์เลนงานซะแล้ว (เจอบอยเลย..) เลยอยากนำมา เตือนไว้ วา จริงๆ มันก็พอมีทางป้องกันได้ ถ้าเราเอาใจใส่เล็กน้อยและทำให้เป็นนิสัย ก็จะปลอดภัยด้วยประการทั้งปวง

ประเด็นแรก ทำไมเราจึงติดไวรัสคอมพิวเตอร์ได้จากอุปกรณ์ยูเอสบีได้

ในบทความนี้ ผู้เขียน ว่า มันคืออาการคล้ายโรคในคน คือ คือการ "สำส่อน" ของอุปกรณ์ที่ผู้ใช้มักจะนำเจ้าพวกนี้ไปจิ้มกับเครื่องคอมพิวเตอร์มากหน้า หลายตา บางตัวรู้จัก บางตัวไม่รู้จัก และส่วนใหญ่ดำเนินการด้วยความไม่ระวัง ซึ่งสิ่งที่ไม่พึงประสงค์ที่ตามมาจากพฤติกรรมดังกล่าวก็คือ **"การติดเชื้อไวรัสคอมพิวเตอร์"**

ต้อง ยอมรับว่า การแพร่หลายของอุปกรณ์ดังกล่าวนี้เอง ทำให้กลุ่มมิจฉาชีพใช้ประโยชน์จากจุดอ่อนของแฟลชเมมโมรี่ที่มีอยู่ส่งไวรัส เข้าแทรกแซง เพื่อแพร่กระจายไวรัสไปยังที่ต่างๆ จนในที่สุดถึงขณะนี้เจาแฟลชเมมโมรีใดกลายเป็นพาหะอันดับหนึ่ง ที่นำ เชื้อไวรัสไประบาดทำลายระบบคอมพิวเตอร์มากที่สุด โดยหากให้สุ่มถามผู้ใช้คอมพิวเตอร์เชื่อว่ากว่า รอยละ 90 ของคนเหลานี้ จะต้องมีประสบการณ์ที่แฟลชไดรฟ์ของตัวเองนำไวรัสที่ไม่พึงประสงค์แฝงตัวเขา มาติดในเครื่องที่ใช้ด้วย

ทั้งนี้ ในปัจจุบันไวรัสที่มาพรอมกับอุปกรณ์เชื่อมตอยูเอสบี มักจะเป็นไวรัสที่โปรแกรมจัดการไวรัสตรวจสอบไมพบ (อัน นี้แลวแตความเกงของโปรแกรมป้องกันไวรัสครับ ถ้าเป็นโปรแกรมแท้ๆ และผู้ใช้งานมั่นดูแลอัพเดทให้โปรแกรมทันสมัยอยู่ตลอดเวลาก็พอจะตรวจเจอ ไวรัสเหล่านี้ได้) **และเมื่อไวรัสเขามาติดในเครื่องแล้ว นอกจากทำลายระบบปฏิบัติของเครื่องใหงอยเปรี้ยเสียขาแล้ว บางครั้งมัน ยังเขามาควบคุมเครื่องเรา (บ็อตเน็ต) และถูกนำไปใช้ในทางที่มิชอบอย่างอื่น ตามบัญชาของผู้ที่เขียนไวรัสเหลานี้ขึ้นมา**

ดัง นั้น เพื่อเป็นการป้องกันไม่ให้เครื่องคอมพิวเตอร์ จะต้องเผชิญกับความเสี่ยงที่มาพร้อมกับอุปกรณ์ยูเอสบีเหล่านี้อีก จึงจะขอแนะนำวิธีการป้องกันตัวง่ายๆ โดยที่ไม่ต้องพึ่งพาโปรแกรมฆ่าไวรัสให้เสียเวลา เพียงแค่ใส่ใจและระมัด ระวังมันซักนิด เครื่องของคุณก็จะหางไกลจากไวรัสที่แสนจะอันตราย ที่จะทำให้คุณทั้งเสียเวลาและเสียเงินไปโดยเหตุที่ไมควรจะเสีย

ก่อน อื่นต้องเข้าใจกันก่อนว่า โดยปกติไวรัสที่มาพร้อมกับอุปกรณ์ยูเอสบีและแฟลชเมมโมรี่นั้น ไม่สามารถที่รันโปรแกรมได้ด้วยตัวเอง ขณะเสียบแฟรชไดรฟ์กับเครื่องคอมฯ ได้ แต่สาเหตุที่ติดก็เพราะ ความอัจฉริยะของวินโดวน์ที่รองรับระบบ Plug and Play ซึ่งพร้อมที่ทำการ Autorun ทุกอุปกรณ์ที่เข้ามาติดต่อตัวเครื่องคอมฯ **ซึ่งตัวนี้เป็นจุดออนที่ผู้เขียนไวรัสนำมันมาใชเป็นตัวเปิดโปรแกรม นั่นก็คือไฟล์ที่ชื่อวา Autorun.inf**

ดังนั้น เพียงแค่เสียบอุปกรณ์เข้าไปและเครื่องทำการ Autorun อุปกรณ์ก็ติดไวรัสแล้ว และวิธีอีกประการหนึ่งที่ทำให้เราติดไวรัสก็คือ การดับเบิลคลิกไปที่โฟลเดอร์ไวรัส **ซึ่งพักหลังๆ จะเห็นวาผู้พัฒนาไวรัสแยบยลมากขึ้น (พวกนี้เกงครับ แตทำเรื่องไรสาระซะมาก) โดยสั่งการให้ไวรัสทำการกอบปี้ตัวเองเป็นไฟล์หรือโฟลเดอรงานของเรา และหลอกเราให้ไปดับเบิลคลิกที่งานชื่อนั้น ซึ่งหากคลิกไปแลวเจาไวรัสตัวรายก็จะมุงเขามาในระบบคอมพิวเตอร์ของเรา ทันที**

ประเด็นที่สอง แล้วจะป้องกันไวรัสจากอุปกรณ์เหล่านี้ อย่างไร?

เมื่อ ทราบถึงปัญหาแลวก็จะพบวาเจา Autorun เป็นตัวตนเหตุของเรื่องทั้งหมด ซึ่งสามารถชี้ขาดชะตาของเครื่องคอมพิวเตอร์ของเราได้เลย ซึ่งหากเปรียบ Autorun เป็นนายด่านเราก็ตองสั่งการโหนายดานคนนี้ จะตองทำการสกรีนทุกสิ่งทุกอย่าง กอนที่จะปลอยสิ่งแปลกปลอมเขาสูเมืองของเรา นั่นก็หมายถึงผู้ใชหรือเจาเมืองจะตองทำการหยุดการ Autoplay การทำงานของ Autorun กอน ทั้งนี้เพื่อบล็อกสิ่งแปลกปลอมที่อาจจะแฝงเขามา

สำหรับวิธีการหยุด Auto play ก็เริ่มจาก

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

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

3.จากนั้นจะปรากฏขอความที่หนาตาง ใหเราเลือกดับเบิลคลิกคำวา Turn off Autoplay และ

4.ในหน้าต่างให้ใส่ดังนี้

4.1 ตรง Option Button เลือกเป็น Enable

4.2 ใน list Box ให้เลือกเป็น All Drive เสร็จแล้วกด Apply และ OK

เทา นี้ก็สามารถหยุดการรันคำสั่งเรียกไวรัสได้แลว แต่ถึงขั้นนี้อยาเพิ่งชะล่าใจ เพราะหากไวรัสมันยังอยู่ในอุปกรณ์มันก็ยังเป็นอันตรายอยู่ โดยไฟล์ของไวรัสเหล่านี้มันมักจะซอนอยู่ โดยปกติจะมองไม่เห็น แตหากอยากจะเห็นก็จะตองแก้ไขตามนี้ คือ

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

(แลวแตระบบของ System ครับ อาจมีความแตกตางกันบาง - ผู้เขียน)

2.ที่หัวขอ 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 ตองระวังสำหรับผู้ใชงานที่ไมชำนาญ เพราะ อาจมีการเผลอไปเปิด Folder ที่เป็นโปรแกรม หรือ ระบบปฏิบัติการ แล้วเผลอหรือมั่วยายไฟล์หรือลบไฟล์ที่เกี่ยวกับการทำงานของเครื่องคอมพิวเตอร์ ทำให้เกิดความเสียหายตอโปรแกรมหรือระบบปฏิบัติการได จึงไมแนะนำสำหรับเครื่องคอมพิวเตอรีที่มีคนที่ใชงานหลายคน - ผู้เขียน)

แค นี้เราก็สามารถหาตัวเจาไวรัสที่ซอนอยู ซึ่งการตรวจพบก็งายมากเพียงไปที่อุปกรณ์ที่เราจะเลือก จากนั้นแค่เพียงคลิกขวาและเลือก Explore แทนที่จะใช้ดับเบิลคลิกที่ไดรฟ์ ซึ่งวิธีการนี้เป็นการหนี autorun ที่ใชดับเบิลคลิกได จากนั้นก็จะเห็นไฟลและโฟลเดอรจางๆ ซึ่งหากเลือกดูในมุมมอง details พบว่า เจ้าตัวที่จางๆ มีสถานะเป็น applicationก็จัดการลบไดเลย โดยการกด Shift+Delete เทานี้ก็เรียบรอย

อย่าง ไรก็ดีหากลบหมดูแล้ว เพื่อความสบายใจจะฟอร์แมตตัวแฟลชไดรฟ์ใหม่ก็ไม่มี ใครว่า และคราวหลังหากต้องนำอุปกรณ์ต่อเชื่อมแบบยูเอสบีมาใช้อีก ก็ขอแค่อย่าลืมตัวดับเบิลคลิกและให้หันมาใชคลิกขวา เลือก Explore แทนวิธีการนี้จะปลอดภัยกวา ซึ่งหากปฏิบัติตามขั้นตอนที่ไหมานี้ เชื่อวาจะชวยสรางภูมิคุมกันให้กับคอมพิวเตอรของคุณเป็นอยางดี

อ้างอิงจาก นสพ. ไทยโพสต์ 27 เมษายน 2551 คอลัมน์ ไอที