ฉบับอ่านเสริม เติมเต็มเนื้อหา

DKD C

ล้วงไต! ไวรัส

Add-Ons

ปรับปรุงล่าสุด 25 ก.ค. 52

ปิยวัฒน์ เกลี้ยงขำ

ฉบับพิเศษ

เพิ่มเติมเนื้อหาที่ไม่ได้ตีพิมพ์ในหนังสือ

ล้วงไต๋! ไวรัส Add-Ons

WWW.DKDC-ULTRA.COM

ความเป็นมาของหนังสือ

หนังสือล้วงไต๋ฯฉบับนี้ ผมตั้งใจจัดทำขึ้นมาเพื่อเป็นการเสริมและเติมเต็มเนื้อหาของหนังสือล้วงไต๋ฯทั้ง 2 เล่ม เนื่องจากมีบางเรื่องราวที่ผมเห็นว่ามีความเกี่ยวข้องหรือต่อเนื่องกับเนื้อหาในหนังสือ แต่ผมเองเพิ่งจะรู้หรือเพิ่งได้ศึกษาอย่างลึกซึ้งหลังจากได้มีการจัดพิมพ์หนังสือไปแล้วทำให้ไม่สามารถที่จะเพิ่มเติมเนื้อหาเหล่านั้นลงในหนังสือได้

ดังนั้นเพื่อประโยชน์สูงสุดแก่ผู้อ่านที่ให้การสนับสนุนหนังสือของผม รวมผู้ที่สนใจทั่ว ๆไป ผมจึงตัดสินใจที่จะทำหนังสือเล่มนี้ขึ้นมาเพื่อเป็นการเพิ่มเติมเนื้อหา รวมถึงปรับปรุงเนื้อหาในบางส่วนในหนังสือที่อาจจะมีความผิดพลาดหรือคลาดเคลื่อนไป ซึ่งผมจะพยายามเพิ่มเติมเนื้อหาใหม่ ๆโดยเฉพาะเนื้อหาที่เห็นว่ามีความต่อเนื่องกับในหนังสือเสมอ ๆครับ

และเนื่องจากหนังสือฉบับนี้ผมได้จัดทำขึ้นเอง ดังนั้นรูปแบบของการจัดหน้าอาจจะไม่สวยงามเหมือนในหนังสือที่มีทีมงานในการจัดทำนะครับ ถ้าผิดพลาดประการใดผมก็ต้องขออภัยไว้ด้วยนะครับ

ปิยวัฒน์ เกลี้ยงขำ

Chapter 1. ล้วงไต Autorun +Autoplay

ความแตกต่างระหว่าง Autorun และ Autoplay

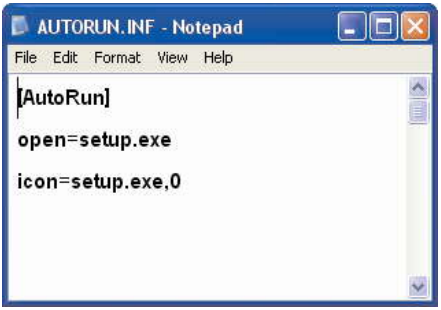
ที่ผ่านมานั้นหลายๆคน(รวมถึงผมด้วย ที่ใช้สับสนในเล่มแรกต้องขออภัยจริงๆครับ)มักจะใช้คำทั้ง 2 คำนี้โดยคิดว่ามันมีความหมายเดียวกัน จนเมื่อลองศึกษาค้นคว้าอย่างจริงจังจึงได้เข้าใจว่าคำทั้ง2คำนั้นมีความหมายต่างกันครับ ผมเห็นว่าน่าสนใจดีเลยเอามาเล่าสู่กันฟังเพื่อจะได้ทำความเข้าใจกันใหม่และแก้ไขปัญหาไวรัสที่เกิดจากไฟล์ Autorun.inf ได้ถูกต้องตรงจุดครับ

รู้จักกับ Autorun

สำหรับคำว่า Autorun นั้นเป็นสิ่งที่มีมานานแล้ว(เริ่มตั้งแต่ Windows 95 เป็นต้นมา) คู่กับเจ้าไฟล์ Autorun.inf นั่นล่ะครับซึ่งทุกคนก็คงเข้าใจแล้วว่ามันคือการทำงานตามคำสั่งที่มีการระบุไว้ในไฟล์ Autorun.inf ตามที่ผมได้อธิบายไปแล้วในเล่มแรก

เช่นการทำงานของ Autorun ในแผ่นติดตั้ง Windows เมื่อเรานำแผ่นใส่ในเครื่องจะเห็นว่ามันจะทำการเปิดโปรแกรมเมนูในการติดตั้ง Windows มาให้ทันที

เราลองมาดูคำสั่งภายในไฟล์ Autorun.inf ซึ่งอยู่ในแผ่นติดตั้ง Windows กันก่อนนะครับแล้วเดี๋ยวผมจะอธิบายเพิ่มเติมอีกที



จะเห็นได้ว่าภายในไฟล์ Autorun.inf นั้นมีส่วนของคำสั่งเพียง 2 บรรทัดคือ Open= ซึ่งจะเป็นส่วนที่ระบุชื่อของโปรแกรมที่ต้องการให้เปิดขึ้นมาแบบอัตโนมัติเมื่อนำแผ่นใส่เข้าไปในไดรฟ์ รวมไปถึงการดับเบิ้ลคลิกที่ไดรฟ์นั้นๆใน My Computer ด้วย

และบรรทัด icon= ซึ่งเป็นส่วนที่ใช้ระบุรูปไอคอนที่จะแสดงให้เห็นนั่นเองครับ(คำสั่งของไฟล์ Autorun.inf ในหน้า 104 ล้วงไต๋ฯ เล่ม1)

ดังนั้นผมขอสรุปในขั้นต้นก่อนนะครับว่า Autorun นั้นหลักการทำงานของมันก็คือการอ่านแล้วทำตามคำสั่งที่มีการระบุไว้ในไฟล์ Autorun.inf ทั้งหมดไม่ว่าจะเป็นส่วนแสดงชื่อไดรฟ์(Label) รูปไอคอนที่แสดงแทนไดรฟ์รวมถึงโปรแกรมที่จะทำการเปิดขึ้นมาแบบอัตโนมัติ

รู้จักกับ Autoplay

คำว่า Autoplay นั้นเป็นคำใหม่(มาทีหลัง Autorun) ที่เพิ่งมีมาพร้อมกับ Windows ตั้งแต่ XP ขึ้นไป เรามาดูรูปตัวอย่างการทำงานของ Autoplay กันก่อนนะครับแล้วผมจะอธิบายต่อว่ามันคืออะไร

สำหรับรูปที่เห็นนั้นเป็นการทำงานของ Autoplay ครับ ทุกคนคงคุ้นเคยกันดีอยู่แล้ว นั่นคือเมื่อเราเสียบแฟลชไดรฟ์เข้ากับเครื่องคอมพิวเตอร์ก็จะมีหน้าต่างลักษณะนี้ขึ้นมาเสมอๆ(ถ้าไม่ได้ปิด Autoplay ไว้) โดยจากรูปตัวอย่างที่ผ่านมานั้นในแฟลชไดรฟ์ของผมจะมีเพียงไฟล์รูปภาพอยู่ด้านใน

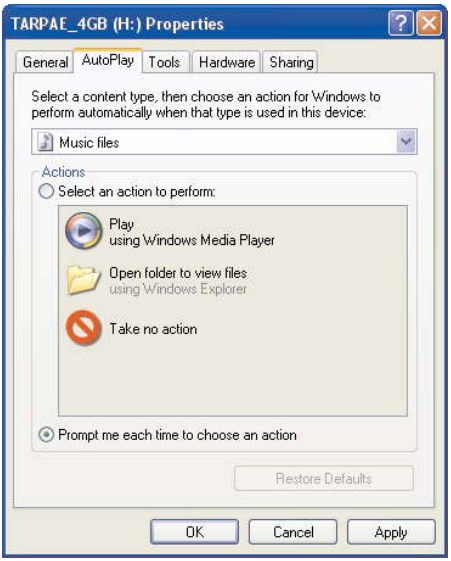
คราวนี้ผมจะลองก๊อบปี้ไฟล์เพลง .mp3 ใส่เพิ่มเข้าไปในแฟลชไดรฟ์ หลังจากนั้นดึงออกแล้วเสียบกลับเข้าไปใหม่มาดูผลกันครับ

จะเห็นได้ว่ามีหน้าต่างคล้ายๆแบบเดิมแต่ด้านบนสุดจะมีรูปไอคอนของโปรแกรม Windows Media Player ซึ่งมีคำว่า Play เพิ่มขึ้นมา นี่ล่ะครับการทำงานของ Autoplay นั่นคือมันจะทำการตรวจสอบไฟล์ทั้งหมดของเราในแฟลชไดรฟ์ว่ามีไฟล์ประเภทไหนบ้างแล้วทำการเปิดโปรแกรมที่มีความเกี่ยวข้องกับประเภทไฟล์ประเภทนั้นๆขึ้นมาให้

เช่นในตัวอย่างแรกแฟลชไดรฟ์ของผมมีเพียงไฟล์รูปภาพ มันจึงขึ้นเมนูในการจัดการรูปภาพ เช่น Print the picture , View a slideshow... ส่วนในตัวอย่างที่ 2 นั้น เนื่องจากผมได้ก๊อบปี้ไฟล์เพลงใส่เพิ่มเข้าไปด้วย

เมื่อมันตรวจพบว่ามีไฟล์เพลงอยู่จึงแสดงเมนูที่จะใช้จัดการกับไฟล์เพลงซึ่งก็คือการเปิดด้วยโปรแกรม Windows Media Player นั่นเอง ซึ่งถ้าผมเลือก Play มันก็จะทำการเปิดเพลงจากในแฟลชไดรฟ์ขึ้นมาให้ หรือถ้าผมเลือกไปที่ View a slideshow... มันก็จะทำการเปิดไฟล์รูปภาพจากในแฟลชไดรฟ์ขึ้นมาให้นั่นเองครับ คงพอจะมองเห็นภาพการทำงานของ Autoplay กันแล้วนะครับ

ซึ่งเราสามารถที่จะตั้งค่าการทำงานแบบอัตโนมัติของ Autoplay ได้ว่าในกรณีที่พบไฟล์ประเภทไหนจะให้มันตอบสนองอย่างไรโดยการคลิกขวาที่ไดรฟ์ที่ต้องการตั้งค่าเช่นผมต้องการตั้งค่าแฟลชไดรฟ์ซึ่งตอนนี้เป็นไดรฟ์ H ผมก็คลิกขวาที่ไดรฟ์ H เลือก Properties แล้วไปที่ Tab Autoplay



จะเห็นว่าเราสามารถที่จะเลือกประเภทของไฟล์และรูปแบบการตอบสนองต่อไฟล์ประเภทนั้นๆเมื่อมีการเสียบแฟลชไดรฟ์ด้วยฟังก์ชั่น Autoplay ซึ่งผมขอไม่อธิบายรายละเอียดนะครับ ลองเล่นกันดูคิดว่าน่าจะทำความเข้าใจได้ไม่ยากครับ

สรุปความแตกต่างระหว่าง Autorun และ Autoplay

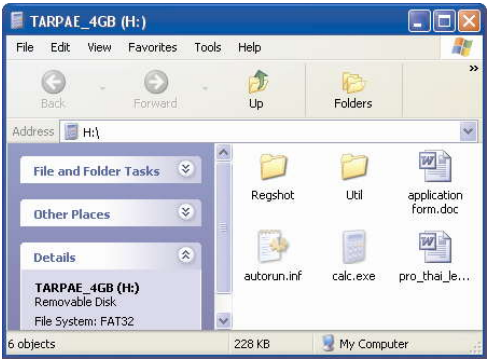
Autorun นั้นเป็นฟังก์ชั่นที่มีมากับ Windows ตั้งแต่ 95 เป็นต้นมาซึ่งการทำงานของ Autorun นั้นจำเป็นจะต้องใช้ไฟล์ Autorun.inf ในการกำหนดการทำงานเสมอ เนื่องจากจะต้องมีการระบุคำสั่งต่างๆไว้ในนั้น

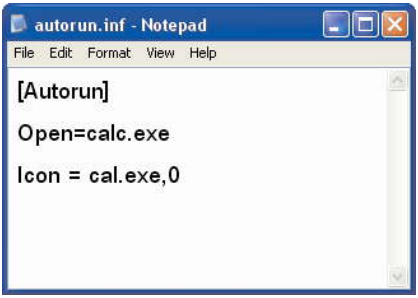
ส่วน Autoplay นั้นเป็นฟังก์ชั่นใหม่ที่เพิ่งมีใช้ครั้งแรกใน Windows XP เป็นต้นไป และในการทำงานนั้นไม่จำเป็นต้องใช้ไฟล์ Autorun.inf แต่อย่างใด เนื่องจากเป็นการอ่านไฟล์จากใน Removable Media(CD/DVD แฟลชไดรฟ์ Card-Reader ฯ) แล้วทำการเปิดโปรแกรมที่ใช้ในการจัดการกับไฟล์ประเภทนั้นๆขึ้นมาให้

โดยสรุปก็คือ Autorun นั้นจะเป็นการสั่งให้เปิดโปรแกรมที่มีอยู่ในแฟลชไดรฟ์ขึ้นมา(จากคำสั่งในไฟล์ Autorun.inf) แต่สำหรับ Autoplay นั้นจะเป็นการเปิดโปรแกรมจากภายนอกเพื่อที่จะใช้จัดการกับไฟล์ที่อยู่ภายในแฟลชไดรฟ์นั่นเองครับ หรือพูดง่ายๆว่า Autorun นั้นจะมองที่ฝั่งโปรแกรม ส่วน Autoplay นั้นจะมองที่ฝั่งของไฟล์นั่นเองครับ

ความเข้าใจผิดเรื่องการติดไวรัส

เมื่อเข้าใจความแตกต่างของทั้ง 2 คำแล้วคราวนี้เรามาดูความเข้าใจผิดที่ทำให้หลายๆคนถึงกับกลัวการนำแฟลชไดรฟ์มาใช้ในเครื่อง เพราะกังวลกันว่าอาจจะติดไวรัสได้ง่ายๆ สำหรับความเชื่อที่ว่าก็คือหลายๆคนมักจะเชื่อกันว่าถ้ามีไวรัสอยู่ในแฟลชไดรฟ์นั้นๆแล้ว เมื่อนำแฟลชไดรฟ์มาเสียบที่เครื่องเราก็จะติดไวรัสทันที ซึ่งเรื่องนี้ไม่เป็นความจริงนะครับ ลองมาดูตัวอย่างกันครับ โดยผมจะสมมุติให้โปรแกรมเครื่องคิดเลข(calc.exe) เป็นตัวไวรัสซึ่งมีการสร้างไฟล์ Autorun.inf ตามรูปนะครับ





จะเห็นได้ว่าคำสั่งภายในไฟล์ Autorun.inf นั้นจะเหมือนกับตัวอย่างแรกที่เป็นแผ่นติดตั้ง Windows เพียงแต่เปลี่ยนชื่อไฟล์ที่จะให้มันเปิดจาก Setup.exe มาเป็น calc.exe ซึ่งผมสมมุติให้เป็นตัวไวรัสนั่นเองครับ

ตอนนี้หลายคนคงคิดว่าเมื่อนำแฟลชไดรฟ์อันนี้มาเสียบที่เครื่องก็จะต้องติดไวรัสแน่นอน เพราะไวรัสมันก็จะทำงานตามคำสั่งใน Autorun.inf บรรทัด Open=calc.exe ซึ่งเป็นการเรียกตัวไวรัส (สมมุติ)ให้ขึ้นมาทำงาน เหมือนตัวอย่างของแผ่นติดตั้ง Windows ซึ่งเรียกไฟล์ Setup.exe ขึ้นมา

จริงๆแล้วเป็นความคิดที่ผิดนะครับ เนื่องจากว่าคำสั่ง Open ซึ่งกำหนดให้มีการเรียกโปรแกรมขึ้นมาทำงานแบบอัตโนมัตินั้นสามารถที่จะใช้งานได้กับไฟล์ Autorun.inf ซึ่งอยู่ในแผ่น CD/DVD เท่านั้น แต่จะไม่มีผลใดๆถ้าไฟล์ Autorun.inf นั้นอยู่ในแฟลชไดรฟ์

สรุปง่ายๆก็คือว่าถ้าเรานำไฟล์ Autorun.inf ตามตัวอย่างนี้ไปใส่ในแผ่น CD/DVD มันก็จะทำการเปิดโปรแกรมเครื่องคิดเลขให้ตามที่ระบุไว้ในบรรทัด Open=calc.exe ทันทีที่เรานำแผ่นใส่ในเครื่องหรือดับเบิ้ลคลิกที่ไดรฟ์นั้นๆ แต่ในกรณีที่ไฟล์ Autorun.inf ดังกล่าวอยู่ในแฟลชไดรฟ์ คำสั่ง Open ในบรรทัดดังกล่าวจะไม่มีผลใดๆครับไม่ว่าจะเป็นการเปิดโปรแกรมขึ้นมาให้อัตโนมัติหรือแม้แต่มีการดับเบิ้ลคลิกที่ไดรฟ์ก็ตาม

จะมีเพียงส่วนของบรรทัด Icon=calc.exe,0 ซึ่งเป็นตัวกำหนดรูปไอคอนเท่านั้นที่ทำงานโดยจะเห็นได้ว่าไอคอนของแฟลชไดรฟ์จะกลายเป็นรูปเครื่องคิดเลขแล้ว ดังนั้นตอนนี้ถ้าผมนำแฟลชไดรฟ์ดังกล่าวมาเสียบที่เครื่อง หรือแม้ผมจะทำการดับเบิ้ลคลิกที่ไดรฟ์ ตัวไวรัสก็จะยังไม่มีการทำงานนะครับ เพราะอย่างที่บอกว่าคำสั่ง Open นั้นใช้ในแฟลชไดรฟ์ไม่ได้ครับ

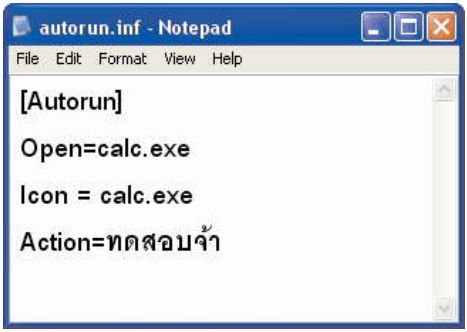
ความแตกต่างของไฟล์ Autorun.inf ในแฟลชไดรฟ์และ CD/DVD

จากในหัวข้อที่แล้วซึ่งผมบอกไว้ว่าการใช้คำสั่ง Open ของไฟล์ Autorun.inf นั้นจะไม่มีผลใดๆ ในกรณีที่ไฟล์ Autorun.inf นั้นอยู่ในแฟลชไดรฟ์ ทำไมจึงเป็นเช่นนั้น แล้วไวรัสที่ติดๆกันมันใช้วิธีการไหนล่ะ เดี๋ยวเรามาดูกันครับ

สำหรับสาเหตุที่คำสั่ง Open ในไฟล์ Autorun.inf ไม่มีผลในกรณีที่เป็นแฟลชไดรฟ์นั้นเท่าที่ผมลองค้นข้อมูลดูก็ยังไม่พบรายละเอียดหรือการยืนยันที่ชัดเจนนะครับว่าจะด้วยเหตุผลเพื่อความปลอดภัยหรือเหตุผลอื่นใดกันแน่ แต่ผมเดาเอาเองว่าอาจจะเป็นเพราะว่าตัว Autorun นั้นมีการพัฒนาขึ้นมาใช้ครั้งแรกสมัย Windows 95 ซึ่งแน่นอนว่าสมัยนั้นอุปกรณ์ที่เป็น Removable ก็จะมีเพียงฟล็อปปี้ดิสก์และแผ่น CD เท่านั้น ตัวแฟลชไดรฟ์ยังไม่มีใช้งานกัน จึงไม่ได้มีการกำหนดคำสั่ง Open ให้รองรับตัวแฟลชไดรฟ์ไว้ก็อาจเป็นได้

แต่สุดท้ายแล้วจะด้วยเหตุผลอะไรก็แล้วแต่ก็นับว่าเป็นผลดีกับผู้ใช้ครับ เพราะนับว่าเป็นการเพิ่มความปลอดภัยให้เราในการใช้แฟลชไดรฟ์ได้อีกขั้น นั่นคือเราไม่ต้องกังวลว่าเมื่อนำแฟลชไดรฟ์มาเสียบที่เครื่องแล้วจะมีการรันโปรแกรมหรือไวรัสขึ้นมาแบบอัตโนมัติโดยที่เราไม่รู้ตัว

แต่ไม่ได้หมายความว่าคำสั่ง Open ใน Autorun.inf นั้นจะไม่มีประโยชน์นะครับ เราลองมาดูตัวอย่างอีกสักตัวอย่างหนึ่ง โดยผมเพิ่มเติมคำสั่งลงไปในไฟล์ Autorun.inf หลังจากนั้นดึงแฟลชไดรฟ์ออกแล้วเสียบกลับเข้าไปใหม่แล้วมาดูผลกันครับ

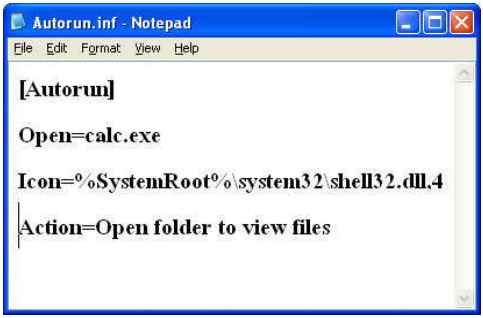


จะเห็นได้ว่าในหน้าต่างของ Autoplay นั้นจะขึ้นรูปโปรแกรมเครื่องคิดเลขเป็นเมนูบนสุดโดยมีคำว่าทดสอบจ้าเป็นชื่อของเมนู นี่คือตัวอย่างการทำงานร่วมกันระหว่างไฟล์ Autorun.inf และ Autoplay ซึ่งจะทำให้มีการเรียกใช้คำสั่ง Open ในกรณีที่เป็นแฟลชไดรฟ์ได้ครับ

นั่นคือตัว Autoplay นั้นจะอ่านชื่อที่จะแสดงในส่วนของเมนูจากคำสั่ง Action ในไฟล์ Autorun.inf และจะกำหนดให้ใช้โปรแกรมจากที่ระบุไว้ตรงคำสั่ง Open นั่นเองครับ

ดังนั้นในตอนนี้ถ้าเราทำการกด Enter หรือเลือก OK ก็จะเป็นการเปิดโปรแกรมเครื่องคิดเลข (ไวรัส)ขึ้นมาทำงานทันทีเพราะเป็นเมนูแรกที่เลือกไว้ แต่ไวรัสเท่าที่พบเห็นในช่วงหลังจะไม่ค่อยใช้วิธีนี้กันแล้วเพราะคนทั่วไปมักจะทำการปิดการทำงานของ Autoplay กันหมดแล้ว เพียงแต่อยากให้รู้กันไว้ว่าถ้าหน้า Autoplay มีการขึ้นชื่อโปรแกรมแปลกๆในเมนูแรกก็อย่าเสี่ยงไปคลิก OK หรือกด Enter เข้านะครับ เพราะจะกลายเป็นการเรียกไวรัสขึ้นมาทำงานนั่นเองครับ

แถมอีกหน่อยแล้วกันสำหรับคนที่อาจจะบอกว่าเราก็ใช้การเลือก Open folder to view files สิมันก็เปิดไดรฟ์ขึ้นมาให้เลยเหมือนๆกับการพิมพ์ชื่อไดรฟ์นั่นล่ะแล้วก็ปลอดภัยด้วย จะเสียเวลาไปพิมพ์ชื่อไดรฟ์ให้ยุ่งยากทำไม สิบล้านตัวหนังสือไม่เท่าลงมือทำครับมาดูตัวอย่างกันเพราะพบว่ามีไวรัสบางตัวใช้วิธีนี้เหมือนกัน โดยผมแก้ไฟล์ Autorun.inf ให้เป็นแบบนี้ครับ



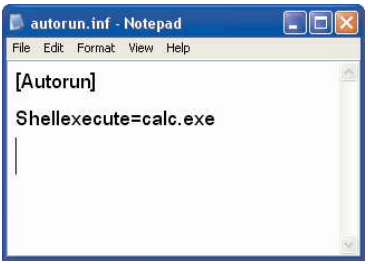
ซึ่งจะทำให้ได้หน้าต่าง Autoplay แบบนี้ครับ

จะเห็นได้ว่ามีเมนู Open folder to view files อยู่ 2 เมนู ซึ่งเมนูบนสุดนั้นเป็นตัวปลอมนะครับ (สังเกตว่าถ้าของจริง ตรงส่วนใต้ชื่อเมนูซึ่งเป็นตัวสีจางๆจะเขียนว่า using Windows Explorer ครับ ส่วนตัวปลอมข้อความส่วนนั้นจะต่างไปครับ) และแน่นอนว่าถ้ามองผ่านๆไม่ได้สังเกตมากเราก็จะเลือกเมนูบนสุด(ตัวปลอม)เพราะคิดว่าเป็นการเปิดไดรฟ์แบบธรรมดาๆ

และแน่นอนอีกเช่นกันที่มันจะเป็นการเรียกไวรัสขึ้นมาทำงานด้วยคำสั่ง Open=calc.exe จากในไฟล์ Autorun.inf ตามที่ได้อธิบายไปแล้วนั่นเองครับ ส่วนรูปแบบการอ้างอิงไอคอนในบรรทัด Icon= นั้นให้ลองดูเปรียบเทียบจาก หน้า 65(เล่ม 1)นะครับเพราะใช้หลักการเดียวกันครับ

ดังนั้นใครที่เปิด Autoplay ไว้และคิดว่าจะใช้การเลือก Open folder to view files เพื่อเปิดไดรฟ์นั้นก็ขอให้เพิ่มความระมัดระวังขึ้นอีกหน่อยนะครับจะได้ไม่ตกหลุมพรางเจ้าไวรัสมันครับ

และอย่างที่บอกว่าสำหรับไวรัสที่ใช้ช่องทาง Autoplay นั้นมีไม่มากแล้ว(แต่ก็ยังมีอยู่นะครับ) คราวนี้เราจะมาดูวิธีการที่ไวรัสมักจะใช้กันบ้าง โดยผมจะทำการแก้ไขคำสั่งใน Autorun.inf อีกครั้งให้เป็นดังนี้ครับ



จะเห็นว่าไม่มีส่วนที่กำหนดรูปไอคอนแล้ว เนื่องจากไวรัสส่วนใหญ่นั้น มันก็มักจะไม่ใช้ส่วนนี้อยู่แล้วเพราะถ้ารูปไอคอนเปลี่ยนก็จะทำให้ผู้ใช้สงสัยได้ และผมได้เปลี่ยนคำสั่งจาก Open มาเป็น ShellExecute แทนซึ่งเป็นคำสั่งที่สามารถใช้งานกับแฟลชไดรฟ์ได้

เมื่อผมแก้ไขไฟล์ Autorun.inf เรียบร้อยและดึงแฟลชไดรฟ์ออกแล้วเสียบกลับเข้าไปใหม่ ผลก็คือหน้า Autoplay นั้นก็เป็นหน้าตาตามปกติคือบนสุดมีเมนูให้เลือกจัดการกับรูปภาพตามปกติไม่มีรายชื่อโปรแกรมใดๆเนื่องจากผมลบคำสั่ง Action ออกไปแล้วและแน่นอนว่าไม่ได้มีการเปิดโปรแกรมเครื่องคิดเลขขึ้นมาให้แบบอัตโนมัติแต่อย่างใด

อ้าวแล้วคำสั่ง ShellExecute มันทำงานตอนไหนล่ะ มันไม่ได้ทำงานเหมือนคำสั่ง Open ใน CD/DVD เหรอ คำตอบคือทำ แต่ทำเพียงครั้งเดียวครับ นั่นคือมันจะไม่มีการเปิดโปรแกรมขึ้นมาแบบอัตโนมัติเมื่อเสียบแฟลชไดรฟ์เหมือนที่คำสั่ง Open ทำในกรณีที่ใส่แผ่น CD/DVD เข้าไปในไดรฟ์ครับ แต่สิ่งที่มันทำเหมือนคำสั่ง Open ก็คือเมื่อเรามีการดับเบิ้ลคลิกที่ไดรฟ์มันก็จะทำการเปิดโปรแกรมตามที่มีการระบุไว้ขึ้นมานั่นเองครับ

แต่คำสั่ง ShellExecute ก็มีจุดอ่อนที่เป็นข้อพิรุธให้ผู้ใช้สามารถสังเกตได้นะครับ นั่นก็คือในกรณีที่ใช้คำสั่ง ShellExecute เมื่อคลิกขวาที่ไดรฟ์มันจะขึ้นเมนู Autoplay อยู่บนสุดครับ

ซึ่งเท่าที่พบมานั้นสำหรับไวรัสพวก Script ส่วนใหญ่ก็ยังมีการใช้คำสั่ง ShellExecute อยู่นะครับ แต่ไวรัสที่เป็นพวก .Exe นั้นโดยส่วนใหญ่จะไม่ใช้ ShellExecute แล้วเนื่องจากมีจุดอ่อนที่ทำให้ผิด

สังเกตอย่างที่บอกไปแล้ว แต่จะมีการใช้คำสั่งในรูปแบบอื่นๆแทน ซึ่งข้อดีของคำสั่งรูปแบบใหม่นั้นนอกจากจะทำให้ไม่ขึ้นเมนู Autoplay เหมือนการใช้ ShellExecute แล้ว ข้อดีอีกอย่าง(แต่ไม่ดีกับผู้ใช้)คือถึงแม้ว่าผู้ใช้จะใช้วิธีการคลิกขวาแล้วเลือกเมนูแทนการดับเบิลคลิกก็ไม่สามารถรอดพ้นไวรัสไปได้ไม่ว่าจะเลือกเมนูไหนซึ่งผมขอยกไปอธิบายในหัวข้อถัดไปนะครับ

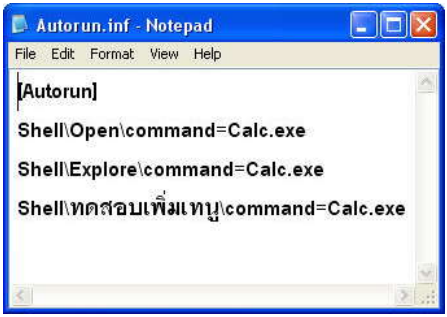
ผมขอสรุปตรงนี้ก่อนว่า สำหรับกรณีของแฟลชไดรฟ์นั้นจะไม่มีการเปิดโปรแกรมใดๆขึ้นมาเมื่อเราทำการเสียบเข้ากับเครื่องแน่นอนครับไม่ว่าในไฟล์ Autorun.inf นั้นจะระบุคำสั่ง Open หรือ ShellExecute หรือคำสั่งอื่นใดก็ตาม ดังนั้นคนที่กังวลว่าเมื่อเอาแฟลชไดรฟ์ที่ติดไวรัสมาเสียบที่เครื่องแล้วจะมีการติดไวรัสทันทีนั้นขอให้เลิกกังวลไปได้เลยครับ เพราะไวรัสจะมีการทำงานตามคำสั่งในไฟล์ Autorun.inf เมื่อเราทำการดับเบิ้ลคลิกที่ไดรฟ์เท่านั้นครับ ดังนั้นเพื่อหลีกเลี่ยงการเรียกไวรัสขึ้นมาทำงานให้เราใช้วิธีการพิมพ์ชื่อไดรฟ์ในช่อง Address ตามที่ผมแนะนำไว้ในเล่มแรกนะครับ

ถึงตอนนี้อาจจะมีหลายคนแย้งว่าไม่จริงหรอกมั้ง เพราะแฟลชไดรฟ์รุ่นใหม่ๆที่เรียกกันว่า U3 นั้นเมื่อนำมาเสียบในเครื่องมันก็ยังรันโปรแกรมขึ้นมาให้เลยนี่นา ซึ่งเดี๋ยวผมจะอธิบายอีกทีในช่วงท้ายๆนะครับว่าทำไมมันถึงรันโปรแกรมแบบอัตโนมัติจากการเสียบแฟลชไดรฟ์แบบ U3 ได้ เอาเป็นว่าในตอนนี้ผมขอสรุปว่าเพียงแค่การนำแฟลชไดรฟ์ที่ติดไวรัสมาเสียบที่เครื่องนั้นจะยังไม่มีการติดไวรัสอย่างแน่นอนเพราะตัวไวรัสยังไม่ได้โดนเรียกขึ้นมาทำงาน

มีเพียง 2 กรณีเท่านั้นที่จะเป็นการเรียกไวรัสขึ้นมาก็คือช่องทาง Autoplay ในกรณีที่ไวรัสใช้คำสั่ง Action ร่วมกับคำสั่ง Open แล้วเรากด Enter หรือเลือก OK ในหน้าต่าง Autoplay เอง กับอีกช่องทางคือช่องทาง Autorun ซึ่งไวรัสจะใช้วิธีการกำหนดคำสั่งที่จะใช้เรียกตัวเองขึ้นมาไว้ในไฟล์ Autorun.inf แล้วเราไปดับเบิ้ลคลิกที่ตัวไดรฟ์นั้นโดยตรง หรือแม้กระทั่งการคลิกขวาแล้วเลือกเมนูต่างๆครับ

เก็บตกเรื่อง Autorun.inf **(จากเล่ม 1 หน้า** 106)

หลังจากได้ออกเล่มแรกไปแล้วมีเพื่อนผมได้มาถาม(กึ่งถากถาง)ว่าถ้าใช้การคลิกขวาเลือก Open แล้วติดไวรัสเราก็เลือก Explore สิจะได้ปลอดภัย ไม่เห็นจะต้องพิมพ์ชื่อไดรฟ์ให้ยุ่งยากเลย คาดว่าหลายๆคนก็คงคิดแบบเพื่อนผม เดี๋ยวเรามาพิสูจน์กันครับว่าจะปลอดภัยจริงหรือไม่ โดยสร้างไฟล์ Autorun.inf ขึ้นมาแล้วเปลี่ยนคำสั่งภายในเป็นแบบนี้แทนนะครับ



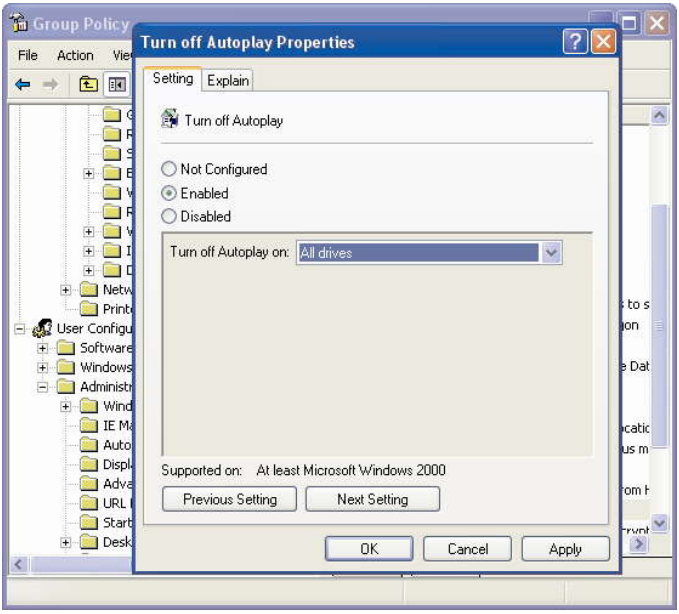
จะเห็นว่าผมใส่ถึง 3 เมนูคือ Open , Explore และ **ทดสอบเพิ่มเมนู** เพื่อจะได้เห็นชัดๆว่าเราสามารถจะกำหนดเมนูชื่ออะไรก็ได้ หลังจากนั้นผมนำแฟลชไดรฟ์ที่ได้สร้างไฟล์ Autorun.inf ใส่ไว้แล้วออกมาแล้วเสียบกลับเข้าไปใหม่ เรามาดูผลจากการคลิกขวากันครับ

จะเห็นว่ามีเมนูทั้ง 3 ที่ผมใส่ไว้ในไฟล์ Autorun.inf และตอนนี้ไม่ว่าผมจะเลือกเมนูไหน(รวมไปถึงการดับเบิ้ลคลิก) ก็จะเป็นการเปิดโปรแกรมเครื่องคิดเลข(Calc.exe) หรือตัวไวรัส(สมมุติ)ขึ้นมาทั้งสิ้นครับ ดังนั้นผมขอยืนยันอีกครั้งว่าการพิมพ์ชื่อไดรฟ์ลงไปตรงๆปลอดภัยที่สุดครับเพราะเราคงคาดเดาได้ยากว่าคนเขียนไวรัสมันจะใช้การกำหนดชื่อเมนูในไฟล์ Autorun.inf แบบไหนบ้าง

การแก้ไขปัญหา Autorun.inf แบบตรงจุด

เอาล่ะครับหลังจากที่ได้ทำความเข้าใจเกี่ยวกับลูกเล่นของไวรัสที่อาศัยไฟล์ Autorun.inf ในการแพร่เชื่อทั้งช่องทาง Autoplay และ Autorun กันมาพอสมควรแล้ว ในหัวข้อนี้เราจะมาดูวิธีการปิดตายการทำงานของเจ้าไฟล์ Autorun.inf กันครับ

จากที่พบเห็นมาโดยส่วนใหญ่จะมีการแนะนำกันว่าเพื่อป้องกันไวรัสจำพวก Autorun ให้ทำการปิดฟังก์ชั่นการทำงานของ Autoplay ด้วยโปรแกรม Gpedit โดยการตั้งค่าในส่วนของ Turn off Autoplay ทั้งใน Computer Configuration และ User Configuration ให้เป็น Enable => All drive

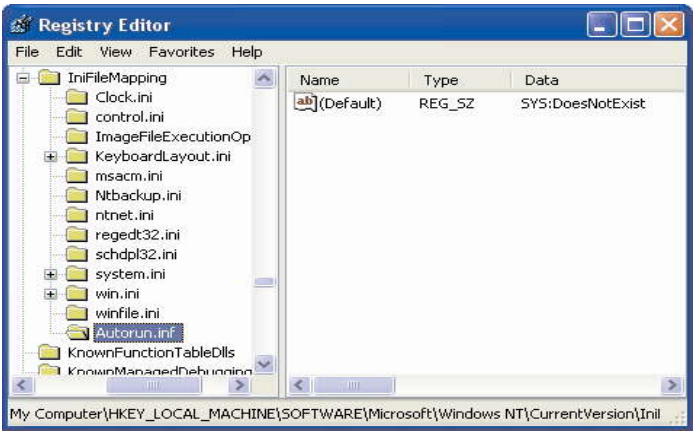


ซึ่งถึงตรงนี้แล้วทุกคนคงจะพอมองออกว่าวิธีข้างต้นนั้น มันเป็นการป้องกันปัญหาได้เพียงครึ่งเดียวเท่านั้นไม่ได้เบ็ดเสร็จเด็ดขาดแต่อย่างใด เพราะ Autoplay และ Autorun นั้นเป็นคนละตัวกัน ดังนั้นเพียงการปิด Autoplay ซึ่งจริงๆแล้วก็คือการยกเลิกหน้าต่าง Autoplay นั้นก็จะสามารถป้องกันไวรัสที่ใช้คำสั่ง Action ร่วมกับ Open ในช่องทางของ Autoplay ตามที่ได้รู้กันไปแล้วเท่านั้นเอง

แต่ในกรณีที่ไวรัส(โดยส่วนใหญ่) ซึ่งใช้ช่องทางของ Autorun คือใช้การระบุคำสั่งให้เปิดตัวไวรัสไว้ในไฟล์ Autorun.inf ซึ่งจะมีผลเมื่อเราทำการดับเบิ้ลคลิกเรียกใช้ไดรฟ์นั้น รวมถึงการคลิกขวาแล้วเลือกเอาจากเมนูกลับไม่ได้รับการป้องกันจากการปิด Autoplay แต่อย่างใดนะครับ นั่นหมายถึงว่าถ้าเราดับเบิ้ลคลิกที่ตัวไดรฟ์ที่มีไวรัสอยู่ ก็ยังเป็นการเรียกไวรัสขึ้นมาทำงานอยู่ดีครับ(ไม่งงนะครับ)

ดังนั้นด้วยวิธีการข้างต้นนั้นนอกจากจะไม่สามารถป้องกันไวรัสได้อย่างแท้จริงแล้วก็ยังทำให้เราไม่สามารถใช้ช่องทางอำนวยความสะดวกของ Autoplay ในการเลือกโปรแกรมเพื่อจัดการกับไฟล์ในแฟลชไดรฟ์ได้อีกต่างหาก

เอาล่ะ ในเมื่อรู้แล้วว่าปัญหามันเกิดจาก Autorun เราก็ปิด Autorun สิจะได้เป็นการแก้ที่ตรงจุด เหมือนการดับทุกข์ก็ควรดับที่เหตุแห่งทุกข์นั่นเองครับ โดยให้เราเปิดโปรแกรม Regedit เข้าไปที่ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping จากนั้นให้สร้าง Key ใหม่ชื่อ Autorun.inf แล้วทำการแก้ไข Value (Default) เป็น SYS:DoesNotExist แล้วปิดโปรแกรม Regedit เพียงเท่านี้ก็จะเป็นการปิดการทำงานของ Autorun เรียบร้อยแล้วล่ะครับ



โดยการเพิ่ม Key ใน Registry(ดูรายละเอียดเรื่องของ Registry หน้า 208 ล้วงไต๋เล่ม 2) ข้างต้นนั้นเป็นการบอกให้ Windows มองข้ามไฟล์ Autorun.inf ไปเลยไม่ต้องสนใจอ่านคำสั่งมัน ซึ่งผลก็คือถึงแม้ว่าไวรัสจะใช้คำสั่ง Action ร่วมกับ Open นั้นในหน้าต่าง Autoplay ที่ขึ้นมาก็จะไม่มีส่วนเมนูของโปรแกรมที่กำหนดไว้ในส่วนนั้นๆแต่อย่าง

หรือในกรณีที่ไวรัสใช้คำสั่ง ShellExecute และคำสั่งเปิดไฟล์อื่นๆก็เช่นเดียวกันครับจะไม่มีผลใดๆเลยเพราะ Windows จะมองข้ามไฟล์ Autorun.inf ไปเลย ทำให้เราสามารถที่จะดับเบิ้ลคลิกเข้าไปในไดรฟ์ได้เลยโดยไม่ต้องกังวลเพราะ Windows มันจะไม่ฟังคำสั่งจาก Autorun.inf อีกแล้ว

ดังนั้นถึงแม้ว่าไวรัสจะเขียนคำสั่งอะไรไว้ข้างในก็ไม่มีผลใดๆครับด้วยวิธีนี้จึงนับว่าปลอดภัยตรงประเด็น แถมยังสามารถใช้ความสามารถของ Autoplay ในการเปิดโปรแกรมที่ใช้ในการจัดการกับไฟล์ที่อยู่ในแฟลชไดรฟ์ได้เหมือนเดิมอีกต่างหาก(เพราะการทำงานของ Autoplay ไม่จำเป็นต้องอาศัยไฟล์ Autorun.inf)

หมายเหตุ ในกรณีที่ได้ยกเลิกไปแล้วและต้องการกลับมาใช้ไฟล์ Autorun.inf อีกก็เพียงทำการลบ Key Autorun.inf ทิ้งแล้วบู๊ตเครื่องใหม่ก็สามารถที่จะใช้ไฟล์ Autorun.inf ได้เหมือนเดิมครับ

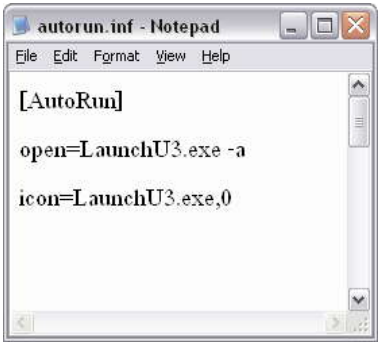
และสำหรับคนที่ไม่อยากแก้ไขค่า Registry ด้วยตนเองนั้นให้โหลดโปรแกรม Dis_Autorun ไปใช้นะครับ โดยสามารถที่จะเลือกปิดหรือเปิดการใช้งาน Autorun ได้เลยครับ

ไขข้อข้องใจแฟลชไดรฟ์แบบ U3

ตามสัญญาครับที่ผมรับปากว่าจะอธิบายถึงสาเหตุที่แฟลชไดรฟ์แบบ U3 สามารถที่จะรันโปรแกรมขึ้นมาได้เมื่อเสียบแฟลชไดรฟ์เข้าเครื่อง ทั้งๆที่ผมบอกเองว่าคำสั่ง Open ที่จะใช้เปิดโปรแกรมขึ้นมาแบบอัตโนมัตินั้นไม่สามารถใช้กับแฟลชไดรฟ์ได้

สำหรับคนที่ใช้แฟลชไดรฟ์แบบนี้นั้นจะสังเกตเห็นว่าเมื่อเราเสียบแฟลชไดรฟ์เข้าไปนั้น Windows มันจะมองเห็นเป็น 2 ไดรฟ์นะครับ โดยหนึ่งในนั้น Windows จะเห็นเป็น CD Drive ลองดูตามรูปตัวอย่างนะครับเมื่อผมเสียบแฟลชไดรฟ์เข้าไปจะเห็นว่ามีไดรฟ์ F และ G เพิ่มขึ้นมา และโดยไดรฟ์ F นั้น Windows จะมองเห็นเป็น CD Drive ส่วนแฟลชไดรฟ์จริงๆของผมจะเป็นไดรฟ์ G ครับ

หลายๆคนคงพอจะเดาออกแล้วว่า U3 นั้นใช้วิธีการอะไรถึงทำการเรียกโปรแกรมขึ้นมาทำงานด้วยคำสั่ง Open ใน Autorun.inf ได้ ใช่แล้วครับมันจะใช้การจำลองไดรฟ์ซึ่งเป็น CD Drive ขึ้นมาซึ่งภายในนั้นก็จะมีไฟล์ Autorun.inf และโปรแกรมซึ่งจะถูกเรียกใช้ด้วยคำสั่ง Open และเมื่อ Windows มองว่าตัวไดรฟ์นั้นเป็นประเภท CD Drive จึงอนุญาตให้สามารถเรียกโปรแกรมโดยใช้คำสั่ง Open ได้นั่นเองครับ เพื่อยืนยันว่าสิ่งที่ผมพูดนั้นถูกต้อง เราลองเข้าไปดูภายในไดรฟ์ F กันครับ



จะเห็นได้ว่ามีการเรียกใช้โปรแกรมด้วยคำสั่ง Open จากไฟล์ Autorun.inf ได้จริงๆด้วย นั่นเป็นเพราะว่ามันหลอก Windows ว่าตัวเองเป็น CD นั่นเองครับจึงสามารถที่จะใช้คำสั่ง Open ได้ คงเข้าใจวิธีการที่ U3 ใช้กันแล้วนะครับ

ส่วนใครที่กังวลใจว่าไวรัสจะอาศัยช่องทางนี้ในการเรียกตัวเองขึ้นมาโดย ก็ไม่ต้องกังวลนะครับ เพราะจากการทดลองดูนั้น CD(จำลอง)ที่ U3 สร้างขึ้นมานั้นเป็น CD แบบธรรมดาๆ(ไม่สามารถเขียนหรือแก้ไขไฟล์ภายในได้ครับ) แต่ถ้าใครยังกังวลว่าในอนาคตไวรัสมันอาจจะพัฒนาให้สามารถเขียนไฟล์ลงไป

ได้ แล้วอยากจะยกเลิก U3 เพื่อใช้เป็นแฟลชไดรฟ์ธรรมดาๆก็สามารถโหลดโปรแกรมในการลบการทำงานของ U3 ทิ้งไปได้ โดยให้เข้าไปโหลดได้ที่

http://u3uninstall.s3.amazonaws.com/U3Uninstall.exe ซึ่งหลังจากทำการ Format ด้วยโปรแกรมดังกล่าวแล้ว แฟลชไดรฟ์แบบ U3 ก็จะกลายเป็นแฟลชไดรฟ์ธรรมดาๆไม่มีการสร้าง CD(จำลอง)และเรียกใช้โปรแกรมใดๆแบบอัตโนมัติขึ้นมาอีกแล้วครับ

แต่ถ้าใคร Format ไปแล้วเกิดเปลี่ยนใจอยากจะกลับมาใช้ U3 อีกก็สามารถหาโปรแกรมในการเปิดใช้ U3 ใหม่ได้จากเว็บไซต์ผู้ผลิตแฟลชไดรฟ์ยี่ห้อนั้นๆนะครับเช่น

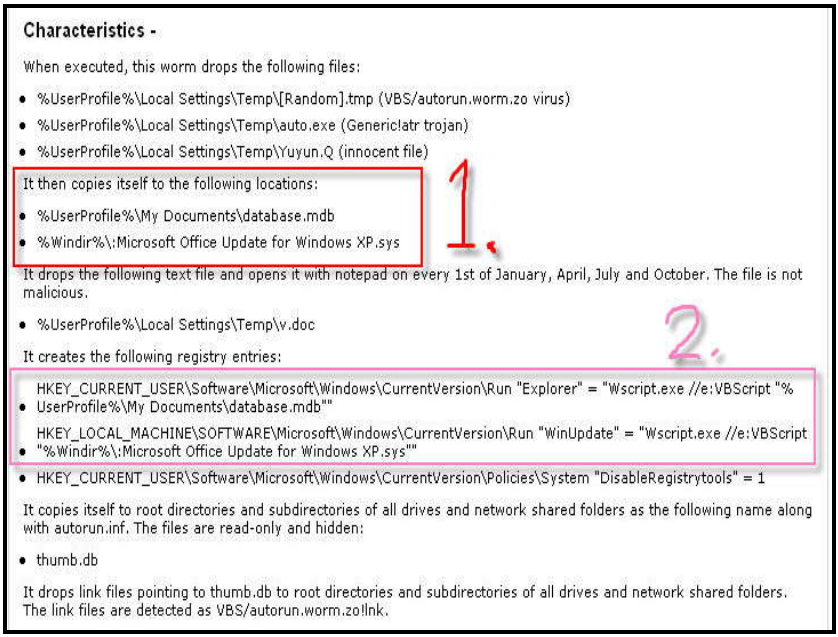
http://u3.sandisk.com/download/apps/LPInstaller.exe ยี่ห้อ Sandisk

http://www.kingston.com/support/downloads/usbdatatrav/U3update.exe ยี่ห้อ Kingston

Chapter 2. วิธีการพรางตัวของไวรัสตระกูล Script

ว่างๆก็นั่งหาความรู้เกี่ยวกับไวรัสตัวใหม่ๆไปเรื่อยๆ จนได้พบไวรัสตัวนึง เห็นว่ามีอาการน่าสนใจและมีความเกี่ยวเนื่องจากเนื้อหาในหนังสือล้วงไต๋ไวรัส 2(บทที่ 1) เลยนำมาเล่าสู่กันฟังเพื่อเป็นการ Update ความรู้เพิ่มเติมจากในหนังสือครับ

เรามาดูข้อมูลของไวรัสตัวที่ผมว่ากันเลยครับจะได้ไม่เสียเวลา(ผู้สนใจสามารถดูรายละเอียดเต็มได้จาก http://vil.nai.com/vil/content/v_153751.htm ครับ)



Characteristics -

When executed, this worm drops the following files:

- %UserProfile%\Local Settings\Temp\[Random].tmp (VBS/autorun.worm.zo virus)
- %UserProfile%\Local Settings\Temp\auto.exe (Generic!atr trojan)
- %UserProfile%\Local Settings\Temp\Yuyun.Q (innocent file)

It then copies itself to the following locations:

- %UserProfile%\My Documents\database.mdb
- %Windir%\:Microsoft Office Update for Windows XP.sys

1.

It drops the following text file and opens it with notepad on every 1st of January, April, July and October. The file is not malicious.

- %UserProfile%\Local Settings\Temp\v.doc

2.

It creates the following registry entries:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Explorer" = "Wscript.exe //e:VBScript "%UserProfile%\My Documents\database.mdb""
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "WinUpdate" = "Wscript.exe //e:VBScript "%Windir%\:Microsoft Office Update for Windows XP.sys""
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System "DisableRegistrytools" = 1

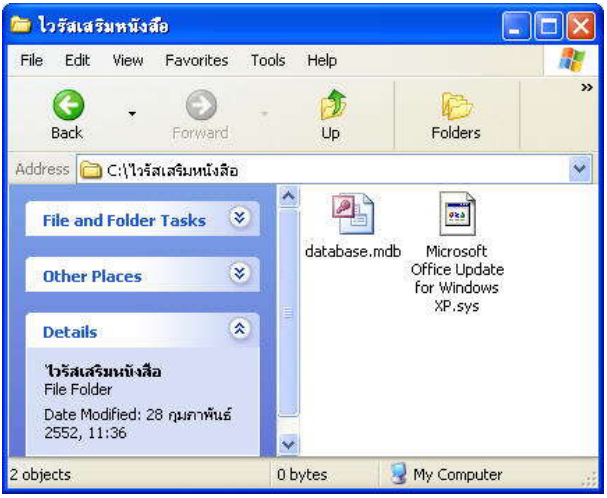
It copies itself to root directories and subdirectories of all drives and network shared folders as the following name along with autorun.inf. The files are read-only and hidden:

- thumb.db

It drops link files pointing to thumb.db to root directories and subdirectories of all drives and network shared folders. The link files are detected as VBS/autorun.worm.zo!lnk.

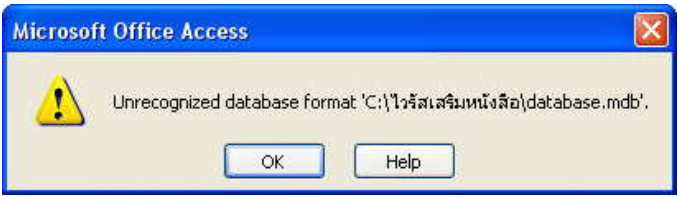
จากรูปผมจะตั้งข้อสังเกตในจุดที่น่าสนใจไว้ 2 จุดนะครับ โดยจุดแรกนั้นจะเห็นว่าไวรัสจะใช้ไฟล์ที่ชื่อ database.mdb และ Microsoft Office Update for Windows XP.sys

และด้วยเหตุผลที่ว่า Windows เองนั้นไม่ได้สนใจเนื้อหาภายในของไฟล์ว่าจะเป็นอะไรแต่มันจะใช้การกำหนดรูปไอคอนตามนามสกุลของไฟล์ดังนั้นไฟล์ทั้ง 2 จึงมีไอคอนตามรูป



นั่นคือไฟล์ database.mdb จะโดนมองว่าเป็นไฟล์ของโปรแกรม Access ซึ่งแน่นอนจากรูปของไอคอนทำให้ผู้ใช้ไม่มีทางเอะใจแน่ว่ามีไวรัสอยู่ในเครื่องเพราะคิดว่าเป็นไฟล์ของ Access ธรรมดาๆ เพราะแม้แต่ Windows เองก็ยังมองว่าไฟล์นี้เป็นไฟล์ Access เลยครับ

นั่นคือถ้าเราทำการดับเบิ้ลคลิกเพื่อเรียกไฟล์ database.mdb ตัว Windows ก็จะพยายามที่จะเปิดไฟล์ที่ว่าด้วยโปรแกรม Access(เพราะ Windows ใช้การแยกแยะประเภทของไฟล์จากนามสกุล) แต่ก็ไม่สามารถเปิดได้หรอกครับเนื่องจากภายในนั้นไม่ใช่ Access แต่เป็นไฟล์ Script ซึ่งเปลี่ยนนามสกุลเอา ดังนั้นเราจะพบกับหน้า Error ดังนี้ครับ



อ้าว! แล้วไวรัสมันจะใช้วิธีการเรียกตัวเองขึ้นมาทำงานยังไงล่ะในเมื่อ Windows ยังมองว่ามันเป็น Access ขืนระบุชื่อ database.mdb ลงไปในจุด Startup ต่างๆให้อาศัยโหลดพร้อมตัว Windows(ล้วงไต๋ เล่ม 1 หน้า 108) แล้วเจ้าตัว Windows เองก็ยังพยายามเปิดกับ Access มันก็ Error น่ะสิ นี่ล่ะครับเป็นจุดที่น่าสนใจและผมอยากจะนำมาเสริมกับเนื้อหาเรื่องของไวรัส Script (ในบทที่ 1 ของล้วงไต๋ไวรัสเล่ม 2)

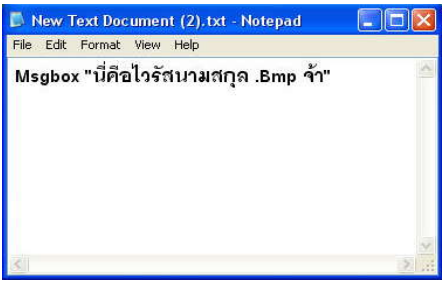
โดยถ้าเราดูจากจุดสังเกตที่ 2 ของรูปแรกที่ผมทำเอาไว้จะเห็นว่าไวรัสมันใช้วิธีการเรียกแบบนี้ครับ Wscript.exe //e:VBScript **ชื่อไฟล์ Script ที่เปลี่ยนนามสกุลแล้ว**

นั่นคือจะเห็นว่ามีส่วนของ //e:VBScript เพิ่มขึ้นมาจากที่ผมเขียนไว้ในบทที่ 1 ซึ่ง //e:VBScript ที่เพิ่มขึ้นมานั้นจะเป็นการระบุตัว Engine ที่ใช้ในการแปลไฟล์ Script นั่นเองครับ สาเหตุเพราะว่าทาง Microsoft ได้อำนวยความสะดวก(รึปล่าว?) ทำให้เราสามารถที่จะใช้ไฟล์ Script ที่มีนามสกุลใดๆก็ได้(จากตัวอย่างไวรัสใช้ .mdb และ .sys) ไม่จำเป็นต้องใช้นามสกุล .vbs หรือ .js เสมอไป เพียงแต่ว่าถ้าจะรันไฟล์ Script ที่มีนามสกุลอื่นๆที่ไม่ใช่มาตรฐาน(.vbs,.js) ก็ขอให้ระบุตัว Engine ที่จะใช้ในการแปล Script ให้มันด้วย Windows จึงสามารถที่จะรู้ได้ว่าจะใช้อะไรในการแปล

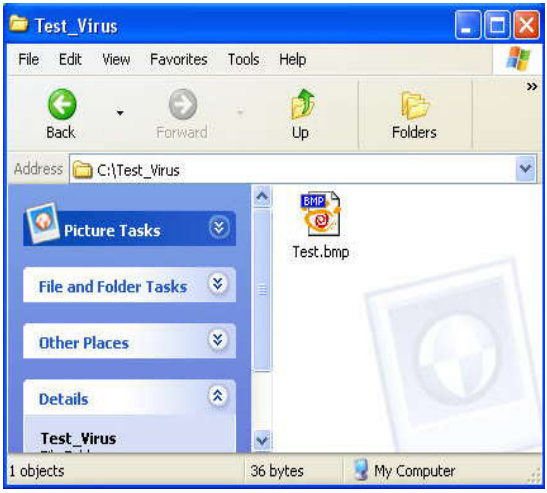
ซึ่งจากตัวอย่างนั้นไวรัสใช้ภาษา VBScript ในการเขียน จึงระบุเป็น //e:VBScript (สามารถเขียนแบบย่อว่า e://VBS ก็ได้เช่นกันครับ)

ซึ่งถ้าแยกให้เห็นชัดคือ //e: ก็คือส่วนที่ใช้กำนหดตัว Engine ส่วน VBScript นั้นก็คือตัว Engine ที่ใช้ในการแปลนั่นเองครับ(ไม่งงนะครับ)

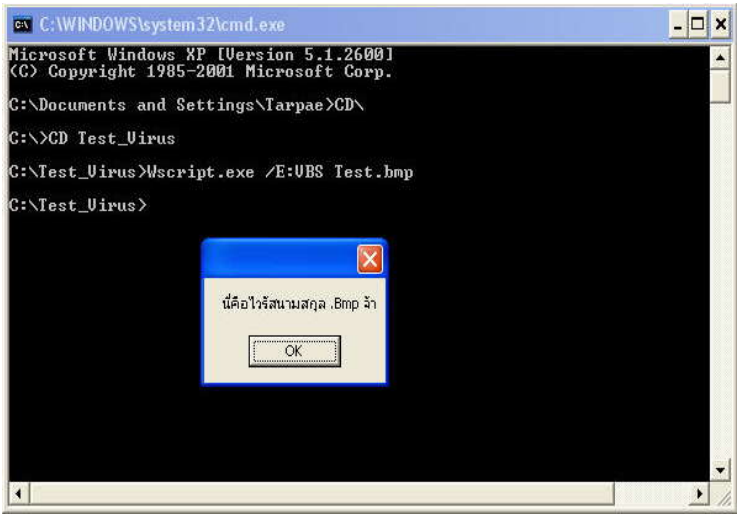
และเช่นเคยครับ สิบล้านตัวหนังสือไม่เท่าลงมือทำ เราจะมาทำการทดลองวิธีการทำงานของเจ้าไวรัสตัวนี้กันครับ โดยในขั้นแรกให้ทำการสร้าง Text ไฟล์ขึ้นมาโดยใช้โปรแกรม Notepad นี่ล่ะครับ แล้วเขียนในไฟล์ว่า Msgbox “**นี่คือไวรัสนามสกุล .Bmp จ้า**”



จากนั้นทำการ Save เป็นไฟล์ชื่อ Test.bmp(ใช้วิธีการ Save As เหมือนที่ทดลองสร้างไฟล์ .VBS ในตัวอย่างบทที่ 1 เล่มที่ 2 แต่เปลี่ยนนามสกุลเป็น .bmp แทน .vbs เท่านั้นเองครับ) ก็จะเห็นว่ารูปไอคอนของไฟล์นั้นเป็นเหมือนไฟล์รูปภาพทั่วๆไปแล้ว เนื่องจากอย่างที่บอกว่า Windows นั้นจะแยกแยะประเภทของไฟล์จากนามสกุลไม่ใช่เนื้อหาภายใน(เหมือนคนบางคนที่ชอบมองกันที่นามสกุลมากกว่าจิตใจหรือการกระทำ เฮ้อ! การมองเพียงนามสกุลนี่มันไม่ดีทั้งคอมพ์และคนเลย)



คราวนี้เรามาทดลองเรียกเจ้าไวรัส(ตัวที่เราสร้าง)ให้ขึ้นมาทำงานกันครับด้วยการเปิด cmd ขึ้นมาแล้วทำการย้าย Path เข้าไปในโฟลเดอร์ที่เราเก็บไฟล์ที่สร้างขึ้นมาเพื่อสะดวกในการอ้างถึงโดยใช้คำสั่ง CD แล้วพิมพ์ตามนี้ครับ Wscript.exe /E:VBS Test.bmp

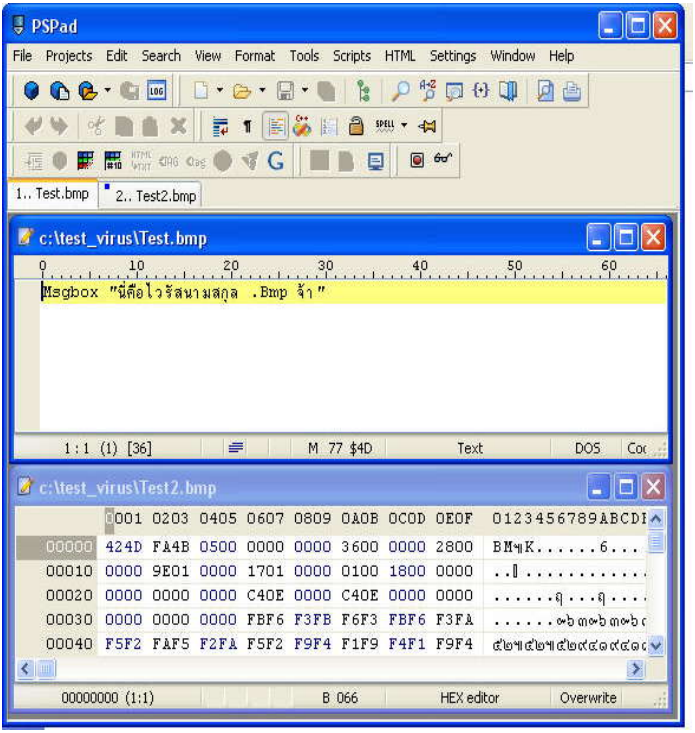


ผลก็คือเราจะเห็นกล่องข้อความว่า “นี่คือไวรัสนามสกุล .Bmp จ้า” ปรากฏขึ้นมา นั่นก็แสดงให้เห็นว่าเราสามารถที่จะเรียกใช้ไฟล์ประเภท Script ที่มีนามสกุลใดๆก็ได้จริงๆด้วย เพียงใช้การระบุตัว Engine ที่จะใช้ในการแปลให้มันนั่นเองครับ

คงมองเห็นภาพแล้วนะครับว่าไวรัสตัวอย่างที่ผมนำมาให้ดูนั้นมันสามารถเรียกใช้ไฟล์ Database.mdb และ Microsoft Office Update for Windows XP.sys ซึ่งเป็นไฟล์ประเภท Script ขึ้นมาทำงานได้อย่างไรทั้งๆที่ไม่ใช่นามสกุล .Vbs หรือ .Js

ดังนั้นขอให้ระมัดระวังไฟล์แปลกๆที่เราไม่ได้เป็นคนสร้างกันหน่อยนะครับ ซึ่งผมมีวิธีการตรวจสอบแบบเบื้องต้นมาแนะนำคือให้ทำการติดตั้งโปรแกรม PSPad editor ซึ่งเป็นโปรแกรม Freeware สามารถโหลดได้ที่ http://www.pspad.com

ถ้าเจอไฟล์ไหนที่ไม่ชอบมาพากลเราก็สามารถคลิกขวาที่ไฟล์นั้นแล้วเลือก PSPad เพื่อทำการตรวจสอบเนื้อหาภายในไฟล์นั้นๆได้เลยว่าเป็นไฟล์ Script ที่ปลอมตัวมาหรือไม่ ตามตัวอย่างผมทำการเปิดไฟล์ Test.bmp ซึ่งเป็นไฟล์ Script ที่เราสร้างขึ้นเทียบกับไฟล์ Test2.bmp ซึ่งเป็นไฟล์รูปภาพจริงๆ



จะเห็นได้ว่าในกรณีที่เป็นไฟล์ Script ที่เปลี่ยนนามสกุลนั้นเราสามารถที่จะอ่านเนื้อหาภายในได้เลยเนื่องจากภายในก็เป็น Text File ธรรมดาๆ แต่ในกรณีที่เป็นไฟล์ .Bmp จริงๆซึ่งมีการเก็บแบบ Binary โปรแกรมจะแสดงเป็นเลขฐาน 16 แทนนั่นเองครับ

แต่ไม่ได้หมายความว่าไฟล์ไหนที่แสดงเป็นเลขฐาน 16 แล้วจะปลอดภัยเสมอไปนะครับ (วิธีการตรวจสอบแบบนี้เราใช้แค่ตรวจสอบว่าเป็นไฟล์ Script ปลอมตัวมาหรือไม่) เนื่องจากไฟล์นั้นๆ อาจจะเป็นไฟล์ประเภท Executable File(นามสกุล .Exe,.Com ...) ที่เปลี่ยนนามสกุลเพื่อตบตาเราก็ได้ครับ ดังนั้นถ้าพบไฟล์ไหนต้องสงสัยก็ให้ใช้การอัพโหลดเพื่อตรวจสอบกับทางเว็บผู้ให้บริการตรวจสอบไฟล์ต้องสงสัยที่ผมแนะนำไว้ในบทที่ 1(เล่ม 2) อีกครั้งก็ดีครับ

วิธีกำจัดไวรัสประเภท Script แปลงโฉม

หลังจากรู้วิธีการทำงานและวิธีตรวจสอบไวรัสตัวนี้กันแล้วคราวนี้เรามาดูวิธีกำจัดมันกันครับ สำหรับการกำจัดไวรัสตัวนี้(หรือตัวอื่นๆที่มีการทำงานแบบนี้)ก็ไม่ได้ยุ่งยากอะไรครับ เนื่องจากเราจับไต๋มันได้แล้วว่าจริงๆแล้วมันก็คือไวรัสประเภท Script ธรรมดาๆเท่านั้นเอง ถึงแม้จะเปลี่ยนนามสกุลไปเป็นหลายๆนามสกุลเพื่อตบตาเรา

ดังนั้นคนที่ได้อ่านล้วงไต๋ฯ(เล่ม 1) มาแล้วก็คงพอจะนึกออกว่าเราสามารถที่จะใช้วิธีการกำจัดแบบเดียวกันกับไวรัส Script ทั่วๆไปนั่นล่ะครับ คือทำการปิดเพียง Process ที่ชื่อ Wscript.exe ซึ่งใช้ในการรัน Script ของตัวไวรัสเหมือนตัวอย่างการกำจัดไวรัส People's Republic of Thailand(PRT) ในหน้าที่ 196(ล้วงไต๋ฯเล่มแรก)ได้เลยครับ

คำถามต่อมาคือแล้วตัวไฟล์ไวรัสล่ะเราจะตามลบมันยังไงในเมื่อมันไม่ได้ชื่อเดียวกันทุกไฟล์ และที่สำคัญมันไม่ได้ใช้นามสกุล .Vbs ทุกไฟล์เหมือนเจ้าไวรัส PRT นะ แล้วจะรู้ได้ไงล่ะว่าไฟล์ไหนบ้างที่เป็นไวรัสหรือต้องใช้วิธีตรวจสอบทีละไฟล์ด้วย PSPad editor อีก(ตายพอดี)

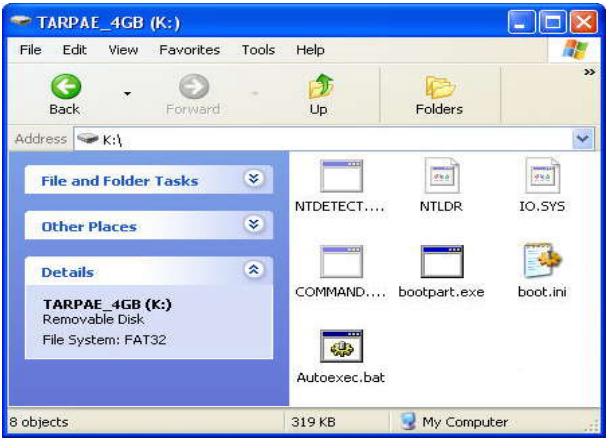
คำตอบคือไม่ต้องยุ่งยากขนาดนั้นหรอกครับ จำได้มั้ยว่าผมได้อธิบายเรื่องของ MD5 ไว้ในหน้าที่ 202 (ล้วงไต๋ฯเล่ม 2) ว่าถึงแม้จะมีการเปลี่ยนชื่อหรือนามสกุลยังไงก็ตามค่าของ MD5 ก็จะไม่เปลี่ยนแปลง ดังนั้นเราสามารถประยุกต์ใช้วิธีการเขียนโปรแกรม จากหน้า 280(ล้วงไต๋ฯเล่ม 2) ในการสร้างโปรแกรมมาค้นหา+ลบมันได้เลย

หรือถ้าไม่อยากเขียนโปรแกรมเองจะใช้โปรแกรม DKDC_Hash จากเล่มแรก(หน้า 210) ที่ใช้ในการกำจัดไวรัสพวกโฟลเดอร์(ปลอม)ก็ได้เช่นกันครับ ถึงมันจะเปลี่ยนเป็นชื่อหรือนามสกุลอะไรก็ไม่มีทางหลุดรอดแน่นอนครับ

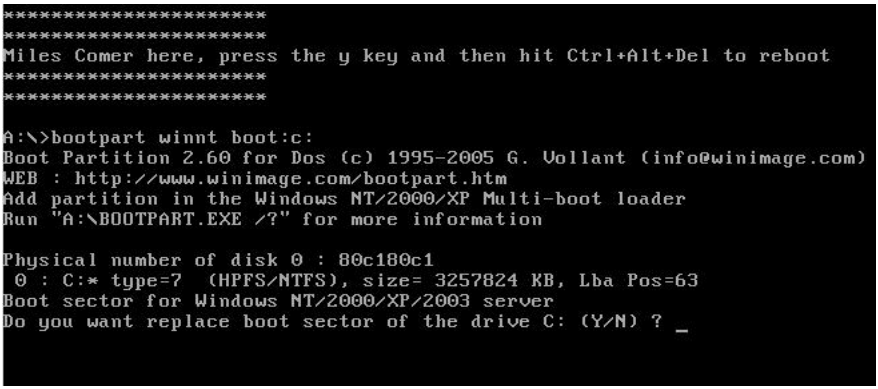
Chapter 3. แก้ไขปัญหา NTLDR is missing(ปรับปรุง)

สืบเนื่องจากในล้วงไต๋ฯเล่มแรก(หน้า 177) ผมได้แนะนำวิธีการแก้ไขปัญหา NTLDR is missing ไปทั้งวิธีการใช้แผ่น Floppy Disk(Drive A) และการใช้แฟลชไดรฟ์ในการแก้ไขปัญหานั้น ได้มีผู้อ่านหลายๆท่านแจ้งมาว่าไม่สามารถใช้แฟลชไดรฟ์ในการแก้ไขปัญหาได้เพราะเมื่อบู๊ตด้วยแฟลชไดรฟ์แล้วมันไม่เข้า Windows แต่จะค้างอยู่ตรงหน้าจอ Dos (C:\>) แทน ผมจึงได้ลองทำการทดสอบกับเครื่องอีกหลายๆรุ่น รวมถึงยืมแฟลชไดรฟ์ของเพื่อนๆหลายยี่ห้อมาทดสอบด้วย เลยได้ข้อสรุป(ที่ผมเองก็ยังไม่ค่อยเข้าใจนัก)ว่ามีบางเครื่องและแฟลชไดรฟ์บางรุ่นที่ไม่สามารถใช้วิธีที่ผมแนะนำตามในหนังสือ เพราะจะมีการบู๊ตเข้า Dos ตามที่หลายคนแจ้งมา ผมจึงต้องขออภัยไว้ ณ.ที่นี้ด้วยที่ก่อนจะเขียนลงไปในหนังสือไม่ได้ทำการทดสอบกับหลายๆเครื่องให้แน่นอนก่อน ต้องขออภัยอย่างสูงครับ

คราวนี้เรามาดูวิธีการในการใช้แฟลชไดรฟ์เพื่อทำการแก้ไขปัญหานี้ซึ่งสำหรับวิธีนี้นั้นผมได้ทำการทดสอบกับเครื่องหลายๆเครื่องรวมถึงแฟลชไดรฟ์หลายๆยี่ห้อจนมั่นใจว่าใช้ได้ผลแน่นอนครับ โดยขั้นตอนเบื้องต้นนั้นจะเหมือนกับในหนังสือทุกอย่าง แต่หลังจากที่ดำเนินการในขั้นที่ 11 (หน้า 180) ให้โหลดไฟล์ NTLDR_Fix.zip(สามารถโหลดได้จากหน้าที่เข้ามาโหลดล้วงไต๋ฯ Add-Ons) ซึ่งเมื่อทำการ Unzip ออกมาแล้วจะเห็นว่ามีไฟล์อยู่ 3 ไฟล์คือ Autoexec.bat, boot.ini และ bootpart.exe ให้ทำการก๊อบปี้ทั้ง 3 ไฟล์ที่ว่าใส่ลงไปในแฟลชไดรฟ์ด้วยนะครับ



เพียงเท่านี้เราก็สามารถที่จะนำแฟลชไดรฟ์นี้ไปใช้บู๊ตเครื่องเพื่อแก้ไขปัญหาได้แล้วล่ะครับ แต่เมื่อบู๊ตด้วยแฟลชไดรฟ์อันนี้นั้น ในครั้งแรกมันจะยังไม่เข้า Windows นะครับ มันจะขึ้นหน้าจอของ DOS คล้ายๆกับรูปด้านล่างนี้(อาจจะยาวกว่านี้ขึ้นอยู่กับจำนวนไดรฟ์ในเครื่อง)



ไม่ต้องตกใจนะครับว่าเราทำผิดขั้นตอนมันหรือไม่ได้ผล เลยเข้า DOS อีก เพราะขั้นตอนนี้จะเป็นขั้นตอนในการสร้าง Boot Sector ให้กับตัวแฟลชไดรฟ์เพื่อให้สามารถอ่านไฟล์ NTLDR จากในตัวแฟลชไดรฟ์ได้(สำหรับขั้นตอนการบู๊ตของ Windows แบบละเอียดผมจะนำมาเขียนในครั้งต่อๆไปนะครับ ขอศึกษาให้รู้จริงก่อน) โดยจะเห็นว่าในบรรทัดสุดท้ายจะถามว่าเราต้องการที่จะเขียนทับ Boot Sector ของไดรฟ์ C: หรือไม่ ให้เราพิมพ์ Y ลงไปนะครับ มันก็จะขึ้นผลการทำงานมาอีก 2-3 บรรทัดแล้วขึ้น C:\>

สำหรับขั้นตอนด้านบนนั้นไม่ต้องตกใจว่ามันจะเขียนทับข้อมูลในฮาร์ดดิสของเรานะครับ เพราะไดรฟ์ C: ในตอนนี้มันหมายถึงตัวแฟลชไดรฟ์นั่นเอง(สำหรับเครื่องที่สามารถใช้วิธีการตามในหนังสือได้มันจะเห็นแฟลชไดรฟ์เป็นไดรฟ์ A: จึงสามารถบู๊ตเข้า Windows ได้เลย แต่ในเครื่องที่มีปัญหามันจะมองแฟลชไดรฟ์เป็นไดรฟ์ C: หรือมองเป็นฮาร์ดดิสตัวหนึ่งนั่นเองเลยไม่เข้า Windows จึงต้องทำการสร้าง Boot Sector ให้มันก่อน)

หมายเหตุสำหรับหน้าจอด้านบนนั้นจะขึ้นครั้งแรกเพียงครั้งเดียวถ้าตราบใดที่เรายังไม่ได้ทำการ Format แฟลชไดรฟ์ใหม่เพราะมันได้สร้าง Boot Sector ที่ทำให้สามารถอ่านไฟล์ NTLDR จากใน

แฟลชไดรฟ์ได้แล้ว นั่นหมายถึงว่าเราสามารถที่จะนำแฟลชไดรฟ์อันนี้ไปบู๊ตเครื่องอื่นๆที่มีปัญหา NTLDR is missing ได้เลย โดยมันจะไม่เข้ามาหน้าจอนี้อีกแล้วเพราะครั้งต่อไปมันจะบู๊ตเข้า Windows เลยครับ

ดังนั้นหลังจากแก้ปัญหาได้แล้วก็ไม่ต้อง Format แฟลชไดรฟ์ใหม่นะครับ เราสามารถที่จะก๊อบปี้ข้อมูลอื่นๆใส่ไว้ในแฟลชไดรฟ์อันนี้เพื่อนำไปใช้งานได้ตามปกติ แถมยังสามารถที่จะนำไปใช้บู๊ตเครื่องที่มีปัญหาได้อีกด้วย (ต้องไม่ลบไฟล์ที่ก๊อบปี้ใส่ไว้ในตอนแรกทิ้งนะครับ หรือถ้ารู้สึกว่ามันเกะกะก็สามารถลบบางไฟล์ได้นะครับให้เหลือแค่ไฟล์ที่จำเป็นต้องใช้งานจริงๆคือ NTLDR,NTDECT.COM และ Boot.ini ก็พอ อีก 4 ไฟล์ลบทิ้งไปก็ได้ครับ)นับว่าสะดวกจริงๆครับ

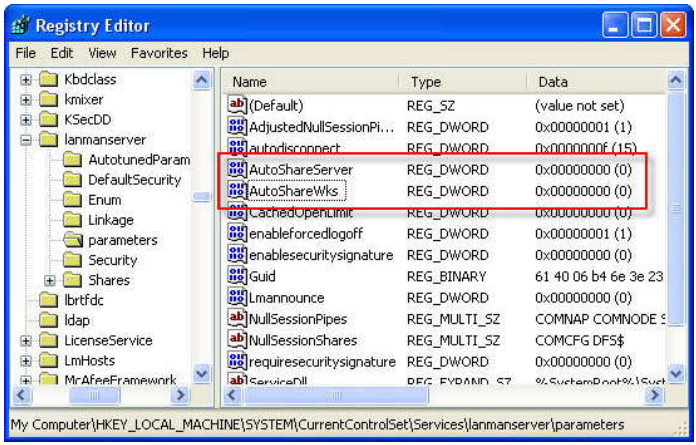
มาต่อกันครับหลังจากที่ขึ้น C:\> ที่หน้าจอแล้วให้เราทำการบู๊ตเครื่องใหม่ จะโดยการกด Ctrl+Alt+Delete หรือกดปุ่ม Reset ก็แล้วแต่สะดวกแต่ที่สำคัญคือจะต้องยังไม่ถอดแฟลชไดรฟ์ออกนะครับเพราะเราจะต้องเลือกให้มันบู๊ตจากแฟลชไดรฟ์อีกครั้งหนึ่ง ซึ่งคราวนี้จะเห็นว่าเราสามารถที่จะบู๊ตเข้า Windows ที่มีปัญหาได้แล้วล่ะครับ และหลังจากเข้า Windows แล้วก็ให้เราทำการก๊อบปี้ไฟล์ NTLDR จากแฟลชไดรฟ์ไปใส่ไว้ใน C:\ ตามที่อธิบายไว้ในหนังสือก็เรียบร้อยครับ(ก๊อบปี้เฉพาะไฟล์ NTLDR ก็พอนะครับไฟล์อื่นๆไม่ต้องก๊อบปี้) ในคราวหน้าเราก็สามารถที่จะเข้า Windows ได้โดยไม่ต้องใช้แฟลชไดรฟ์นี้อีกแล้วล่ะครับ

ปล.ขอบคุณสำหรับข้อมูล+โปรแกรมจาก http://tinyempire.com/notes/ntldrismissing.htm ซึ่งผมได้นำมาแก้ไขเล็กน้อยเพื่อให้ง่ายในการใช้งาน(ต้องให้เครดิตต้นฉบับเค้าด้วย) สำหรับใครที่สนใจจะศึกษาจากต้นฉบับก็เชิญตาม Link ได้เลยนะครับ ซึ่งภายในเว็บนี้จะมีวิธีการใช้ CD/DVD ในการบู๊ตเพื่อแก้ปัญหานี้เป็นอีกทางเลือกหนึ่งสำหรับคนที่ไม่อยากใช้แฟลชไดรฟ์ด้วยครับ

เพิ่มเติมการปิด Share$

จากที่มีท่านผู้อ่านผู้อ่านถามมาว่าใช้ Windows 2003 และได้ลองทำการปิด Administrative Share ตามที่ผมบอกไว้ในหนังสือล้วงไต๋ฯเล่ม 1(หน้า 25) แล้วไม่ได้ผล ผมจึงขอนำเนื้อหามาเพิ่มเติมดังนี้ครับ เนื่องจากเนื้อหาที่ผมบอกไปในเล่ม 1 นั้นผมจะเน้นไปที่ Windows XP เป็นหลักดังนั้นวิธีการที่ว่าจึงไม่สามารถใช้กับ Windows 2003 ซึ่งเป็นตระกูล Server ได้ครับ

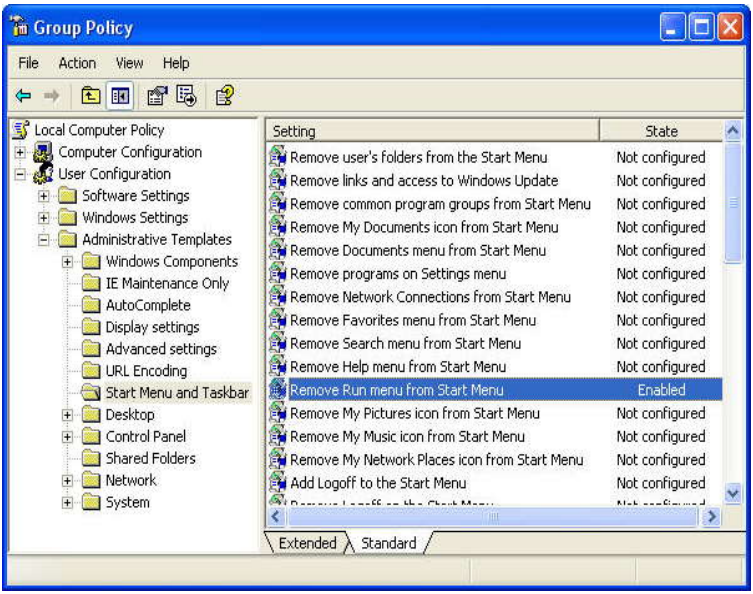
สำหรับวิธีการปิด Administrative Share ใน Windows 2003 หรือพวก Windows ตระกูล Server นั้นจะมีวิธีการที่ใกล้เคียงกันล่ะครับ เพียงแค่ให้เปลี่ยนชื่อ Value จาก AutoShareWks (Workstation) เป็น AutoShareServer (Server) เท่านั้นก็สามารถปิดการ Share ได้แล้วล่ะครับ หรือถ้าใครไม่แน่ใจจะใส่ทั้ง 2 ตัวก็ไม่ผิดกติกาแต่อย่างใดนะครับ ต้องขออภัยจริงๆที่ไม่ได้พูดถึงตระกูล Server ไว้ตั้งแต่แรก และต้องขอขอบคุณสำหรับคำถามจากผู้อ่านท่านนี้ด้วยครับ



ทางเลือกเปิด Drive ไม่ให้ติดไวรัส

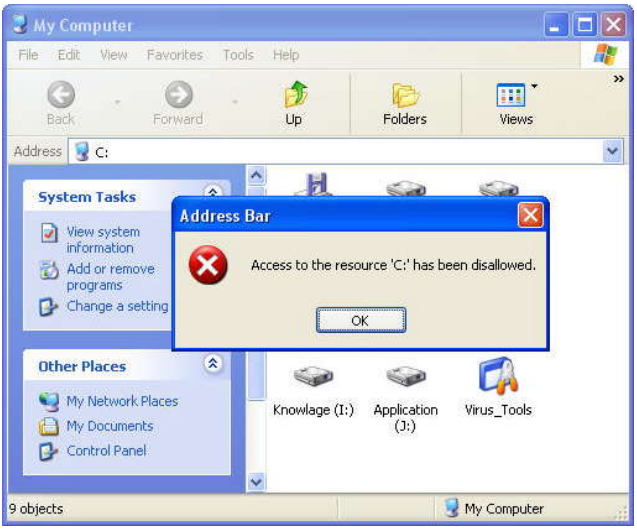
มีคำถามจากผู้อ่านมาอีกแล้วครับว่าตามที่ผมได้แนะนำในหนังสือเล่ม 1(หน้า 107) ว่าการเปิดแฟลชไดรฟ์ให้ปลอดภัยจากไวรัสนั้นให้ใช้วิธีพิมพ์อักษรชื่อไดรฟ์ลงไปในช่อง Address Bar โดยตรงเพื่อหลีกเลี่ยงการทำงานของไฟล์ Autorun.inf แต่เมื่อเค้าใช้วิธีนี้แล้วมันดันมี Error ผมจึงได้ลองหาข้อมูลดูจนพบสาเหตุและเห็นว่าน่าสนใจดีเลยนำมาเล่าสู่กันฟังครับ

ก่อนอื่นเรามาจำลองสถานการณ์กันก่อนจะได้อ่านแล้วเข้าใจง่ายขึ้น โดยให้เราเปิด Gpedit ขึ้นมา(วิธีการเปิดคงไม่ต้องแนะนำแล้วนะครับ)แล้วไปที่ User Configuration => Administrative Templates => Start Menu and Taslbar แล้วตั้งค่าของ Remove Run menu from Start Menu ให้เป็น Enabled ซึ่งก็คือการซ่อนเมนู Run ที่ไวรัสชอบทำกันนั่นเองครับ



หลังจากแก้ไขค่าตามด้านบนเรียบร้อยแล้วก็จะเห็นว่าเมนู Start => Run หายไปแล้ว ซึ่งวิธีการเอากลับมานั้นก็แค่แก้กลับเป็น Disabled ตามที่ผมได้อธิบายไว้แล้วทั้งในเล่ม 1(หน้า 166) แต่ตอนนี้เรายังไม่ต้องแก้กลับนะครับมาดูกันก่อนว่าแล้วการซ่อนเมนู Run นั้นมันเกี่ยวอะไรกับการเปิดไดรฟ์ที่ผมแนะนำไว้ล่ะ

ให้เราไปที่ Address Bar แล้วพิมพ์ชื่อไดรฟ์อะไรก็ได้ที่อยากจะเปิดลงไปสักไดรฟ์(ไม่จำเป็นต้องเป็นแฟลชไดรฟ์ก็ได้ครับ)แล้วลองมาดูผลกัน เช่นตามตัวอย่างผมต้องการเปิดไดรฟ์ C ก็พิมพ์ C: ลงไปแล้วกด Enter ผลที่ได้ก็คือเปิดไม่ได้และมี Error ตามภาพครับ

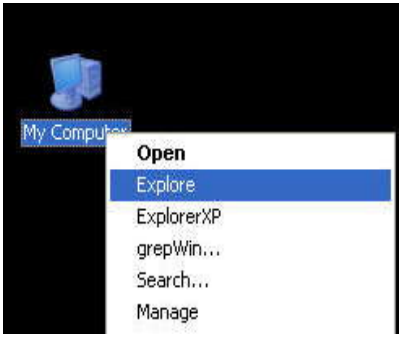


ขอขยายความตรงนี้เพิ่มอีกหน่อยนะครับว่าอาการและ Error จะต่างจากในหนังสือเล่ม 1(หน้า 170) ตรงที่ว่าอาการของหน้า 170 นั้นจะมี Error แบบนี้

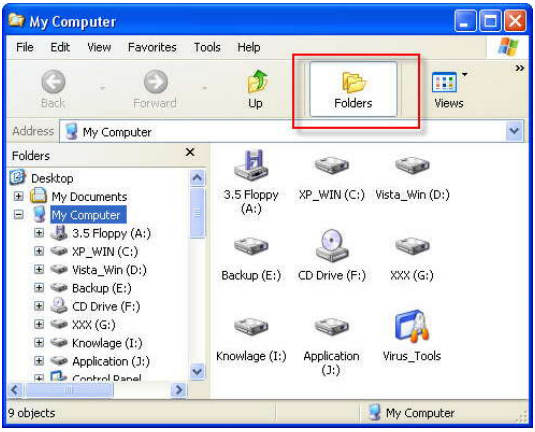
ซึ่งอาการของหน้า 170 นั้นนอกจากไม่สามารถพิมพ์ชื่อไดรฟ์ลงไปแล้วก็ยังรวมถึงการดับเบิ้ลคลิกเรียกไดรฟ์โดยตรงหรือแม้แต่การเรียกใช้โฟลเดอร์อื่นใดในไดรฟ์ที่โดน Lock ก็ไม่สามารถทำได้เลยครับ(โหดกว่ามาก)โดยจะมี Error ตามด้านบนนั่นล่ะครับ แต่สำหรับอาการที่โดนซ่อนเมนู Run นั้นเราสามารถที่จะดับเบิ้ลคลิกเรียกใช้ไดรฟ์หรือโฟลเดอร์ใดๆได้ตามปกติครับ เพียงแต่ไม่สามารถใช้การพิมพ์ชื่อไดรฟ์ลงไปได้เท่านั้นเอง ไม่งงนะครับ

คราวนี้เรามาดูวิธีการแก้ไขปัญหากันครับ สำหรับการแก้ไขปัญหานั้นก็ตรงไปตรงมาคือเมื่อรู้ว่าอาการนี้เกิดจากเมนู Run โดนซ่อนไว้เราก็ไปปิดใช้เมนู Run เท่านั้นเองครับ(แต่ต้องกำจัดไวรัสให้หมดก่อนนะครับ ไม่งั้นเราเปิดไปไวรัสมันก็แก้กลับอีก)

แต่จริงๆแล้วจุดประสงค์หลักๆที่ผมเขียนเรื่องนี้ก็คืออยากจะแนะนำอีกวิธีที่สามารถเปิดไดรฟ์ได้โดยไม่ต้องกังวลว่าไฟล์ Autorun.inf มันจะทำงาน(ในกรณีที่ยังไม่ได้ปิดการทำงานของไฟล์ Autorun.inf ตามบทข้างบนเท่านั้น แต่ถ้าเราปิดการทำงานของ Autorun.inf เรียบร้อยแล้วจะเปิดแบบไหนก็ปลอดภัย 100% ครับเพราะไฟล์ Autorun.inf นั้นโดน Windows มองข้ามไปแล้ว) นั่นคือการเปิดโดยใช้ Windows Explorer นั่นเองครับ โดยวิธีการเปิดคือ ใช้การกดปุ่ม ⊞ + E (จากที่ใดๆก็ได้ไม่จำเป็นต้องทำใน My Computer นะครับ) หรือจะใช้การคลิกขวาที่ My Computer แล้วเลือก Explore ก็ได้เช่นกัน



หรือจะใช้การเลือกรูปโฟลเดอร์บน Menu Bar ก็ได้ผลเช่นเดียวกัน ไม่ผิดกติกาแต่อย่างใดครับ แล้วแต่ว่าใครจะถนัดแบบไหน



ถึงตรงนี้ทุกคนคงนึกออกแล้วว่า Windows Explorer หน้าตาเป็นยังไง ใช่แล้วครับสำหรับหน้าต่างของ Windows Explorer นั้นก็คืออันเดียวกันกับที่เราคลิกขวาแล้วเลือก Explore ที่ตัวไดรฟ์นั่นล่ะครับ ตอนนี้หลายคนก็คงมีคำถามแล้วล่ะว่าในเมื่อบทแรกๆผมบอกไว้ว่าการคลิกขวาแล้วเลือก Explore ก็ไม่ได้ปลอดภัยจากไวรัสเช่นกัน แล้วทำไมตอนนี้ถึงให้เลือก Explore ล่ะ?

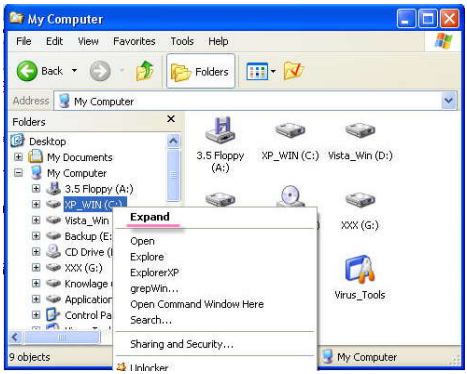
ผมขออธิบายดังนี้นะครับคือสำหรับการทำงานของไฟล์ Autorun.inf นั้นเป็นการทำงานในระดับไดรฟ์ คือจะทำงานเมื่อไฟล์ Autorun.inf อยู่ในไดรฟ์เท่านั้น ไม่ได้มีผลเมื่ออยู่ในตำแหน่งอื่นๆเช่น โฟลเดอร์ (ถึงเอาไฟล์นี้ใส่ไว้ในโฟลเดอร์ก็ไม่ได้มีผลใดๆ) ใครจะลองเอาไฟล์ Autorun.inf ตามตัวอย่างด้านบน (หน้า 14) ใส่ในโฟลเดอร์ดูก็ได้นะครับจะเห็นว่าไม่ว่าเราจะเลือก Open หรือ Explore ไฟล์ Autorun.inf ซึ่งอยู่ในนั้นก็ไม่ได้ส่งผลใดๆต่อเมนูของโฟลเดอร์นั้นๆ ต่างจากที่เอาใส่ไว้ในไดรฟ์ครับ คงพอจะเข้าใจแล้วนะครับ

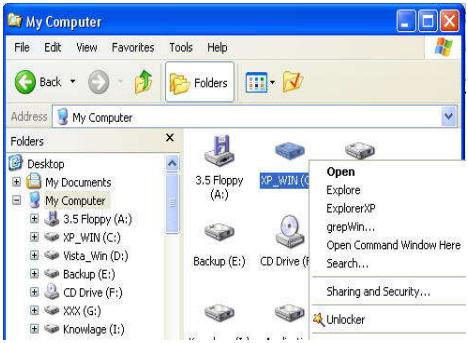
ดังนั้น My Computer ซึ่งก็เปรียบเสมือนเป็นโฟลเดอร์ๆหนึ่งซึ่งมีการเก็บไดรฟ์ไว้ภายในเท่านั้น รวมถึงการที่เราไม่สามารถที่จะนำไฟล์ใดๆรวมถึงไฟล์ Autorun.inf ไปใส่ไว้ใน My Computer โดยตรง(ถ้าจะใส่ต้องใส่ในไดรฟ์เท่านั้น) ดังนั้นเราก็หมดความกังวลเรื่องของการคลิกขวาแล้วเลือก Explore หรือ

Open ที่ My Computer แล้วจะตกหลุมพรางไปได้เลยครับ คงเข้าใจแล้วนะครับว่าทำไมผมถึงบอกว่าการเลือก Explore ที่ My Computer นั้นปลอดภัยไร้กังวล

เอาล่ะครับมาดูกันต่อเรื่องของ Windows Explorer ว่าควรใช้ยังไงและมันจะมีประโยชน์ต่อการหลีกเลี่ยงไวรัสยังไงบ้าง จากหน้าจอของ Windows Explorer นั้นเมื่อเราต้องการที่จะเรียกใช้ไดรฟ์ใดๆนั้นให้เลือกคลิกจากเมนูด้านซ้ายมือเท่านั้นนะครับห้ามดับเบิ้ลคลิกเรียกไดรฟ์ทางขวามือโดยตรง เพราะถ้ามีไฟล์ Autorun.inf อยู่ในไดรฟ์นั้นๆ การดับเบิ้ลคลิกเรียกไดรฟ์จากทางขวามือก็จะมีผลเช่นเดียวกันกับเราดับเบิ้ลคลิกเรียกใน My Computer นั่นล่ะครับ คือมันจะทำตามคำสั่งในไฟล์ Autorun.inf ทันที

เราลองมาดูรูปเปรียบเทียบกันก่อนนะครับแล้วผมจะอธิบายอีกทีว่าทำไมการเลือกจากฝั่งซ้ายถึงปลอดภัย

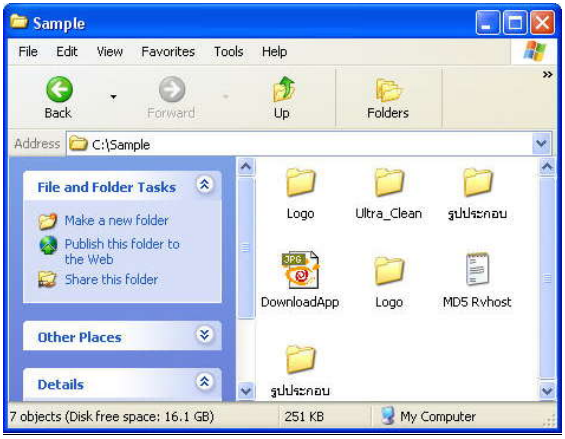




สำหรับในรูปแรกนั้นเป็นเมนูที่เกิดจากการคลิกขวาที่ไดรฟ์ C (ในฝั่งซ้ายมือ) ส่วนอีกรูปก็เป็นการคลิกขวาที่ไดรฟ์ C (ทางด้านขวามือ) เราจะเห็นว่าเมนูแรก(ตัวเข้ม)ซึ่งเป็นค่า Default นั้นจะต่างกัน โดยทางซ้ายจะเป็น **Expand** ส่วนทางขวาจะเป็น **Open** ซึ่งอธิบายง่ายๆคือค่า Default นั้นก็คือการตอบสนองต่อการดับเบิ้ลคลิกของผู้ใช้นั่นเอง(เหมือนที่กล่าวไว้ในล้วงไต๋ฯเล่ม2 หน้า 50)ครับ

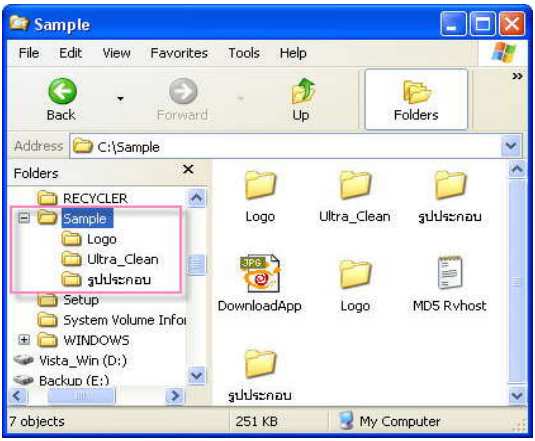
ซึ่งสำหรับเมนู Open นั้นไวรัสสามารถที่จะใช้การกำหนดค่าไว้ในไฟล์ Autorun.inf ได้ตามที่ผมได้อธิบายไว้ในล้วงไต๋เล่ม 1 และในบทแรกๆของเล่มนี้ ดังนั้นผมขอไม่อธิบายเพิ่มแล้วนะครับ ส่วนเมนู Expand นั้นยังไม่เคยพบว่าไวรัสตัวไหนใช้คำสั่งนี้ในไฟล์ Autorun.inf ครับ และจากการที่ผมทดลองดูก็ใช้ไม่ได้ผลครับแต่ผมขอไม่ทดลองให้ดูนะครับเดี๋ยวจะยืดยาวไป ถ้าใครสนใจก็ทดลองกันดูได้โดยการกำหนดเมนู Expand ในไฟล์ Autorun.inf นั่นล่ะครับ

คราวนี้เรามาดูข้อดีอีกข้อของการเปิดไดรฟ์ด้วยวิธีนี้กันครับ นั่นคือในกรณีที่เป็นไวรัสจำพวกที่สร้างโฟลเดอร์ปลอม(ล้วงไต๋ฯเล่ม 1 หน้า 117) การเปิดไดรฟ์ด้วยวิธีการนี้ทำให้เราสามารถแยกแยะไวรัสออกจากโฟลเดอร์ได้อย่างชัดเจนและสะดวกขึ้นมากเลยครับ



จากในรูปนั้นจะเห็นว่ามีโฟลเดอร์ชื่อซ้ำกันอยู่ 2 โฟลเดอร์ ซึ่งคนที่ได้อ่านเล่มแรกมาก็คงเข้าใจแล้วว่าหนึ่งในโฟลเดอร์ที่ชื่อซ้ำกันนั้นโดยแท้จริงแล้วก็คือไวรัสปลอมตัวมานั่นเอง(ผมสร้างโฟลเดอร์ Ultra_Clean ซึ่งเป็นโฟลเดอร์จริงๆไว้ด้วยโดยไม่มีไวรัสที่ปลอมตัวเป็นโฟลเดอร์ชื่อนี้เพื่อจะได้เห็นภาพชัดๆในตัวอย่างต่อไป) ซึ่งการมองแบบผ่านๆนั้นเป็นการยากที่จะแยกแยะว่าไหนตัวจริงไหนตัวปลอม

จะต้องทำการแยกแยะด้วยวิธีที่ผมได้แนะนำไว้ในหนังสือเล่มแรกจึงจะรู้ซึ่งหลายคนอาจจะรู้สึกว่ายุ่งยากโดยเฉพาะในกรณีที่ต้องรีบใช้งาน แต่การเปิดด้วย Windows Explorer นั้นจะมาช่วยแบ่งเบาภาระในการแยกแยะไวรัสจำพวกนี้ออกจากโฟลเดอร์จริงๆได้อย่างดีทีเดียวครับ ลองดูรูปประกอบนะครับ

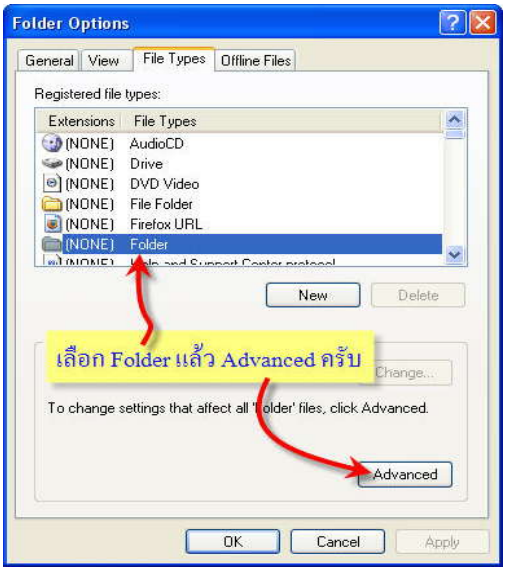


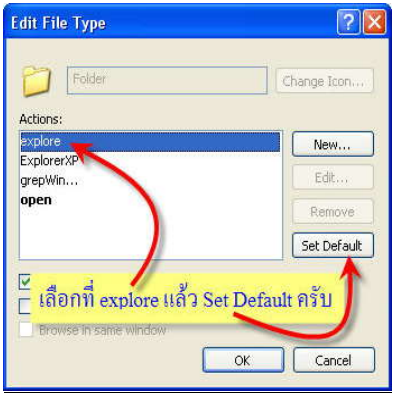
จะเห็นได้ว่าเมื่อใช้การเปิดด้วย Windows Explorer แล้วจะมีเพียงโฟลเดอร์(จริง)เท่านั้นที่ปรากฏอยู่ในเมนูฝั่งซ้ายมือ ทำให้เราสามารถที่จะเลือกเปิดโฟลเดอร์จากเมนูฝั่งซ้ายมือได้เลยโดยไม่ต้องกังวลใจว่าจะพลาดไปเรียกเจ้าตัวไวรัสขึ้นมา นั่นเป็นเพราะในเมนูทางฝั่งซ้ายของ Windows Explorer นั้นมันจะแสดงเพียงรายชื่อของไดรฟ์และโฟลเดอร์เท่านั้น ดังนั้นเจ้าไวรัสที่ปลอมตัวมาเป็นโฟลเดอร์ทั้งๆที่จริงๆแล้วเป็นไฟล์ .Exe จึงหมดสิทธิ์ที่จะมาอยู่ในฝั่งซ้ายนี้ได้ครับ ข้อสำคัญก็คือถ้าเราต้องการจะเข้าไปในโฟลเดอร์ใดๆก็ให้ใช้การเลือกจากเมนูฝั่งซ้ายเท่านั้นนะครับ(เหมือนกรณีเลือกไดรฟ์ใน My Computer ที่บอกไว้ก่อนหน้านี้) อย่าไปเผลอดับเบิ้ลคลิกเรียกทางขวาล่ะ เดี๋ยวจะพลาดตกหลุมพรางเรียกไวรัสขึ้นมาแทน

ตั้งค่าให้เปิดด้วยไดรฟ์ด้วย Windows Explorer

หลังจากได้เห็นถึงข้อดีของการเปิดไดรฟ์หรือโฟลเดอร์ด้วย Windows Explorer(ต่อไปขอเรียกว่า Explorer เพื่อความกระชับนะครับ) หลายๆคนคงอยากที่จะใช้วิธีการเปิดแบบนี้กันแล้ว

แต่ยังมีความรู้สึกว่ายุ่งยาก(ไม่ค่อยคุ้นเคย) เนื่องจากธรรมดาใช้การดับเบิ้ลคลิกเรียกเอาใน My Computer ได้เลยไม่ต้องมานั่งกดคีย์บอร์ดหรือไปเลือกเมนู Folders อีกซึ่งทำให้เสียเวลา และอาจจะลืมตัวใช้วิธีการดับเบิ้ลคลิกเหมือนเดิม(ในกรณีที่รีบมากๆ) ดังนั้นถ้าใครที่ตัดสินใจว่าจะใช้การเปิดแบบ Explorer แทนวิธีเก่าๆไปเลยล่ะก็ในหัวข้อนี้เรามาดูวิธีการตั้งค่า Default ในการเปิดให้เป็นการเปิดด้วย Explorer กันนะครับ โดยการเปิด Folder Options ขึ้นมาแล้วดูตามรูปนะครับ





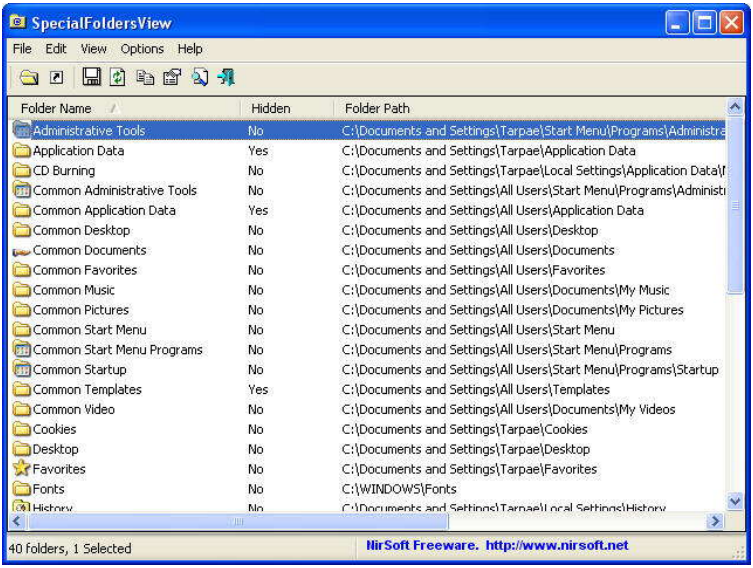
จากรูปประกอบซึ่งไม่ได้มีอะไรซับซ้อนผมคงไม่ต้องอธิบายแล้วนะครับ ขอเพิ่มเติมเพียงแค่ว่าในกรณีที่ได้ทำการติดตั้งโปรแกรม ExplorerXP ไว้ในเครื่องด้วยก็จะเห็นว่าในรูปที่ 2 นั้นเราสามารถที่จะเลือกให้ ExplorerXP เป็นค่า Default ก็ได้เช่นกัน(แล้วแต่ความชอบส่วนบุคคล ซึ่งจะว่าไปแล้วโปรแกรม ExplorerXP เองก็มีจุดแข็งกว่า Windows Explorer ตรงที่มันจะแสดงนามสกุลไฟล์ด้วยทุกๆครั้ง รวมถึงแสดงไฟล์ที่โดนซ่อนไว้ สำหรับข้อดีของ ExplorerXP นั้นอ่านได้จากทั้งในหนังสือล้วงไต๋ฯทั้ง 2 เล่มหรือจากบทความในหน้าเว็บของผมนะครับ ดังนั้นใครที่ไม่ได้มีไฟล์ที่ต้องการแอบซ่อนไว้ในเครื่อง การเลือกตั้ง ExplorerXP ให้เป็น Default ก็เป็นเรื่องดีๆที่น่าพิจารณาครับ) เพียงเท่านี้ต่อไปนี้ทุกๆครั้งที่เราดับเบิ้ลคลิกเรียกใช้ My Computer(รวมไปถึงไดรฟ์และโฟลเดอร์ต่างๆ) ก็จะกลายเป็นการเปิดด้วย Explorer แล้วล่ะครับ สังเกตได้ว่าเมื่อคลิกขวาที่ My Computer(รวมไปถึงไดรฟ์และโฟลเดอร์ต่างๆ) เมนูแรก(สีเข้ม) ซึ่งหมายถึงค่า Default จะกลายเป็น Explore แทน Open ไปเรียบร้อยแล้วครับ

สุดท้ายก่อนจบหัวข้อนี้ก็ขอย้ำอีกครั้งว่าถึงแม้เราจะตั้งค่า Explore ให้เป็นค่า Default แล้วก็ตาม แต่ขอให้เราทำการดับเบิ้ลคลิกเพียงแค่ My Computer เท่านั้นนะครับ ในส่วนของไดรฟ์และโฟลเดอร์นั้นผมแนะนำให้เลือกใช้เมนูฝั่งซ้ายของ Explorer จะปลอดภัยที่สุดครับ เนื่องจากในระดับไดรฟ์นั้นไวรัสสามารถสร้างเมนู Explore ปลอมขึ้นมาดักการดับเบิ้ลคลิกของเรา ส่วนระดับโฟลเดอร์นั้นมันก็ยังสามารถสร้างโฟลเดอร์(ปลอม)ขึ้นมาได้อีก ถ้าเราดับเบิ้ลคลิกเมื่อไหร่ก็ตกหลุมพรางของมันทันทีครับ

แนะนำโปรแกรมช่วยเปิด Special Folders

อย่างที่ได้รู้กันอยู่แล้วว่าไวรัสนั้นมักจะอาศัยสร้างตัวเองไว้ในโฟลเดอร์หลักๆของ Windows เช่น \Windows ,\Windows\System32 หรือ \Temp เป็นต้นเนื่องจากว่ามันจะง่ายในการที่จะเรียกใช้ตัวเองโดยไม่จำเป็นต้องอ้างอิง Path ตามที่ผมได้อธิบายไปแล้วในหนังสือทั้ง 2 เล่ม ซึ่งแน่นอนว่าการที่เราจะกำจัดไวรัสนั้นย่อมหลีกเลี่ยงไม่ได้ที่จะต้องเข้าไปยังโฟลเดอร์พวกนี้บ่อยๆเพื่อไปลบเจ้าไฟล์ไวรัสข้างในแต่หลายๆคนรวมทั้งผมเองด้วยก็รู้สึกว่าการเข้าโดยผ่านทาง My Computer นั้นค่อนข้างเสียเวลาเพราะจะต้องดับเบิ้ลคลิกเข้าไปทีละชั้นๆ ยิ่งถ้าเป็นโฟลเดอร์ที่อยู่ลึกๆยิ่งเสียเวลามากกว่าจะเข้าไปถึง เช่น โฟลเดอร์ Temp ซึ่งจะมี Path เป็น \Documents and Settings\ชื่อ User\Local Settings\Temp จะเห็นได้ว่าเข้าไปค่อนข้างลึก นั่นคือจะต้องดับเบิ้ลคลิกถึง 6 ครั้ง(นับตั้งแต่ My Computer)จึงจะเข้าไปถึงโฟลเดอร์นี้ได้ หรืออีกกรณีคือในบางเครื่องนั้นไม่ได้ตั้งชื่อของโฟลเดอร์เหล่านี้ตามค่า Default เช่น ตำแหน่งโฟลเดอร์ของ Windows บางคนอาจจะตั้งเป็นอย่างอื่นแทนคำว่า Windows ที่เป็นค่า Default ในกรณีที่อาจจะมีการติดตั้ง Windows ไว้หลายๆตัว

จากปัญหาที่พูดมาข้างต้นนั้นผมจึงอยากจะแนะนำให้ใช้โปรแกรม SpecialFoldersView ซึ่งเป็นโปรแกรมฟรีสามารถโหลดได้จาก http://www.nirsoft.net/utils/special_folders_view.html เพื่อเป็นการเพิ่มความสะดวกและแก้ไขปัญหาครับ สำหรับวิธีการใช้นั้นคงไม่ต้องแนะนำอะไรมากเพราะเป็นโปรแกรมที่โหลดมาก็สามารถใช้งานได้เลยโดยไม่จำเป็นต้องติดตั้ง เหมาะอย่างยิ่งที่จะเซฟเก็บไว้ในแฟลชไดรฟ์เพื่อนำติดตัวไปใช้กับเครื่องอื่นๆที่เราจะต้องไปแก้ไขปัญหาไวรัสกัน

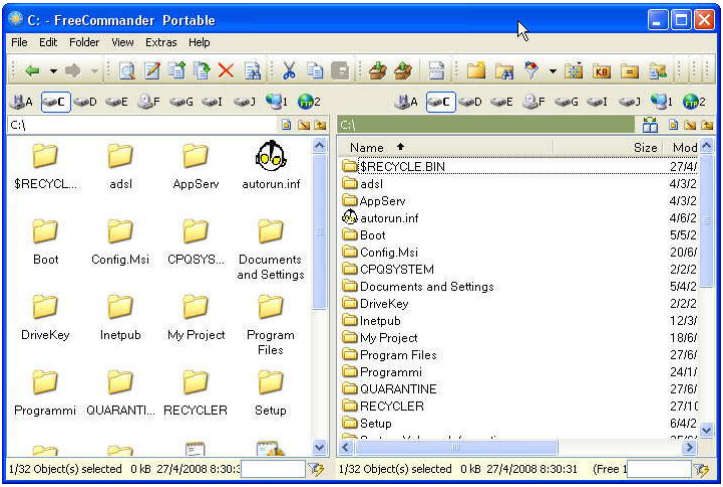


โดยสรุปการทำงานของโปรแกรมคร่าวๆคือมันจะทำการ List รายชื่อของโฟลเดอร์ที่สำคัญๆ ของ Windows ขึ้นมาทั้งหมดเราต้องการจะเข้าโฟลเดอร์ไหนก็สามารถดับเบิ้ลคลิกเพื่อเข้าไปได้เลยครับ นับว่าช่วยประหยัดเวลาไปได้มากทีเดียว แถมยังมีความสามารถ Export รายชื่อโฟลเดอร์ทั้งหลายออกมาเป็นไฟล์ HTML และอื่นๆได้อีกด้วย ลองเล่นกันดูนะครับ

แนะนำโปรแกรม FreeCommander

ห่างหายจากการอัพเดทเนื้อหาไปพอสมควรเนื่องจากไม่มีข้อมูลใหม่ๆเกี่ยวกับไวรัสที่เห็นว่าน่าสนใจพอที่จะนำมาเผยแพร่ให้รู้กัน อีกทั้งงานประจำก็ค่อนข้างยุ่งๆทำให้ไม่ค่อยมีเวลามากนัก วันนี้พอจะมีเวลาแต่ก็ไม่มีเนื้อหาที่จะเขียนมากนัก เลยตัดสินใจหยิบเอาโปรแกรมตัวหนึ่งที่ผม(เพิ่ง)ได้ไปเจอมาแนะนำกันเผื่อว่าจะยังมีใครที่เชยเหมือนผม(ไม่เคยใช้)จะได้ใช้ประโยชน์จากโปรแกรมที่ว่านี้กันครับ

สำหรับโปรแกรมที่ผมพูดถึงก็คือโปรแกรม FreeCommand ซึ่งเป็นโปรแกรมฟรี สามารถโหลดได้จาก http://www.freecommander.com โดยมีให้เลือกทั้งแบบตัว Setup ที่จะต้องทำการติดตั้งลงในเครื่องก่อน และแบบ Portable ที่สามารถใส่ในแฟลชไดรฟ์เพื่อนำไปใช้ในเครื่องอื่นๆได้เลยโดยไม่ต้องติดตั้ง



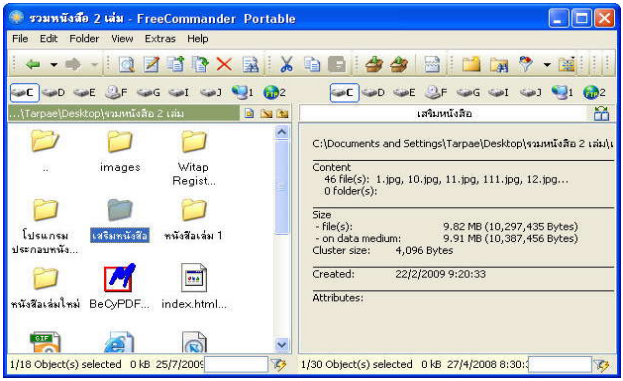
จะเห็นได้ว่าหน้าตาของโปรแกรมก็จะคล้ายๆกับ Explorer ของ Windows นั่นล่ะครับ และเนื่องจากลูกเล่นของเจ้าโปรแกรมตัวนี้มีค่อนข้างมาก ผมจึงขอพูดถึงจุดเด่นๆที่เห็นว่าน่าสนใจเท่านั้นนะครับ ในจุดอื่นๆคงต้องลองเล่นกันดูเองครับเพราะลูกเล่นมันมากจริงๆ

- สามารถใช้ดูและแก้ไขไฟล์ได้หลายรูปแบบ

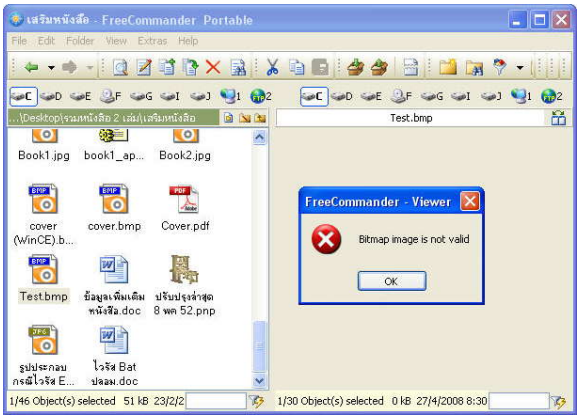
โดยตัวโปรแกรมมันเองแล้วนั้นสามารถที่จะใช้ดูไฟล์ได้หลายชนิดโดยไฟล์พื้นฐานทั่วๆไปประเภท Text , Image นั้นสามารถดูได้โดยต้องทำการติดตั้งโปรแกรมใดๆเพิ่มเติมอีก แต่ถ้า

พวกไฟล์เฉพาะๆเช่น Word มันก็จะใช้ Word ในการเปิดขึ้นมาให้เราดู โดยวิธีการดูที่ผมว่านั้นก็คือให้เราเลือกไปที่เมนู View => Quick view เท่านั้นเองครับ หน้าต่างทางฝั่งขวาก็จะทำการแสดงรายละเอียดของไฟล์ที่เราเลือกจากทางฝั่งซ้ายให้เห็นครับ เช่นจากตัวอย่างผมเลือกไฟล์รูปภาพทางฝั่งซ้าย ตัวโปรแกรมก็จะทำการแสดงรูปนั้นๆให้เห็นทันที

แล้วมันมีประโยชน์ยังไงล่ะ? สำหรับประโยชน์ของการใช้รูปแบบ Quick view นั้นข้อแรกคือถ้าทางฝั่งซ้ายมือเป็นโฟลเดอร์(ของจริง) โปรแกรมมันจะทำการแสดงรายละเอียดของโฟลเดอร์นั้นๆเช่นจำนวนไฟล์รวมถึงขนาดของไฟล์ทั้งหมดในโฟลเดอร์นั้นๆ ซึ่งข้อนี้ก็ทำให้เราสามารถที่จะแยกแยะโฟลเดอร์(จริงๆ)ออกจากตัวไวรัสที่ใช้วิธีการพรางตัวเป็นรูปโฟลเดอร์ได้อีกขั้นหนึ่ง (นอกเหนือจากการแสดงนามสกุลของไฟล์ซึ่งทำให้เราแยกแยะได้อยู่แล้ว)นั่นเอง



หรือจากกรณีตัวอย่างของไวรัสพวกตระกูล Script แปลงโฉมใน Chapter 2. ที่ผ่านมานั้นเมื่อเราดูจาก Quick view เนื่องจากไฟล์รูปภาพ .Bmp นั้นไม่ได้เป็นไฟล์รูปภาพจริงๆ ดังนั้นเมื่อโปรแกรมพยายามที่จะเปิดแบบ Quick view ขึ้นมาให้เราดูจึงทำไม่ได้และจะแสดง Error ออกมา ซึ่งสามารถทำให้เรารู้ได้ทันทีว่าไฟล์นั้นๆไม่ใช่ไฟล์รูปภาพจริงๆ ซึ่งถ้าเราต้องการที่จะดูรายละเอียดเนื้อหาภายในของไฟล์นั้นๆว่าเป็นไฟล์อะไรกันแน่ก็ให้เลือกเมนู File => Edit หรือกดปุ่ม F4 ได้เลยครับ



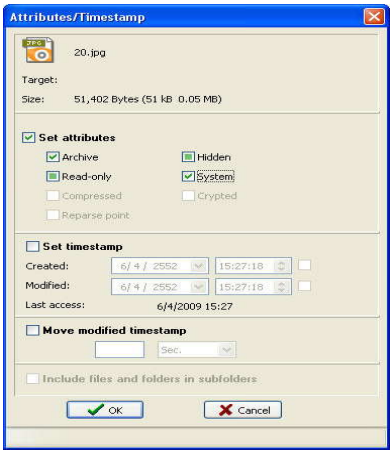
- สามารถคำนวณค่า MD5 ได้

สำหรับโปรแกรมนี้นั้นสามารถที่จะใช้ในการคำนวณหาค่า MD5 ของไฟล์ได้เลยโดยไม่จำเป็นต้องติดตั้งโปรแกรมใดๆเพิ่มเติมอีก(รายละเอียดของค่า MD5 ซึ่งเราจะนำมาประยุกต์ใช้ในการกำจัดไวรัสประเภทที่สร้างโฟลเดอร์(ปลอม)นั้นให้อ่านที่หน้า 202(ล้วงไต๋! ไวรัส เล่ม 2)นะครับ) โดยเลือกจากเมนู File => Create MD5-checksums หรือใช้ปุ่ม Ctrl+K ก็ได้ครับ

- สามารถแก้ไข Attribute ของไฟล์ประเภท System ได้

จากปัญหาการยกเลิกคุณสมบัติไฟล์ซ่อน(Hidden)ไม่ได้ ซึ่งเป็นผลพวงที่เจ้าไวรัสทิ้งไว้เนื่องจากติดปัญหาของคุณสมบัติไฟล์ระบบ(System) ตามที่ได้เขียนไว้ในล้วงไต๋!ไวรัส เล่ม 1(หน้า 176) นั้น เราสามารถใช้โปรแกรมนี้แก้ไขปัญหานี้ได้เช่นกันโดยเลือกเมนู File => Attributes หรือกดปุ่ม Shift+Enter เพื่อทำการแก้ไขค่า Attribute ต่างๆของไฟล์ได้เลยโดยไม่

จำเป็นต้องใช้คำสั่ง Attrib ผ่านทาง Cmd ให้ยุ่งยากแถมทั้งยังสามารถที่จะแก้ไขเวลาต่างๆ ของไฟล์(Timestamp)นั้นๆได้อีกด้วยครับ



- เรียกใช้เมนู Run ได้แม้โดนไวรัสปิดไว้

จากปัญหาที่ไวรัสมักจะทำการซ่อนเมนู Start =>Run เพื่อไม่ให้เราเรียกใช้โปรแกรมต่างๆได้สะดวกมากนั้น ในเบื้องต้นก่อนที่จะทำการแก้ไขปัญหาด้วย Gpedit(การแก้ปัญหาอ่านได้จากล้วงไต้ไวรัส!เล่ม 1 หน้า 166) ถ้าเรามีโปรแกรมนี้ติดตั้งไว้ก็สามารถที่จะเรียกใช้เมนู Run ได้โดยไปที่เมนู Extras => Run ได้เลยครับ

เพิ่มเติมอีกหน่อยคือจะเห็นว่าจากเมนู Extras นั้นจะมี DOS box อยู่ด้วยซึ่งอาจจะทำให้หลายๆคนคิดว่าน่าจะสามารถใช้ได้เช่นกันในกรณีที่โดนไวรัสปิดการทำงานของ CMD ไว้ ซึ่งคำตอบคือใช้ไม่ได้นะครับ เพราะตัว Dos box ที่เห็นนั้นก็เป็นเพียงการไปเรียก CMD ขึ้นมาอีกทีน่ะครับ ดังนั้นถ้า CMD ยังโดนปิดอยู่ก็ไม่สามารถใช้งานได้นะครับ ทางเลือกก็คืออาจจะใช้โปรแกรมอื่นๆแทน CMD ไปก่อน(ล้วงไต้ไวรัส! เล่ม 2 หน้า 134) ครับ

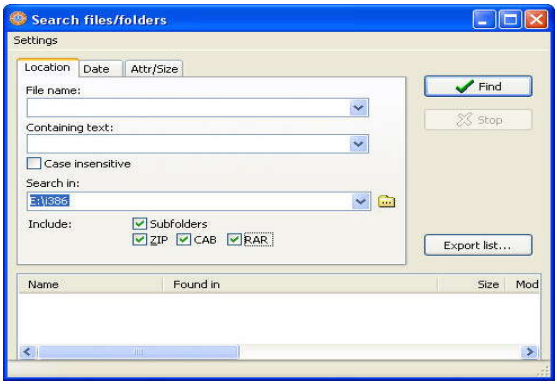
- ดู+ค้นหาไฟล์ที่มีการบีบอัดไว้ได้เลย

สำหรับข้อนี้ก็น่าสนใจครับคือโปรแกรมนี้สามารถที่จะดูไฟล์ที่มีการบีบอัด (Zip,Rar,Cab) ได้เลยโดยการดับเบิ้ลคลิกที่ไฟล์นั้นๆเราก็สามารถที่จะมองเห็นไฟล์ที่อยู่ภายในได้เลย ซึ่งจริงๆแล้วสำหรับตัว Windows เองนั้นก็สามารถที่จะดับเบิ้ลคลิกเพื่อดูไฟล์

ภายใน .Zip ได้อยู่แล้ว หรือในกรณีที่ติดตั้ง WinRAR ไว้ในเครื่อง เราก็สามารถที่จะดับเบิ้ลคลิกเพื่อดูไฟล์ใน .Rar ได้เช่นกัน แต่จุดเด่นหลักๆของโปรแกรมตัวนี้ที่ผมเห็นว่ามีประโยชน์มากกว่าการดับเบิ้ลคลิกเพื่อดูไฟล์ภายในก็คือการที่มันสามารถค้นหาภายใน ไฟล์ที่มีการบีบอัดได้อีกต่างหากครับ

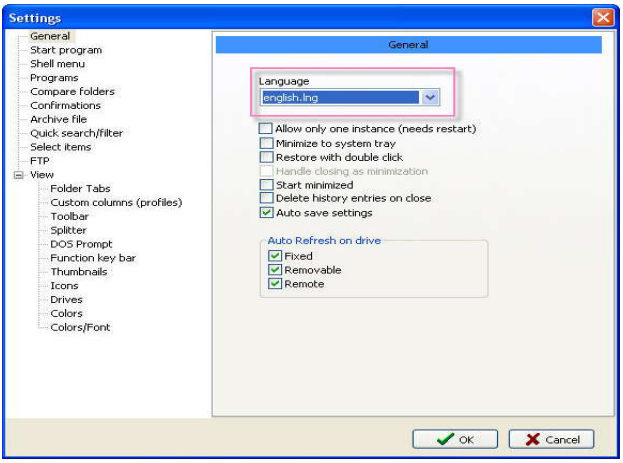
ซึ่งประโยชน์ของมันก็คือในบางครั้งเราอาจจะทำการบีบอัดไฟล์หลายๆตัวไว้ด้วยกันไม่ว่าจะใช้วิธีการ Zip หรือ Rar แต่พอนานๆไปดันจำไม่ได้ว่าไฟล์นั้นๆเราบีบอัดไว้ในชื่ออะไรกันแน่ การจะมานั่งดับเบิ้ลคลิกเพื่อดูทีละไฟล์คงเป็นเรื่องที่เสียเวลาไม่ใช่น้อย หรือในอีกกรณีตัวอย่างหนึ่งคือสำหรับไฟล์ที่อยู่ในโฟลเดอร์ I386(รายละเอียดเรื่องโฟลเดอร์นี้อยู่ในล้วงไต๋!ไวรัส เล่ม 2 หน้า 107) นั้น มีบางตัวที่ใช้วิธีการบีบอัดด้วยตัว Windows(นามสกุล .CAB) ซึ่งเราสามารถเปิดดูด้วยโปรแกรม WinRAR ได้เช่นกัน(สำหรับรายละเอียดเรื่องของไฟล์ .CAB นั้นผมจะนำมาอธิบายไว้ในคราวต่อๆไปนะครับ) ดังนั้นถ้าเราต้องการใช้ไฟล์บางไฟล์ซึ่งอยู่ในนั้นเพื่อนำมาทดแทนไฟล์ที่หายไป แน่นอนว่าเราเองไม่มีทางรู้ได้เลยว่าไฟล์นั้นๆอยู่ใน .CAB ตัวไหนเพราะเราไม่ได้สร้างเองนี่นา ดังนั้นเราจะได้ใช้ประโยชน์การค้นหาไฟล์ที่มีการบีบอัดไว้ในกรณีนี้ละครับ

โดยวิธีการค้นหาไฟล์นั้นก็ให้เราเลือกเมนู File => Search หรือกด Alt+F7 ก็จะเห็นว่ามีหน้าจอค้นหาคล้ายๆกับ Search ของตัว Windows นี่ล่ะครับ ดังนั้นวิธีการใช้ผมจึงคงไม่ต้องอธิบายเพราะใช้เหมือนกับ Search ของตัว Windows เกือบทุกอย่าง แต่จะมีเพิ่มเติมขึ้นมาคือเราสามารถที่จะเลือกให้มันทำการค้นหาภายในไฟล์ .ZIP , RAR และ .CAB ได้ด้วยนั่นเองครับ



ฝากเรื่องเมนูภาษาไทย

สำหรับโปรแกรม FreeCommander นั้นเราสามารถที่จะเลือกใช้เมนูได้หลายภาษา นอกเหนือจากภาษาอังกฤษเพียงอย่างเดียว โดยเลือกที่เมนู Extras => Settings จะเห็นได้ว่าเราสามารถที่จะเลือกรูปแบบภาษาได้มากมายตรงส่วนของ Language (รวมถึงภาษาเวียดนามที่เพิ่งเพิ่มเข้ามาเมื่อวันที่ 21 กค. 52 อ้างอิงจาก http://www.freecommander.com/fc_languages.htm) แต่ยังไม่มีภาษาไทยครับ

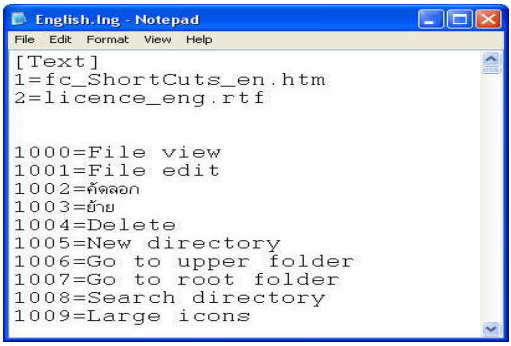


ดังนั้นผมอยากฝากว่าถ้าท่านผู้อ่านท่านไหนพอจะมีเวลาก็คงเป็นเรื่องดีที่เราจะทำเมนูภาษาไทยสำหรับโปรแกรมนี้เพื่อแจกจ่ายให้คนไทยอีกหลายๆคนที่อาจจะไม่แข็งแรงเรื่องของภาษามากนักสามารถที่จะใช้ประโยชน์จากโปรแกรมนี้ได้อย่างเต็มที่

โดยวิธีการสร้างเมนูภาษาไทยนั้นก็ทำได้ไม่ยากเย็นอะไรครับ ให้เราเข้าไปที่โฟลเดอร์ชื่อ LNG ซึ่งจะอยู่ภายในโฟลเดอร์ของโปรแกรม FreeCommander อีกที่หนึ่งขึ้นอยู่กับว่าเราใช้โปรแกรมแบบติดตั้งหรือแบบ Portable เช่นกรณีของผมใช้แบบ Portable ตำแหน่งของโฟลเดอร์ก็จะเป็นดังนี้ครับ \FreeCommanderPortable\App\FreeCommander\LNG ซึ่ง

ภายในนั้นเราจะพบไฟล์นามสกุล .lng ซึ่งทุกคนคงเดาออกว่าเป็นไฟล์ที่เก็บเมนูของแต่ละภาษานั่นเอง

สำหรับวิธีการสร้างเมนูภาษาไทยนั้นก็เพียงแค่เปิดไฟล์ English.lng ขึ้นมาด้วยโปรแกรม Notepad เราก็จะเห็นชื่อของเมนูต่างๆทั้งหมด เราเพียงทำการแก้ไขเมนูหลังเครื่องหมาย = ให้เป็นภาษาไทยตามที่เราต้องการ(ตามตัวอย่างผมแก้ไขเมนู Copy , Cut เป็นคัดลอก , ย้าย) แล้วเซฟเป็นชื่อ Thai.lng ไว้ในโฟลเดอร์เดิม เพียงเท่านี้เราก็จะมีตัวเลือกเมนูภาษาไทยเพิ่มขึ้นมาอีกภาษาแล้วล่ะครับ

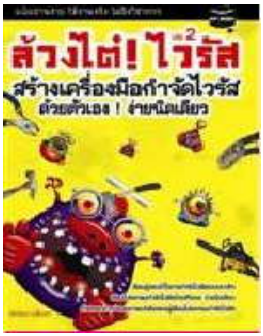


ถ้าผู้อ่านท่านไหนทำการสร้างเมนูภาษาไทยเรียบร้อยแล้วและต้องการที่จะแจกจ่ายให้คนอื่นๆได้ใช้งานด้วย ผมเองก็ยินดีที่จะเป็นศูนย์กลางในการแจกจ่ายให้โดยผ่านทางหน้าโหลดหนังสือเล่มนี้นะครับ สังคมยังอยู่ได้เพราะคนไทยเรายังแบ่งปันกันนี่ล่ะครับ

ขอขอบคุณเป็นพิเศษ

คุณ Layiji จาก www.FOnt.com สำหรับ Font สวยๆครับ

สำนักพิมพ์ Exp-Media (www.Exp-Media.net) ที่ทำให้เกิดหนังสือล้วงไต๋! ไวรัส เล่ม 1 และ 2 (แอบโฆษณาซะเลย)



สำหรับผู้ที่ต้องการรับข่าวสารการ Update ของหนังสือล้วงไต๋ฯ Add-Ons ให้เมล์มาที่ Book@DKDC-Ultra.com โดยระบุ Subject ว่า "รับข่าวหนังสือล้วงไต๋!" ผมจะได้ทำการเมล์แจ้งทุกครั้งที่มีการปรับปรุงและเพิ่มเติมเนื้อหาในหนังสือครับ

หรือสามารถเข้าไปตรวจสอบเล่มล่าสุดรวมถึงโหลดโปรแกรมต่างๆที่ผมเขียนขึ้นมาประกอบหนังสือเล่มนี้ได้ตาม Link ด้านล่างนะครับ

http://cid-53bd29aef03dd4d3.skydrive.live.com/browse.aspx/Virus-Books