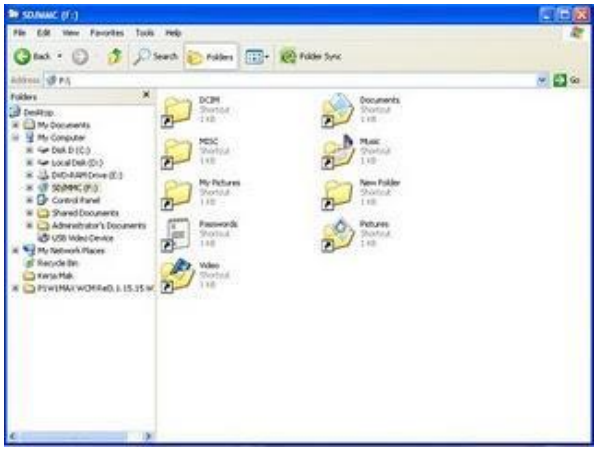
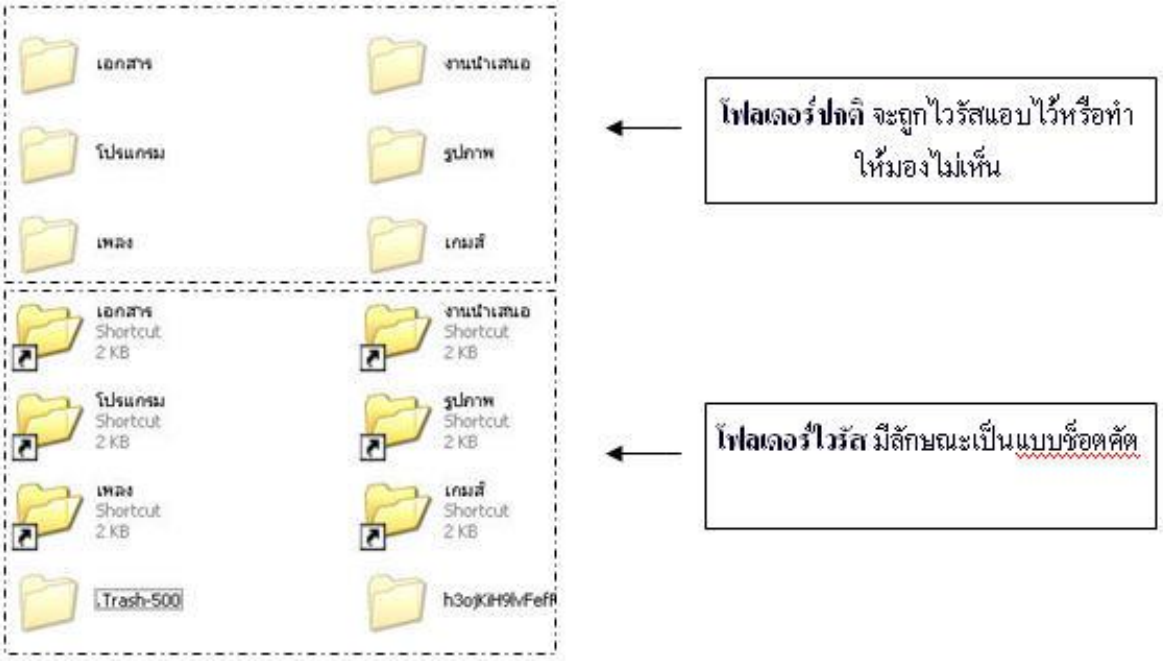
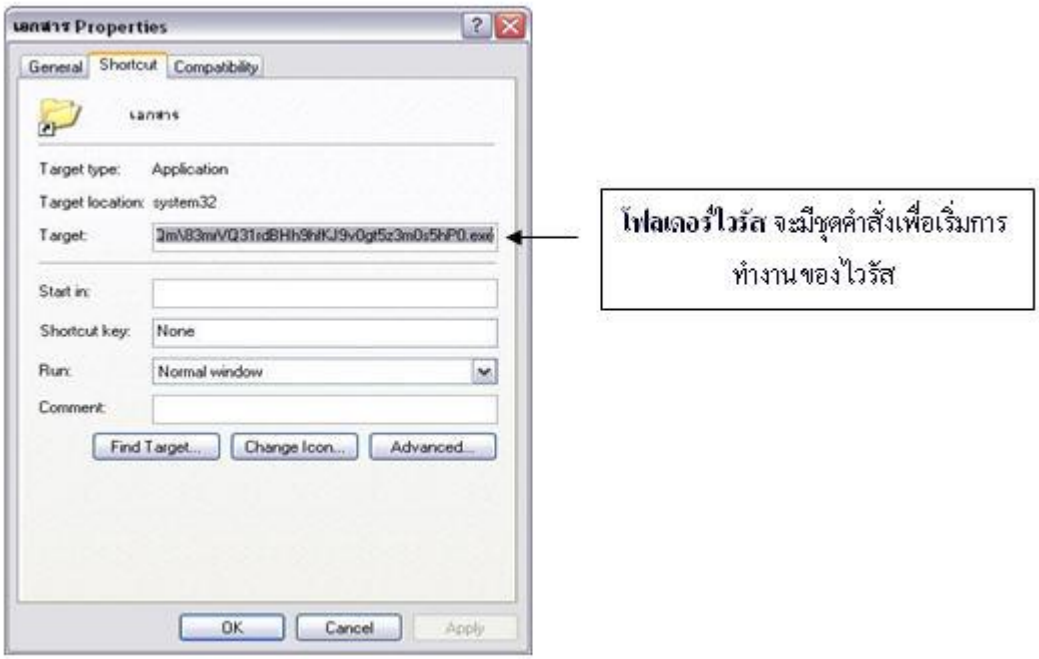


เป็นไวรัสตัวใหม่ที่กำลังแพร่กระจายผ่านทางแฮนดี้ไดร์ฟและระบบเครือข่าย ไวรัสถูกเขียนโดยคำสั่งสคริปต์ (Script) โดยจะสร้างไฟล์ช็อตคัต ลงในแฮนดี้ไดร์ฟ พร้อมคัดลอกไฟล์ไวรัส .Trash-๕๐๐ ซึ่งจะมีผลทำให้เครื่องมีประสิทธิภาพในการทำงานลดลง เป็นแหล่งแพร่กระจาย ของไวรัสไปยังเครื่องอื่นๆ หรือเปิดใช้งานไม่ได้เลย

รูปแบบและลักษณะของไวรัส





หลักการทำงาน

- เมื่อเสียบแฮนดี้ไดร์ฟที่มีไวรัสตัวนี้ ในแฮนดี้ไดร์ฟจะมีไฟล์ไวรัสซึ่งจะแฝงตัวอยู่และมีลักษณะเป็นโฟลเดอร์แบบช็อตคัต ตามรูปที่๑ ซึ่งในช็อตคัตก็จะแฝงชุดคำสั่ง เพื่อเรียกการทำงานของไวรัส
- เมื่อดับเบิลคลิกที่โฟลเดอร์ต่างๆ ที่มีลักษณะเป็นช็อตคัตภายในแฮนดี้ไดร์ฟ ไวรัสตัวนี้ก็จะทำงานโดยการก๊อปปี้ตัวเองลงไปในเครื่อง
- ไวรัสจะทำการแพร่กระจายตัวเองไปในระบบเครือข่ายและดาวน์โหลดไวรัสมาเพิ่ม
- เมื่อมีการเสียบแฮนดี้ไดร์ฟที่เครื่องที่ติดไวรัส ไวรัสจะทำการแอบซ่อนโฟล์เดอร์ที่มีอยู่ในแฮนดีไดร์ฟและคัดลอกตัวเองลงในแฮนดี้ไดร์ฟพร้อมกับเปลี่ยนชื่อให้เหมือนกับโฟลเดอร์ที่เคยมีอยู่ เพื่อหลอกให้ผู้ใช้ดับเบิลคลิกและแพร่กระจายไวรัสต่อไปเรื่อยๆ

วิธีการป้องกันและกำจัดไวรัสช็อตคัต

- อุปกรณ์แฮนดี้ไดร์ฟ หรือสื่อบันทึกข้อมูลแบบพกพา จะมีโฟลเดอร์ที่เป็นช็อตคัตดัง รูปที่๑ และโฟลเดอร์แบบปกติจะถูกแอบซ่อน หรือทำให้มองไม่เห็น
- หน้าแรก(Homepage) ของเว็บบราวเซอร์ จะถูกเปลี่ยนเป็นเว็บไซต์ที่มีตัวอักษรแปลกๆ ซึ่งตรวจสอบพบว่าจะมีการไปโหลดไวรัสมาเพิ่มเมื่อเข้าเว็บไซต์
- เครื่องมีอาการผิดปกติ เช่น เครื่องจะทำงานช้า เข้าเว็บไซต์ไม่ได้ มีเสียง "ติ๊ดๆ” ดังเป็นระยะ
- เข้าใช้งานวินโดวส์ไม่ได้ โดยมีลักษณะโหลดหน้าต่างก่อนเข้าวินโดวส์ซ้ำๆ

วิธีการใช้งานโปรแกรม SPKAutorunKiller

- ดาวน์โหลดโปรแกรมได้จาก SPKAutokillerV2.4.exe
- เมื่อดาวน์โหลดเสร็จสิ้น สามารถติดตั้งโปรแกรมได้ ๒ วิธี
    - คลิกเลือกที่ปุ่ม Run ----> Install เพื่อติดตั้งโปรแกรม
    - ดับเบิลคลิกที่ไฟล์ SPKAutokillerV2.4.exe -----> Run -----> Install เพื่อติดตั้งโปรแกรม
    - หาก ติดตั้งโปแกรมแล้วเครื่องเตือนว่ามีerror บางอย่างและไม่มีสัญลักษณ์ SPK ขึ้นที่มุมล่างขวา ให้ดาวน์โหลด โปรแกรม dotnetfxซึ่งเป็นตัวเสริมมาติดตั้งเพิ่มและดิบเบิลคลิกที่ไอค่อน Spk ที่หน้าจออีกครั้ง
- โปรแกรมจะถูกติดตั้งไว้ในเครื่อง และทำการลบไวรัสโดยอัตโนมัติเมื่อมีการเสียบแฮนดี้ไดร์ฟ หรือสื่อบันทึกข้อมูลแบบพกพา ตามรูปที่ ๒

เผยแพร่โดย : กลุ่มงานเทคโนโลยีสารสนเทศเพื่อการจัดการสำนักงาน