บทความวิชาการ

รู้ทันไวรัสคอมพิวเตอร์จาก Flash Drive

ปรีชา สมหวัง[1]
ธนัท มณีม่วง[2]

ปัจจุบันคอมพิวเตอร์ถือเป็นอุปกรณ์ช่วยอำนวยความสะดวกในการทำงาน และการสำรองข้อมูลจากคอมพิวเตอร์อุปกรณ์ Flash Drive ได้รับความนิยมอย่างมาก เนื่องจากมีขนาดเล็ก ราคาไม่แพง แต่การใช้งานดังกล่าวถ้าผู้ใช้งานไม่มีความรู้เพียงพอก็อาจไม่ได้รับความสะดวกจากอุปกรณ์ดังกล่าวมากนัก ซึ่งอาจเป็นด้วยสาเหตุจากไวรัสคอมพิวเตอร์ที่เป็นอุปสรรคดังกล่าว

ไวรัสคอมพิวเตอร์ คือ โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้ และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิดจากการนำเอาข้อมูลที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงว่าไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรมๆ หนึ่ง การที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้น จะต้องมีการถูกเรียกให้ทำงานได้นั้น ยังขึ้นอยู่กับประเภทของไวรัสแต่ละตัว ปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว จุดประสงค์ของการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับตัวผู้เขียนโปรแกรมไวรัสนั้น เช่น อาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์

วัตถุประสงค์ของบทความนี้เพื่อรู้จักวิธีป้องกันและกำจัดไวรัสคอมพิวเตอร์ที่มี Flash Drive เป็นพาหะ โดยใช้คุณสมบัติระบบปฏิบัติการวินโดว์เอ็กพี (Windows XP)

คุณลักษณะจำเพาะอุปกรณ์สำรองข้อมูล

Flash Drive มีชื่อจริงว่า USB Mass Storage Device ส่วนใหญ่เรียกกันว่า USB Flash Memory Drive , USB Flash Drive Memory หรือ USB Flash Drive การใช้งานเชื่อมต่อกับ Computer ผ่านทาง Port USB ใช้ Flash Memory เก็บข้อมูล ทำงานเป็น Drive เหมือน Hard Disk อ่านและบันทึกข้อมูลได้อย่างเดียวไม่สามารถทำอย่างอื่นได้ ซึ่งเป็นยุคต่อมาจาก Thumb drives ราคาถูกลง ความจุมีมากขึ้น ขนาดตัว Flash Drive เล็กลงด้วย บางยี่ห้อมีขนาดประมาณ 1 นิ้ว

Handy drive เป็นชื่อทางการค้า คุณสมบัติและการทำงานเหมือน Flash drive แต่ที่เพิ่มขึ้นมาคือสามารถเล่นไฟล์ Mp3 ไฟล์

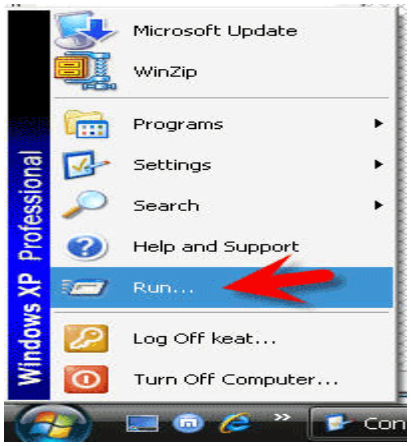
[1-2] อาจารย์ประจำคณะสารสนเทศศาสตร์ วิทยาลัยนครราชสีมา

วีดีโอ ไฟล์รูปภาพ ฟังวิทยุผ่านช่องเสียบหูฟัง และฟังก์ชันอื่นๆ ที่ผู้ผลิตจะใส่ลงไป ใช้แบตเตอรี่มีทั้งแบบใช้ถ่าน AA, AAA หรือถ่านชาตร์ ซึ่งจะชาตร์ถ่านผ่านทาง Port USB รูปลักษณ์สวยงาม แต่มีขนาดใหญ่กว่า Flash drive เนื่องจากต้องใช้แบตเตอรี่ สำหรับราคาแพงกว่า Flash drive อยู่บ้างเหมาะกับผู้ที่ต้องการใช้งานที่หลากหลาย

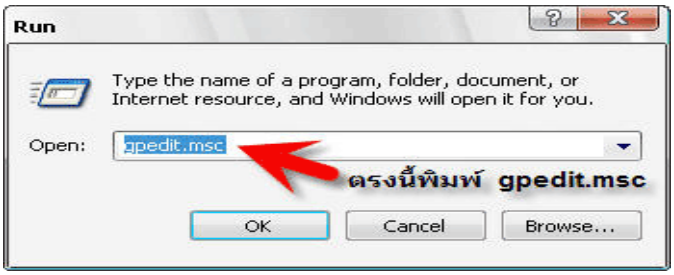
ปัญหาไวรัสที่แอบแฝงมากับ Handy drive หรือ Flash drive ติดต่อง่าย เพียงแค่ต่อ Handy drive เข้ากับคอมพิวเตอร์ ไวรัสก็พร้อมที่จะทำงาน เพื่อกระจายตัวเองได้ทุกเมื่อ บางตัวก็แค่ก่อความรำคาญ บางตัวอาจทำให้ต้องลง Windows ใหม่

ดังนั้นการป้องกัน อีกวิธีหนึ่งคือ การปิดช่องทางในการกระจายไวรัส จาก Handy drive หรือ Cd-rom ไม่รวมการแพร่กระจายทาง Network ขั้นตอนการป้องกันการแพร่กระจายไวรัสกลุ่มนี้ ก็คือบังคับไม่ให้ทำงานเมื่อนำ Handy drive มาต่อกับคอมพิวเตอร์ในทันที เพราะโดยปกติ ใน Window 2000 , XP ระบบจะทำการอ่านไฟล์ใน Handy drive หรือ CD-Rom โดยอัตโนมัติ ทำให้เจ้าไวรัสตัวนี้ กระจายตัวได้อย่างสบาย แถมเมื่อเข้าไปอยู่ในเครื่องคอมพิวเตอร์ แล้วยังเอาออกยากซะด้วย การป้องกันที่ดีที่สุดก็คือ การปิด Autorun อุปกรณ์ที่จะนำมาต่อกับคอมพิวเตอร์ ซะ คราวนี้ มันก็ไม่มีทางแพร่กระจายเข้ามาในคอมพิวเตอร์ ได้อีกต่อไป (แต่กรณีที่ ในเครื่องติดไวรัสไปแล้ว Scan แล้วลบออกไปก่อน) ขั้นตอนการปิด Autorun ก็ง่ายๆ

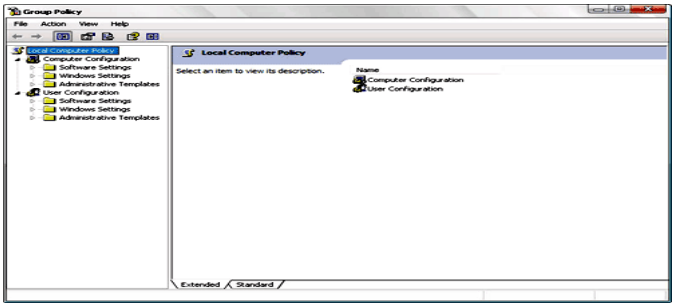
ไปที่ Start menu แล้วคลิ๊กที่ Run... ตามรูป

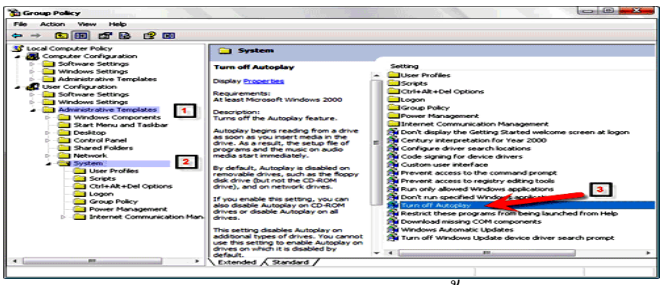


จากนั้นจะเจอ Box ตามรูป ให้พิมพ์คำว่า gpedit.msc แล้ว OK



จากนั้นจบเจอหน้าต่าง แบบรูปนี้

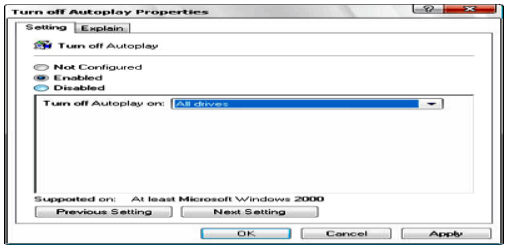




ถ้าอ่านไม่ออกก็ตามนี้ 1). Administrative template--> 2). system -->

3). ให้ Double click ที่ Turn off Autoplay กรณี win 2000 จะไม่ใช้คำว่า Turn off Autoplay

เมื่อ Double click แล้วจะได้หน้าต่างโปรแกรม หน้าตาประมาณนี้ เลือก Enable และเลือก Turn off Auto play on --> All drive

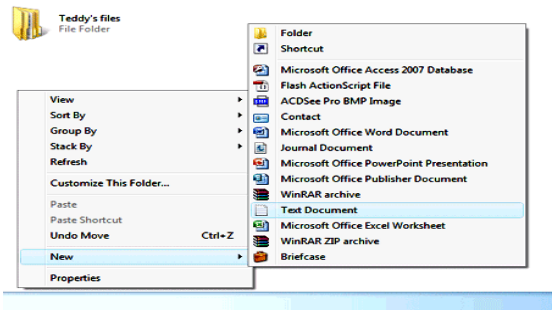


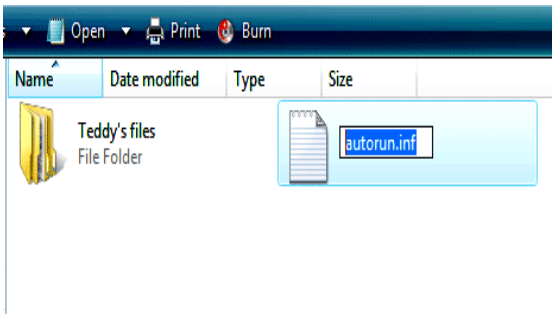
ทุกครั้งที่มีการนำเอา Handy drive มาต่อกับเครื่อง อย่าDouble Click ที่ Handy drive ทันที เพราะหากทำเช่นนั้น ที่ทำมาข้างต้นก็ไม่มีประโยชน์ (โดยเฉพาะเครื่องที่ไม่มี Scan Virus) ให้ คลิ๊กขวาที่ drive Handy drive ที่นำมาต่อกับเครื่องคอมพิวเตอร์ จากนั้นเลือก Explore เพื่อเปิดเข้าไปใน Handy drive แทนการ Double click

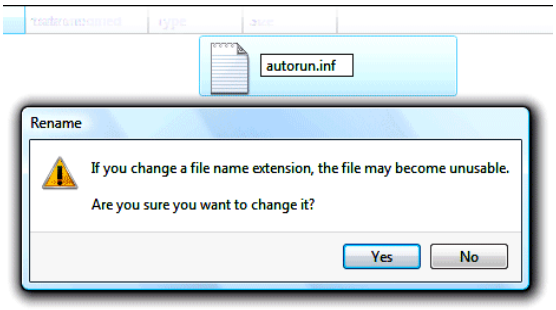
กรณี Handy drive ปกติ (แบบที่เก็บข้อมูลอย่างเดียว ดูหนังฟังเพลงไม่ได้) เมื่อคลิ๊กขวาไม่มีคำว่า Auto play โดยส่วนมากจะเจอประมาณในรูปภาพด้านล่าง หากพบ Autoplay หรือ Autorun ให้สันนิษฐานไว้ก่อนว่าในนั้นอาจมีไวรัส (http://www.mfu.ac.th)

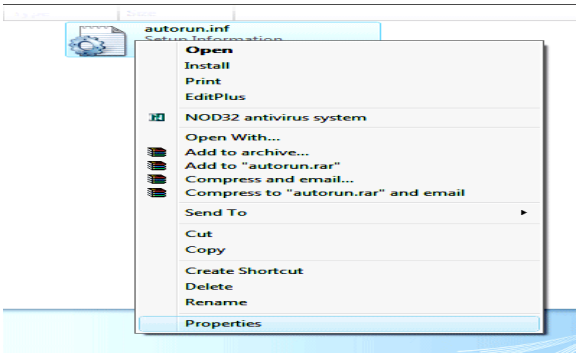
วิธีป้องกันไวรัสโดยการเขียนไฟล์ autorun.inf ลงใน Handy Drive

มีไวรัส อยู่ หลายชนิด ที่อาศัย ไฟล์ Autorun.inf ในการกระจายตัวไปติดยังคอมพิวเตอร์ เครื่องอื่นๆ ในเมื่อ ไวรัส อาศัยไฟล์ดังกล่าว แล้วจะทำอย่างไร ที่จะไม่ให้ไวรัสใช้ไฟล์ดังกล่าวได้สะดวก เริ่มจากการสร้างไฟล์ autorun.inf สร้างไว้ใน Handy Drive เพื่อป้องกัน virus ที่อยู่ใน Handy Drive ทำงานแบบ auto run









เปลี่ยนแอดทิบิวไฟล์ autorun.inf

วิธีการนี้ สามารถ ป้องกันไวรัส ที่จะอาศัยไฟล์ autorun.inf ในการแผ่กระจายตัวออกไป ถึงแม้ จะไม่ได้ป้องกัน ไม่ให้ไวรัสเขียนไฟล์ไวรัส ลงใน Handy Drive ได้ ก็ตามแต่ ก็ สามารถป้องกัน การเขียนไฟล์ Autorun.inf ได้อย่างได้ผล (http://www.com-th.net)

วิธีแก้ไข Virus Handy Drive (Flashy.exe)

ชื่อไวรัส : Backdoor.Glupzy / Disabler.I Trojan

ไฟล์ : Flashy.exe

อาการที่พบ : ไม่สามารถเรียกใช้ Task Manager, Registry Editor และ Folder Option ได้ ไม่ว่าจะเรียกด้วยวิธีใด

- หากพยายามแก้ไขด้วยวิธีการทำ System Restore ถ้าเครื่องได้ทำการตั้งรหัสเอาไว้ Flashy.exe จะทำการแก้รหัสใหม่ กรณีที่เครื่องคอมพิวเตอร์ถามรหัสผ่าน Administrator ให้ใส่ password ว่า hacked
- Error นี้จะแสดงขึ้นมาทันทีเมื่อตรวจพบการใช้งาน Controller Removeble Media ต่างๆ อยู่เฉยๆอาจจะปกติไม่มีอะไร แต่เมื่อเสียบ Card Reader เข้าไปก็จะโชว์ Error นี้ทันที
- เมื่อเสียบ Flash Drive หรือ Memory Card เข้าไปใน Card Reader แล้ว หากว่า ใน Memory Card นั้นมี Folder อยู่ Folder เหล่านั้นจะถูกเปลี่ยนให้ไปอยู่ใน สถานะ Hidden ทำให้ไม่สามารถมองเห็น Folder ในนั้นได้
- หากว่าใน Flash Drive หรือ Memory Card มี Aplication อยู่ (ที่มีนามสกุล .exe) Flashy.exe จะทำการปลอมชื่อตัวเอง ไปเป็นชื่อเดียวกันกับ Aplication นั้นๆ ทำให้เข้าใจว่า Aplication กำลังเรียกใช้งานอยู่ตามปกติ
- จะมีการเขียนค่าลงใน Memory Card ที่ไส่ลงไป และทำให้ตัวเองมีหน้าตาเหมือน Folder (คล้ายๆเจ้า Brontok) เครื่องอื่นจะมองเห็นเป็น Folder ทำให้ User ไม่ทันระวังตัว พอดับเบิ้ลคลิกไปก็เท่ากับเป็นการรัน Virus เข้าเครื่องในทันที
- Virus ตัวนี้ไม่แพร่กระจายในเครือข่าย ไม่ไปเขียนค่าหรือติดตั้งตัวเองในเครื่องอื่นๆ ในวง Lan แต่ใช้ Flash Drive หรือ Memory Card เป็นพาหะ

วิธีแก้ไขที่เครื่องคอมพิวเตอร์

1). Restart เครื่อง และระหว่างที่ Boot อยู่นั้น ให้กด F8 เพื่อเข้า Safe Mode

2). เมื่อเข้า Safe Mode แล้ว คลิกขวาที่ My Computer > Properties > แท็บ System Restore เลือก Turn off System Restore on all drives > OK

3). คลิกขวาที่ Task Bar > Task Manager (หรือ Ctrl+Alt+Del) > แท็บ Processes หาตัวที่ชื่อ Flashy.exe และ systemID.pif > End Process (กรณีถ้าตรวจพบ..)

4). เปิด Notepad แล้วก็อบปี้ข้อความด้านล่างไปวาง เซฟชื่อ killfrashy.bat เมื่อเซฟเสร็จแล้ว ให้ดับเบิ้ลคลิกที่ไฟล์ killfrashy.bat เพื่อเรียกให้ไฟล์ดังกล่าวทำงาน

@ECHO OFF

REGdeleteHKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System/vDisableRegistry Tools /f
REGdeleteHKLM\Software\Microsoft\Windows\CurrentVersion\Run /v Flashy Bot /f
REGaddHKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v Hidden /t REG_DWORD /d 2 REG
REGaddHKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v HideFileExt /t REG_DWORD /d 0
REGaddHKLM\SYSTEM\CurrentControlSet\Services\SharedAccess /v Start /t REG_DWORD /d 2

5). ไปที่ Start Menu > Programs > Startup หา systemID.pif แล้วลบทิ้ง (คลิกขวา > Delete) ไปที่ C:\WINDOWS\system และ C:\WINDOWS\system32 หาไฟล์ Flashy.exe แล้วลบทิ้ง

6). จบขั้นตอนการกำจัด Flashy.exe > Restart เครื่อง

(เข้าไปแก้ไขใน regedit)

HKEY_CURRENT_USER > Software > MicrosoftWindows > CurrentVersion > Policies > Explorer "NoFolderOptions" = "1"

HKEY_CURRENT_USER > Software > MicrosoftWindows > CurrentVersion > Explorer > Advanced "HideFileExt" = "1"

HKEY_CURRENT_USER > Software > MicrosoftWindows > CurrentVersion > Explorer > Advanced "Hidden" = "2"

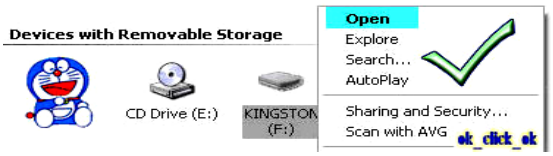
HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > SharedAccess "Start" = "4"

ข้อควรระวัง : ก่อนที่จะทำการคลิกเข้าไปยัง Folder ต่างๆ ใน Flash Drive หรือ Memory Card ให้ตรวจสอบก่อนว่าเป็น Folder หรือ Aplication

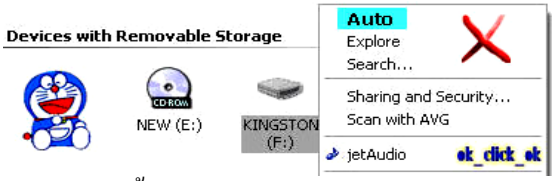
ตรวจสอบได้โดย คลิกขวาที่ Folder >Properties > ให้ดูที่ Type: ถ้าเป็น Aplication อย่าไปคลิก (http://nisit.buu.ac.th)

สำรวจให้แน่ใจว่าใน flash drive มีไวรัสอยู่หรือไม่

ก่อนเสียบ flash drive เข้าพอร์ต USB ให้กด Shift ที่คีย์บอร์ดค้างไว้ก่อน เพื่อกันไม่ให้มันเปิดขึ้นมา (Auto run) กรณีที่มีไวรัสอยู่



จากนั้นเข้าไปใน My Computer คลิกขวาที่ flash drive ถ้าขึ้นคำว่า Open อยู่ด้านบน แสดงว่าไม่มีไวรัส



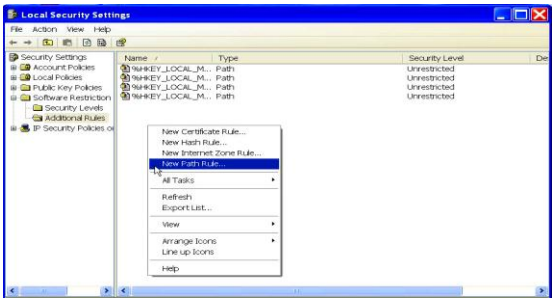
แต่ถ้าขึ้นคำว่า Auto หรือ Auto play อยู่ด้านบน แสดงว่ามีไวรัสแฝงตัวอยู่ หรือดับเบิ้ลคลิกที่ flash drive แล้วมีหน้าต่าง Open With เด้งขึ้นมาแสดงว่ามีไวรัสแฝงตัวอยู่เช่นกัน ให้ใช้โปรแกรม Antivirus สแกนหาไวรัสอีกครั้งหนึ่ง (http://okclickok.blogspot.com)

เนื่องด้วยในวันหนึ่งๆ จะมีไวรัสคอมพิวเตอร์ออกมาใหม่เป็นจำนวนมาก ดังนั้นการรับรู้ข้อมูลข่าวสารที่รวดเร็วและหาทางป้องกันจึงนับเป็นหนทางที่ดีที่สุดวิธีหนึ่งในการป้องกันไวรัสคอมพิวเตอร์ ไม่ว่าจะเป็นผู้ใช้ทั่วๆ ไปหรือแม้กระทั่งผู้ดูแลระบบเอง จึงควรที่จะหาช่องทางในการรับรู้ข่าวสารเกี่ยวกับไวรัสคอมพิวเตอร์และข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้วย (กิติศักดิ์ จิรวรรณกูล.2546)

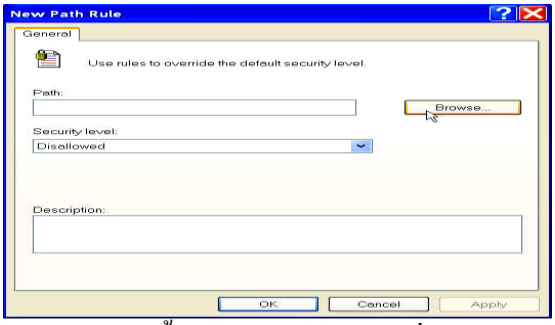
วิธีป้องกันไวรัส .Exe

ไวรัสนามสกุล .Exe เป็นอีกปัญหาหนึ่งที่สามารภสร้างปัญหาการใช้งานคอมพิวเตอร์เป็นอย่างยิ่ง วิธีป้องกันการทำงานผ่าน Flash Drive สามารถป้องกันได้ ไปที่ Start menu แล้วคลิ๊กที่ Run... ตามรูป

จากนั้นจะเจอ Box ตามรูป ให้พิมพ์คำว่า secpol.msc แล้ว OK



เลือก Software Restriction Policies ->Additional Rule ->New Path Rules



จากนั้นเลือก Browse เพื่อเลือก Drive ที่ต้องการป้องกันไฟล์ .Exe ทำงาน สามารถทำการป้องกันทุก Drive ยกเว้น Drive: C หรือที่รันระบบปฏิบัติการเนื่องจากจะทำให้ระบบปฏิบัติการทำงานไม่ได้

เอกสารอ้างอิง

กิติศักดิ์ จิรวรรณกูล. 2546. http://www.thaicert.nectec.or.th.

http://nisit.buu.ac.th.

http://okclickok.blogspot.com

http://www.com-th.net.

http://www.mfu.ac.th.