ใบความรู้ที่ 4
โปรแกรมอรรถประโยชน์

โปรแกรมอรรถประโยชน์ คืออะไร

โปรแกรมอรรถประโยชน์ (อังกฤษ: utility program/software) เรียกสั้นๆ ว่า ยูทิลิตี้ เป็นโปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ คุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ยูทิลิตี้แบ่งออกเป็นสองชนิดคือ ยูทิลิตี้สำหรับระบบปฏิบัติการ (OS utility program) และ ยูทิลิตี้อื่นๆ (stand–alone utility program) ยูทิลิตี้สำหรับระบบปฏิบัติการ

ประเภทการจัดการไฟล์ (File manager)

ประเภทการถอนโปรแกรม (Uninstaller)

ประเภทการสแกนดิสก์ (Disk Scanner)

ประเภทการจัดพื้นที่เก็บข้อมูล (Disk Defragmenter)

ประเภทรักษาหน้าจอ (Screen Saver)

ยูทิลิตี้อื่นๆ

โปรแกรมป้องกันไวรัส (Anti Virus Program)

โปรแกรมไฟร์วอลล์ (Firewall)

โปรแกรมบีบอัดไฟล์ (File Compression Utility)

โปรแกรมอรรถประโยชน์ (**อังกฤษ: utility program/software) เรียกสั้นๆ ว่า *ยูทิลิตี้* เป็นโปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ คุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ยูทิลิตี้แบ่งออกเป็นสองชนิดคือ ยูทิลิตี้สำหรับ**

ไวรัสคอมพิวเตอร์คืออะไร

โปรแกรมที่สร้างปัญหาและก่อนกวนการใช้งานคอมพิวเตอร์ อาจทำให้คอมพิวเตอร์ทำงานช้าลงหรือไม่สามารถทำงานได้เลย ปัจจุบันไวรัสคอมพิวเตอร์ได้มีการพัฒนาในรูปแบบต่างๆ ไม่ว่าจะเป็น หนอนอินเตอร์เน็ต (Worm) โทรจัน (Trojan) ข่าวไวรัสหลอกลวง (Hoax) เป็นต้น

สปายแวร์คืออะไร

โปรแกรมที่แอบติดตั้งเข้ามาในเครื่องคอมพิวเตอร์ของเรา เพื่อแสดงความโฆษณา ขณะที่เราทำงานอยู่ หรือเก็บข้อมูลการใช้อินเตอร์เน็ต เพื่อตรวจสอบพฤติกรรมการใช้งาน โดยส่วนใหญ่จะสร้างความรำคาญให้กับผู้ใช้คอมฯ

อาการของคอมพิวเตอร์ที่ติดไวรัส สปายแวร์

- มีหน้าต่างโปรแกรมเปิดอัตโนมัติ ทั้งๆ ที่ไม่ได้ทำอะไร
- คอมพิวเตอร์ทำงานช้าผิดปกติ
- การทำงานโปรแกรมต่างๆ ผิดเพี้ยนไปจากปกติ
- มีความผิดพลาดของ Windows บ่อยๆ มาก
- เครื่อง Restart Windows ตลอดเวลา

ระบบปฏิบัติการ (OS utility program) และ ยูทิลิตี้อื่นๆ (stand-alone utility program)

TOP 10 FREEWARE UTILITY PROGRAM

?

No.	ชื่อโปรแกรม	รายละเอียดความสามารถ
1	7-Zip	โปรแกรมสำหรับบีบอัดข้อมูล และเปิดดูไฟล์ รองรับไฟล์ประเภท Zip, RAR ไฟล์
2	CCleaner	โปรแกรมช่วยตรวจสอบ ลบขยะภายในเครื่องคอมพิวเตอร์ พร้อมความสามารถอื่นๆ อีก เช่น Uninstall, เช็ค Registry เป็นต้น
3	Client for Google Translate	ตัวช่วยแปลภาษา สามารถติดตั้งในเครื่องคอมฯ และเช็คผ่านออนไลน์ได้ รองรับการใช้งานแปลภาษาจากInternet, E-mail, Microsoft Word, Excel และอื่นๆ อีกมากมาย
4	LockNote	โปรแกรมช่วยเก็บรหัสผ่าน สำคัญๆ ใช้งานง่าย
5	MPCStar	โปรแกรมสำหรับดูหนัง ฟังเพลง รองรับไฟล์วิดีโอทุกประเภท
6	PDFCreator	โปรแกรมสำหรับการแปลงไฟล์จากทุกประเภทเป็น PDF เหมาะสำหรับการส่งไฟล์ผ่านอีเมล รวมทั้งเพิ่มระบบ security ให้ไฟล์ด้วย
7	PicPick Tools	เป็นโปรแกรมมากกว่าการจับภาพหน้าจอ หรือ Capture เพราะมีเครื่องมืออื่นๆ เสริมให้ด้วยอีกหลายอย่าง แถมยังเป็น Portable โปรแกรม ที่ไม่จำเป็นต้องติดตั้งลงในเครื่องคอมฯ แต่อย่างใด
8	Panda USB Vaccine	โปรแกรมยกเลิก Autorun เพื่อป้องกันไวรัส Autorun โดยเฉพาะ (ต้องมี)
9	avast! Home Antivirus	ฟรีโปรแกรมกำจัดไวรัส และสปายแวร์ ในตัวเดียวกัน
10	CDBurnXP	โปรแกรมสำหรับการ write แผ่น หรือ burn แผ่น CD ในประเภทต่างๆ ไม่ว่าจะเป็นการ burn แบบ Audio, Image, VCD/DVD เป็นต้น

Malware คืออะไร

อ่านว่า มัลแวร์ มีความหมายรวมๆ หมายถึงภัยที่เกิดขึ้นจาก ไวรัส สปายแวร์ โทรจัน และภัยอันตรายอื่นๆ ที่เกี่ยวเนื่องกับไวรัส คำว่า มัลแวร์ อาจยังไม่ได้ยินหน้าหูมากนัก และหลายๆ คนก็มักพูดรวมๆ ว่าไวรัส เช่นเดียวกัน

.....

ไวรัส Brontok

ลักษณะอาการ

- Menu Folder Option จะหายไป
- จะเกิดไฟล์ .exe ชื่อเหมือน Folder ในทุก Folder ที่เปิดเข้าไปดู
- มีหน้าเวปขึ้นมาเขียนว่า Brontok

– ไม่สามารถเรียกใช้ Registry Editor และFolder Option ได้

.....

ไวรัสคลิป VDO.EXE

เป็นไวรัสที่ไม่ได้สร้างความเสียหายร้ายแรงแก่ระบบเท่าใดแต่สร้างความรำคาญให้แก่ผู้ใช้ที่ติดไวรัสชนิดนี้มา โดยไวรัสชนิดนี้จะมีรูปร่างเหมือนFolderที่อยู่ในWin dows ทั่วๆไป แต่จะมีนามสกุลเป็น.exeทำให้เมื่อคลิกมัน ก็จะทำการฝังตัวไว้ใน C:WINDOWSsystem32 โดยจะทำการรันตัวมันเองขึ้นมาเรื่อยๆและสร้างไฟล์ คลิปVDO.exe ขึ้นมาใหม่เรื่อยๆ แม้ว่าจะทำการลบไฟล์ คลิปVDO.exe แล้วก็ตาม

.....

Svchost.exe

เป็นWormชนิดหนึ่ง ที่สร้างชื่อเลียนแบบไฟล์ Svchost.exe ของระบบปฏิบัติการWindow ซึ่งไฟล์ svchost.exe เป็นไฟล์ generic host processใช้รัน กับ DLL ไฟล์เพื่อสร้าง Service ขึ้นมาเช่น EventSystem, Netman, NtmsSvc, RasMan โดยที่สามารถรันได้หลายๆ instance พร้อมกัน อีกชื่อหนึ่งที่ใช้คือW32.CodeBlue ซึ่งส่งผลกระทบกับระบบปฏิบัติการ Windows ที่ใช้งานโปรแกรมประยุกต์ IIS

.....

Flashy.exe

ลักษณะอาการ

– ไม่สามารถเรียกใช้ Task Manager, Registry Editor และFolder Option ได้

–หากพยายามแก้ไขด้วยวิธีการทำ System Restore ถ้าเครื่องของเราได้ทำการตั้งรหัสเอาไว้ Flashy.exe จะทำการแก้รหัสของเราใหม่ ทำให้ไม่สามารถ Login เข้าเครื่องของเราได้อีกเลย

– Error นี้จะแสดงขึ้นมาทันทีเมื่อ ตรวจพบการใช้งาน Controller ของ Removeble Media ต่างๆ

–อยู่เฉยๆอาจจะปกติไม่มีอะไร แต่เมื่อเสียบ Card Reader เข้าไปก็จะโชว์ Error นี้ทันที

– เมื่อเสียบFlash Driveเข้าไปหรือเสียบ Memory Card เข้าไปใน Card Reader แล้ว

– หากว่าใน Memory Card หรือ Flash Drive ของเรามี Aplication อยู่ (นามสกุล .exe) Flashy.exe จะทำการปลอมชื่อตัวเองไปเป็นชื่อเดียวกัน Aplication นั้นๆ ทำให้เข้าใจว่าAplication ของเรากำลังเรียกใช้งานอยู่ตามปกติ จะมีการเขียนค่าลงใน Memory Card ที่เราไส่ลงไป และทำให้ตัวเองมีหน้าตาเหมือน Folder และเมื่อเราเอาไปใช้ที่ใหม่ เครื่องอื่นจะมองเห็นเป็น Folder ทำให้ User ไม่ทันระวังตัว พอดับเบิ้ลคลิกไปก็เท่ากับเป็นการรัน Virus เข้าเครื่องในทันที

– Virus ตัวนี้ไม่แพร่กระจายในเครือข่าย (คือไม่ใช่ อยู่ๆก็ไปเขียนค่าหรือ ติดตั้งตัวเองในเครื่องอื่นๆในวง Lan ของเรา มันจะอยู่แต่เครื่องที่มันอยู่เท่านั้น แต่ใช้ Flash Drive เป็นพาหะแทน)

– อาการจะแสดงผลในทันที ไม่รีรอค่อยๆ เป็นค่อยๆ ไป

.....

Toy.exe

ลักษณะอาการ

1.เมื่อเปิดเครื่องขึ้นมาหน้า Desktop จะมีภาษาจีนและ ภาษาอังกฤษขึ้นมา

2.ไม่สามารถ เข้า Local Disk ต่างๆได้ตามปกติรวมถึงFlash Drive ด้วยโดยจะดับเบิ้ลคลิ๊กเข้าDrive ต่างๆ

โดยตรงไม่ได้ ต้องคลิ๊กขวาแล้ว Open หรือ Explore เท่านั้น

.....

Windows Genuine

เนื่องจากคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows XP PRo ผิดลิขสิทธิ์ทั่วโลกกว่าครึ่งกำลังถูก Microsoft ตรวจสอบลิขสิทธิ์ทำให้ต้อง Format Harddisk ใหม่ทั้งหมด ผ่านทาง Windows Update ปัญหานี้เกิดจากตัวอัพเดตที่มีรหัส KB890859 โดยจะทำให้ user mode ของWindowsเกิดปัญหา จะเริ่มจาก Microsoft จะเข้ามาเตือนว่า Update พร้อมสำหรับ โหลดแล้ว (สำหรับผู้ที่ตั้งเป็น Notify me but don't download) เมื่อการอัพเดตเสร็จสมบูรณ์ Product Key จะถูกส่งไปยัง Microsoft Server เพื่อดูว่าผิดลิขสิทธิ์หรือไม่ หากผิด เมื่อเครื่องคุณ Restart แล้วก็จะไม่สามารถLogonได้ เครื่องจะมีหน้าจอสีฟ้า เกิดจากการแก้ไขไฟล์ในระดับ kernel ทำให้เกิด c000021a fatal error

.....

ไวรัส Godzila

ลักษณะอาการ

1.เครื่องจะไม่สามารถ Double Click เปิดไดร์ฟต่างๆได้ แต่จะคลิกเมาส์ขวาเพื่อเปิดไดร์ฟโดยเลือกเมนู Open หรือExplore

2.มีข้อความปรากฏบน Title Bar ของ Internet Explorer ว่า “Hacked By Godzilla”

.....

ไวรัส AdobeR.exe Win32/RJump.A

วิธีกำจัด

ไวรัสตัวนี้ติดจากแฮนดี้ไดว์ฟเราควรปิดไม่ให้แฮนดี้ไดว์ฟเปิดเองอัตโนมัติเวลาเสียบ เพราะปกติเสียบแฮนดี้ไดว์ฟปุ๊บ ก็จะเด้งขึ้นขึ้นมา ถามเราว่าจะเปิดแฮนดี้ไดว์ฟด้วยโปรแกรมอะไรซึ่งหากว่ าในแฮนดี้ไดว์ฟนั้นมีไฟล์ Autorun.inf อยู่ มันก็จะเปิดตามคำสั่งที่อยู่ในไฟล์Autorun.infโดยอัตโนมัติ ซึ่งแล้วแต่ไวรัสว่ามันจะเขียนคำสั่งให้รันตัวไหนขึ้ นมาไฟล์Autorun.infสามารถเปิดอ่านได้โดยดับเบิ้ลคลิก ได้เลยไม่เป็นอันตรายครับ

.....

วิธีปิดไม่ให้แฮนดี้ไดว์ฟเปิดเองอัตโนมัต

Start ----> Run ---> gpedit.msc ---->Computer Configuration--->Administrative Templetes ----> system --->ดูในช่องขวามือ ดับเบิ้ลคลิกคำว่า Turn Off Auto play เลือกเป็น Enabled ในช่อง Turn Off Auto playon = All drives กด OK แล้วเวลาเสียบแฮนดี้ไดว์ฟเข้า My computer เพื่อความปลอดภัยอย่าไปดับเบิ้ลคลิกแฮนดี้ไดว์ฟ ควรคลิกขวาดูว่ามีคำว่า Auto หรือ Auto run หากมีมีไวรัสแน่นอน ให้เราเลือกOpenนะครับ แล้วเราก็ไปลบไฟล์ ไปลบไฟล์ไวรัส โดย ไปที่ My computer -->Tools --> Folder options -->View --> หัวข้อ Hiden files and folder ใต้นั้นให้ติ๊ก เลือก Show hiden file and folder แล้วติ๊กถูกสองบรรทัดล่างออกด้วย แล้วOK (อย่าทำกลับคืน) แล้วคลิกขวาที่แฮนดี้ไดว์ฟ เลือก Open แล้วลบไฟล์ Autorun.inf Adober.exe msvcr71.dll ravmonlog สังเกตง่ายจะจางๆ หากลบไม่ได้แสดงว่าไวรัสมันทำงานอยู่นั่นหมายความว่า คุณเผลอดับเบิ้ลคลิกแฮนดี้ไดว์ฟ ให้คุณกด Ctrl+Alt+Delete โปรแกรม Task Manager จะขึ้นมานะครับ หลังจากนั้นให้คุณเลือกในแถบProcesses หาโปรแกรมที่ชื่อว่า AdobeR.exe หลังจากนั้นให้คุณกด End Task แล้วกด OKได้เลย แล้วก็ไปลบไฟล์AdobeR.exe ใน C:WINDOWS แล้ว

ก็ไปลบคำสั่งในรีจิสทรี้ โดย Start ----> Run --->regedit

-->HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run

แล้วมองขวามือลบDWORDชื่อว่า RAVD แล้วก็ปิด ก็เสร็จ

.....

Sality Off สำหรับคนโดนไวรัส Win32/sality เล่นงาน

ขั้นตอนการแก้ไข

ข้อควรจำหลังจากโหลดไฟล์เสร็จแล้วไม่ต้องคลายออกมาจาก Zip คลายออกปุ๊บโดนมันเกาะปั๊บแน่ๆ ให้เปิดไฟล์ Sality_off ในไฟล์ zip เปิดแล้วโปรแกรม Sality_off จะทำการสแกนและหยุดไวรัส Sality รอจนเสร็จ อาจจะนานหน่อย โดยโปรแกรมนี้จะสแกนทุกๆไดว์ฟทุกๆไฟล์ที่น่าสงสัยว่า Salityเกาะอยู่ เมื่อเสร็จแล้วจะขึ้นให้คุณกดปุ่มใดก็ได้ แล้วก็ติดตั้งแอนตี้ไวรัสKASPERSK