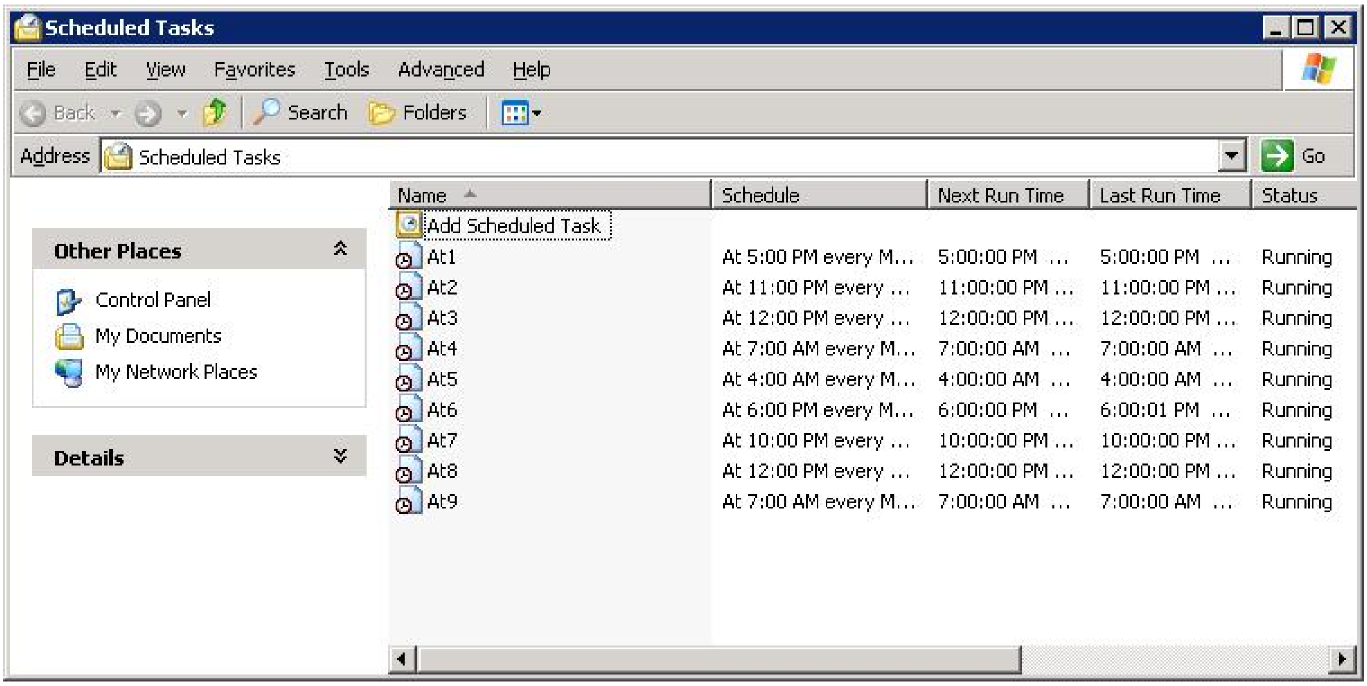
ฆ่าล้างเผ่าพันธุ์ Conficker

ชื่อที่คุ้นหู Conficker , Downandup , Kido เป็นหนอนที่แพร่กระจายตัวเองโดยโจมตีผ่านช่องโหว่ Windows Server service (SVCHOST.EXE) ของระบบปฏิบัติการไมโครซอฟท์วินโดว์ รายละเอียดติดตามได้ที่ http://www.thaicert.nectec.or.th/advisory/alert/conficker_r.php

เมื่อติดหนอนชนิดนี้แล้ว สิ่งที่เกิดขึ้นคือ เครื่องแม่ข่ายที่ทำหน้าที่เป็นโดเม็น จะเกิดภาวะ Over Load คือ ไม่สามารถรองรับการเรียกใช้งานของเครื่องลูกข่ายได้ สืบเนื่องมาจากหนอนชนิดนี้จะสร้าง Connections จำนวนมาก

วิธีสังเกตุการติดเชื้ออย่างง่ายคือ

- คลิ๊กที่ start –> accessories –> system tools –> scheduled tasks จะสังเกตุเห็น tasks ที่ขึ้นต้นด้วย At


Scheduled Tasks
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Folders
Address
Scheduled Tasks
Go
Other Places
Control Panel
My Documents
My Network Places
Details

Name	Schedule	Next Run Time	Last Run Time	Status
Add Scheduled Task				
At1	At 5:00 PM every M...	5:00:00 PM ...	5:00:00 PM ...	Running
At2	At 11:00 PM every ...	11:00:00 PM ...	11:00:00 PM ...	Running
At3	At 12:00 PM every ...	12:00:00 PM ...	12:00:00 PM ...	Running
At4	At 7:00 AM every M...	7:00:00 AM ...	7:00:00 AM ...	Running
At5	At 4:00 AM every M...	4:00:00 AM ...	4:00:00 AM ...	Running
At6	At 6:00 PM every M...	6:00:00 PM ...	6:00:01 PM ...	Running
At7	At 10:00 PM every ...	10:00:00 PM ...	10:00:00 PM ...	Running
At8	At 12:00 PM every ...	12:00:00 PM ...	12:00:00 PM ...	Running
At9	At 7:00 AM every M...	7:00:00 AM ...	7:00:00 AM ...	Running

- ที่ Task Manager จะสังเกตุการทำงานของ Process ที่ชื่อ rundll32.exe จำนวนมาก

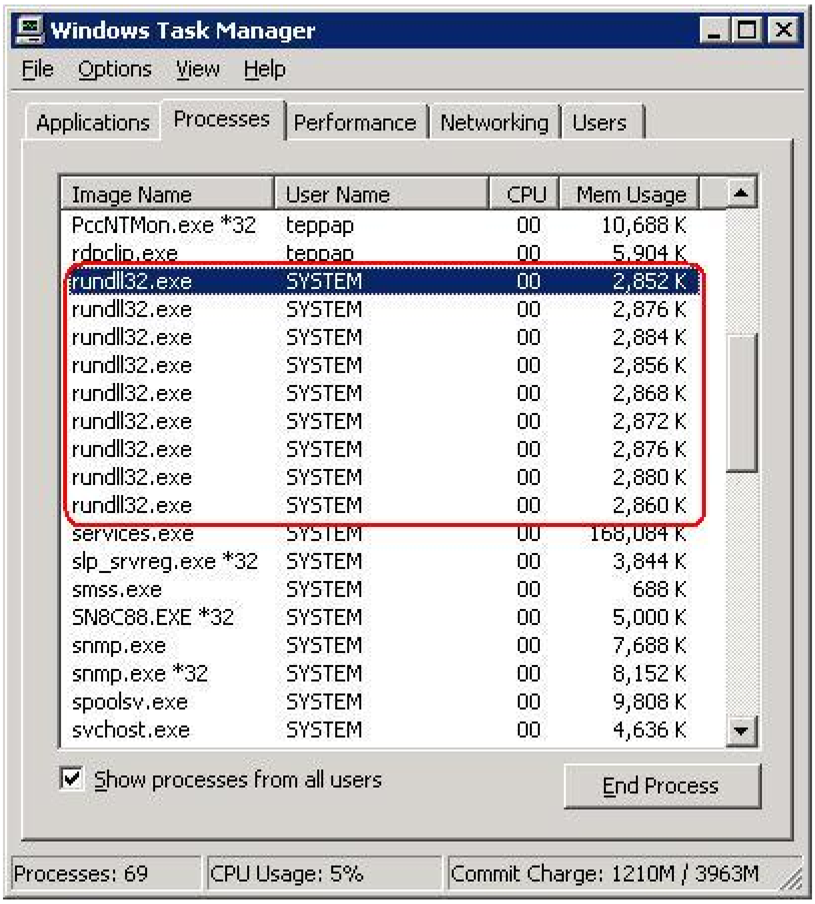
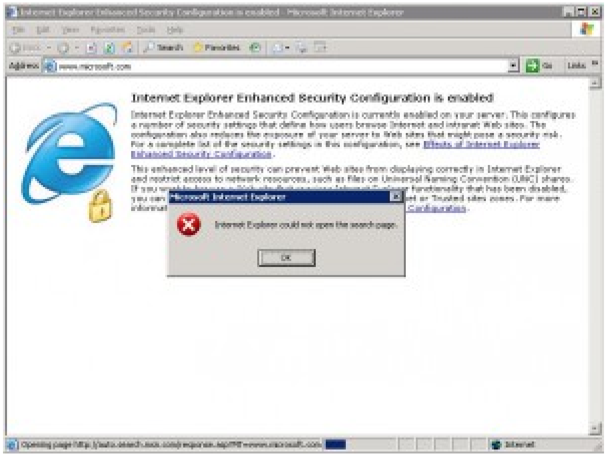

Windows Task Manager
File
Options
View
Help
Applications
Processes
Performance
Networking
Users
End Process

Image Name	User Name	CPU	Mem Usage
PccNTMon.exe *32	teppap	00	10,688 K
rdpclip.exe	teppap	00	5,904 K
rundll32.exe	SYSTEM	00	2,852 K
rundll32.exe	SYSTEM	00	2,876 K
rundll32.exe	SYSTEM	00	2,884 K
rundll32.exe	SYSTEM	00	2,856 K
rundll32.exe	SYSTEM	00	2,868 K
rundll32.exe	SYSTEM	00	2,872 K
rundll32.exe	SYSTEM	00	2,876 K
rundll32.exe	SYSTEM	00	2,880 K
rundll32.exe	SYSTEM	00	2,860 K
services.exe	SYSTEM	00	168,084 K
slp_srvreg.exe *32	SYSTEM	00	3,844 K
smss.exe	SYSTEM	00	688 K
SN8C88.EXE *32	SYSTEM	00	5,000 K
snmp.exe	SYSTEM	00	7,688 K
snmp.exe *32	SYSTEM	00	8,152 K
spoolsv.exe	SYSTEM	00	9,808 K
svchost.exe	SYSTEM	00	4,636 K

☑ Show processes from all users

Processes: 69 | CPU Usage: 5% | Commit Charge: 1210M / 3963M

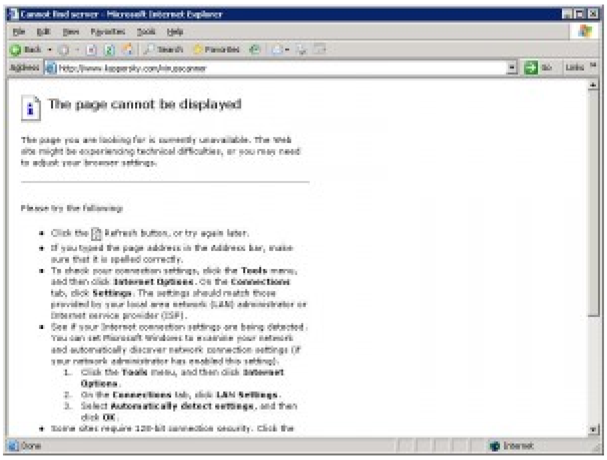
- ที่เบราเซอร์ จะไม่สามารถเข้าเว็บไซต์ที่เป็นระบบ https และเว็บไซต์เกี่ยวกับ antivirus รวมไปถึงเว็บไซต์ของ microsoft ด้วย


Address
www.microsoft.com
OK

Internet Explorer Enhanced Security Configuration is enabled

Microsoft Internet Explorer

Internet Explorer could not open the search page.


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Done
Internet

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the **Tools** menu, and then click **Internet Options**.
  2. On the **Connections** tab, click **LAN Settings**.
  3. Select **Automatically detect settings**, and then click **OK**.
- Some sites require 128-bit connection security. Click the

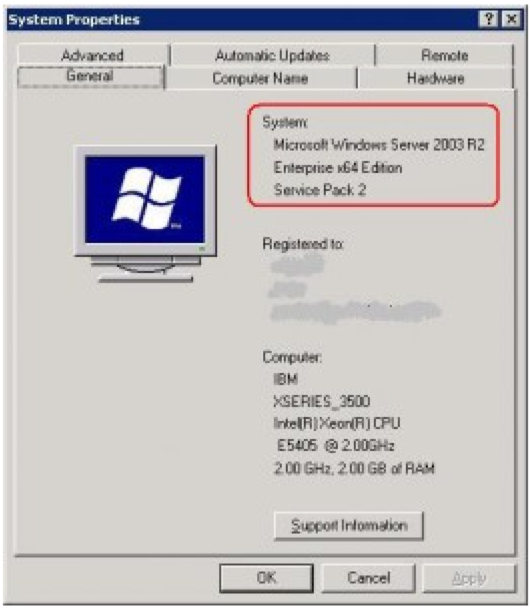
เมื่อมีอาการอย่างใดอย่างหนึ่งใน 3 อาการข้างต้นนี้ ขอให้แน่ใจได้เลยว่า เครื่องของท่านอาจจะมีหนอนชนิดนี้ฝังตัวอยู่ในเครื่องแล้ว การแก้ไขปัญหาของหนอนชนิดนี้ ค่อนข้างยุ่งยากพอสมควร เพราะหนอนอาศัยการทำงานผ่านระบบเครือข่าย ที่สำคัญดังนี้

- แชร์ไฟล์ โดยไม่ใส่รหัสผ่าน หรือรหัสผ่านคาดเดาได้ง่าย
- ตั้งรหัสผ่านของ Administrator หรือผู้ที่ถือสิทธิของ Administrator ง่ายเกินไป
- ฐานข้อมูลของ Antivirus เป็นรุ่นเก่า
- การใช้งาน Flash Drive อย่างไม่ระมัดระวัง

ขั้นตอนการกำจัดหนอนชนิดนี้ ฉบับราชมงคลล้านนา (เฉพาะ ระบบปฏิบัติการ windows 2003 server 32 และ 64 bit) คือ

- ดาวน์โหลด patch และ Fix tools ที่นี่ [download id=”4″] (เฉพาะ kb890830 และ kkiller ให้ดาวน์โหลดเวอร์ชั่นล่าสุดจากเว็บไซต์เจ้าของผลิตภัณฑ์)
  - หรือตรวจสอบไฟล์ KB ดังต่อไปนี้ที่เว็บไซต์ Microsoft อีกครั้ง
    - KB957097
    - KB958644
    - KB958687
    - kb890830 ** สำหรับสแกนไวรัส ในเว็บ noc.rmutl.ac.th นี้เวอร์ชั่น 2□.□8
    - KKiller.exe ในเว็บ noc.rmutl.ac.th นี้เวอร์ชั่น 3.□4.□4

- ทำการแตกไฟล์ไว้ตำแหน่งที่สังเกตุเห็นได้ชัด
- ตรวจสอบดูว่า ระบบปฏิบัติการที่ใช้เป็น 32 หรือ 64 bit

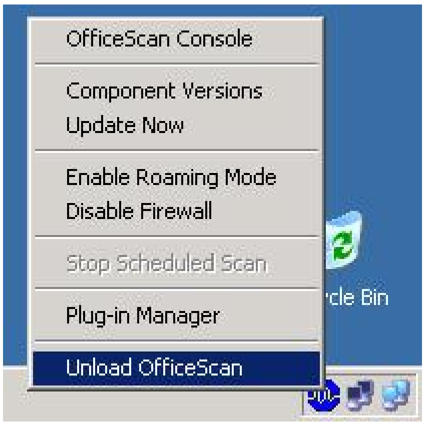

System Properties
Advanced
Automatic Updates
Remote
General
Computer Name
Hardware
Support Information
OK
Cancel
Apply

System:
Microsoft Windows Server 2003 R2
Enterprise x64 Edition
Service Pack 2

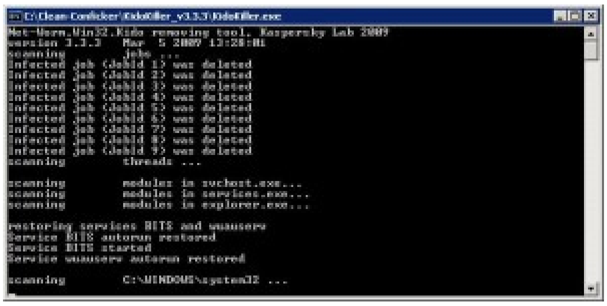
Registered to:
[redacted]

Computer:
IBM
XSERIES_3500
Intel(R) Xeon(R) CPU
E5405 @ 2.00GHz
2.00 GHz, 2.00 GB of RAM

- ให้หยุดการทำงานของ antivirus ในเครื่อง เพื่อป้องกันการรบกวนการทำงานของซอฟต์แวร์ตัวอื่น **สำคัญมาก


OfficeScan Console
Component Versions
Update Now
Enable Roaming Mode
Disable Firewall
Stop Scheduled Scan
Plug-in Manager
Unload OfficeScan
cle Bin

- ยกตัวอย่างว่าเป็น 64 bit ขั้นตอนแรก ให้คลิ๊กที่ ไฟล์ KKiller.exe


C:\Clean Conficker\KidoKiller_v3.3.3\KidoKiller.exe

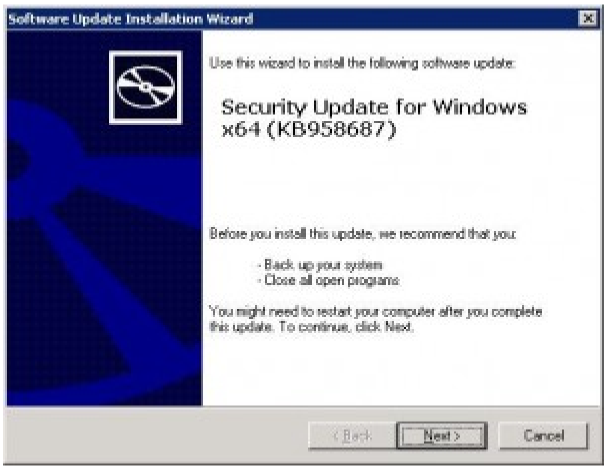
```
Net-Worm.Win32.Kido removing tool. Kaspersky Lab 2009
version 3.3.3   Mar  5 2009 13:28:01
scanning         jobs ...
Infected job (JobId 1) was deleted
Infected job (JobId 2) was deleted
Infected job (JobId 3) was deleted
Infected job (JobId 4) was deleted
Infected job (JobId 5) was deleted
Infected job (JobId 6) was deleted
Infected job (JobId 7) was deleted
Infected job (JobId 8) was deleted
Infected job (JobId 9) was deleted
scanning         threads ...

scanning         modules in svchost.exe...
scanning         modules in services.exe...
scanning         modules in explorer.exe...

restoring services BITS and wuauserv
Service BITS autorun restored
Service BITS started
Service wuauserv autorun restored

scanning         C:\WINDOWS\system32 ...
```

- ทำการสแกนหนอนอีกครั้งด้วยเครื่องมือของไมโครซอฟต์ที่ชื่อว่า windows-kb890830-x64-v2.8.exe (เจอหรือไม่เจอไวรัส ก็ไม่เป็นไรครับ)
- ให้ทำการติดตั้ง patch (เลือกว่าเป็น 32 หรือ 64 bit) ให้ครบทั้ง **3** ตัว เพื่ออุดช่องโหว่ที่หนอนใช้ในการติดต่อ



Use this wizard to install the following software update:

Security Update for Windows x64 (KB958687)

Before you install this update, we recommend that you:

- Back up your system
- Close all open programs

You might need to restart your computer after you complete this update. To continue, click Next.

- รีสตาร์ทเครื่องทันที
- เมื่อรีสตาร์ทเครื่องมาแล้ว ให้หยุดการทำงานของ Antivirus ในเครื่อง
- ใช้ Antivirus Online ในการตรวจสอบอีกครั้ง (เลือกตัวใดตัวหนึ่งก็ได้ แต่ผมเลือก kaspersky ขนาดประมาณ 50 Mb)
  - Kaspersky
  - Trend Micro
  - Bitdefender ** ติดตั้งที่เครื่องแม่ข่าย ล็อกอินด้วยผู้ใช้ที่มีสิทธิ Administrator แล้วสั่งสแกนทั้งระบบ รวมไปถึงเครื่องลูกข่ายที่ Join Domains ด้วย
- ให้ทำการเปิดระบบ **Automatic update** และทำการ **update** ระบบปฏิบัติการทันที
- ทดสอบว่ายังมีอาการผิดปกติดังที่แจ้งไว้ขั้นต้นหรือไม่ หากไม่พบแล้ว แสดงว่า ได้กำจัดหนอนชนิดนี้ออกจากเครื่องเป็นที่เรียบร้อยแล้ว แต่ต้องคอยดูแลอีกซักระยะ เพื่อไม่ให้กลับมาติดอีก

** หวังว่า คงช่วยแก้ไขปัญหาเบื้องต้นได้นะครับ