เกิดมาก็ฆ่าอีก Conficker ภาค 3

แม้ว่าข่าวคราวของ Conficker จะเงียบ ๆ ไปบ้างแล้ว แต่จากสถิติ ที่ยังพบอย่างต่อเนื่อง ทำให้เชื่อได้ว่า มันยังไม่ตายไปจากโลกไอที แต่เป้าหมายตอนนี้ น่าจะเป็น คอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบปฏิบัติการเข้าไปใหม่ และยังไม่มีการอัพเดทแพทซ์ตามที่ได้แจ้งไว้ก่อนหน้านี้ ทำให้เครื่องเหล่านั้นกลายเป็นแหล่งกบดานอย่างดี และหากมีจำนวนเครื่องที่ติด conficker มากพอแล้ว แน่นอน ว่า ระบบเครือข่ายโดยรวม ก็คงจะรับมือไม่ไหว มันช่างเหมือนกับไวรัสของคนเรามาก ถ้าคนเราไม่ป้องกันตนเอง ก็จะแพร่เชื้อสู่คนอื่น หรือ หากไม่ใส่ใจในสุขภาพ (ของเครื่อง) ไวรัสก็จะมาเคาะหน้าบ้านได้อยู่เสมอ

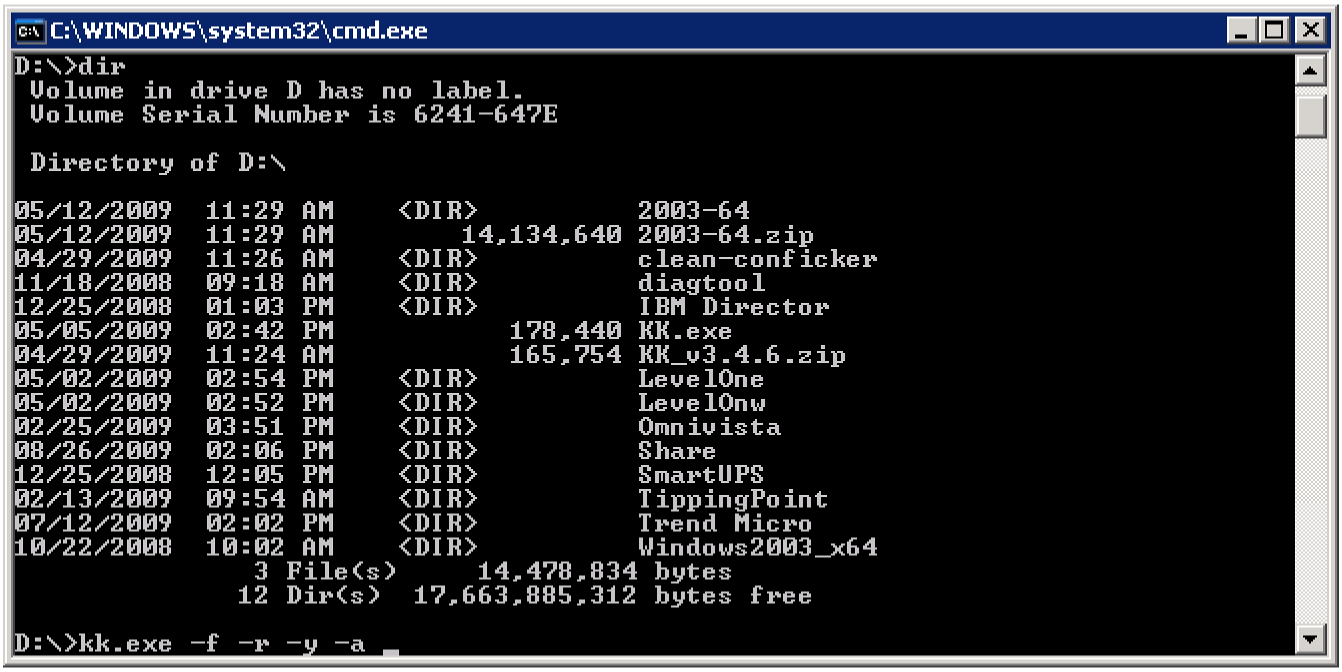
วันนี้ ผมขอแนะนำตัวจัดการกับ Conficker แบบเด็ดขาด (ผมคิดว่างั้นนะ)มาฝากครับ

จากก่อนหน้านี้เคยแนะนะ ฆ่าล้างเผ่าพันธุ์ Conficker และ แจ้งเตือนการระบาดของไวรัส Kido , Conficker

ซึ่งบ่อยครั้งที่เจ้าตัว conficker ไม่ได้หลบอยู่ที่ system32 จึงทำให้การค้นหาไม่พบ ดังนั้น จึงต้องเพิ่มออปชั่นพิเศษสำหรับ kk.exe (ดาวน์โหลดเวอร์ชั่นใหม่จากเว็บไซต์ผู้ผลิตที่นี่ครับ) ไปแบบนี้ครับ

โดยทำการรันจาก คอมมานด์ไลน์ ดังนี้

```
kk.exe -f -r -y -a
```



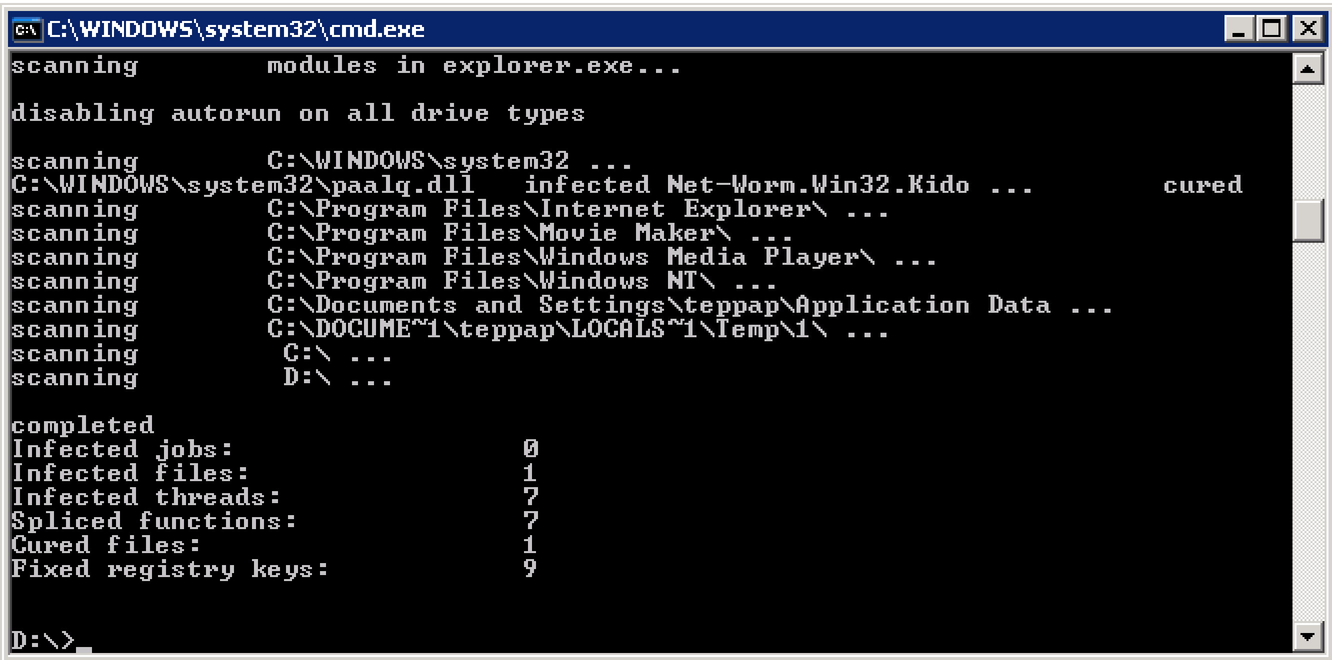
```
D:\>dir
 Volume in drive D has no label.
 Volume Serial Number is 6241-647E

 Directory of D:\

05/12/2009  11:29 AM    <DIR>          2003-64
05/12/2009  11:29 AM        14,134,640 2003-64.zip
04/29/2009  11:26 AM    <DIR>          clean-conficker
11/18/2008  09:18 AM    <DIR>          diagtool
12/25/2008  01:03 PM    <DIR>          IBM Director
05/05/2009  02:42 PM           178,440 KK.exe
04/29/2009  11:24 AM           165,754 KK_v3.4.6.zip
05/02/2009  02:54 PM    <DIR>          LevelOne
05/02/2009  02:52 PM    <DIR>          LevelOnw
02/25/2009  03:51 PM    <DIR>          Omnivista
08/26/2009  02:06 PM    <DIR>          Share
12/25/2008  12:05 PM    <DIR>          SmartUPS
02/13/2009  09:54 AM    <DIR>          TippingPoint
07/12/2009  02:02 PM    <DIR>          Trend Micro
10/22/2008  10:02 AM    <DIR>          Windows2003_x64
               3 File(s)     14,478,834 bytes
              12 Dir(s)  17,663,885,312 bytes free

D:\>kk.exe -f -r -y -a _
```

ซึ่งระยะเวลาการตรวจสอบจะประมาณ 15-30 นาที แล้วแต่ความไวของเครื่อง



```
scanning        modules in explorer.exe...

disabling autorun on all drive types

scanning        C:\WINDOWS\system32 ...
C:\WINDOWS\system32\paalq.dll   infected Net-Worm.Win32.Kido ...        cured
scanning        C:\Program Files\Internet Explorer\ ...
scanning        C:\Program Files\Movie Maker\ ...
scanning        C:\Program Files\Windows Media Player\ ...
scanning        C:\Program Files\Windows NT\ ...
scanning        C:\Documents and Settings\teppap\Application Data ...
scanning        C:\DOCUME~1\teppap\LOCALS~1\Temp\1\ ...
scanning         C:\ ...
scanning         D:\ ...

completed
Infected jobs:                  0
Infected files:                 1
Infected threads:               7
Spliced functions:              7
Cured files:                    1
Fixed registry keys:            9


D:\>_
```

ซึ่งรายละเอียดของค่าตัวแปรต่าง ๆ มีดังนี้ครับ

Switches to run the utility KK.exe from the command prompt:

Switch	Description
-p <scan path>	scan a defined folder
-f	scan hard disks, scan portable hard disks

-n	scan network disks
-r	scan removable drives
-y	end program without pressing any key
–s	silent mode (without a black window)
-l <file name>	write info into a log
-v	extended log maintenance (the switch **-v** works only if the **-l** switch is entered in the command prompt)
–z	restore the services • Background Intelligent Transfer Service (BITS), • Windows Automatic Update Service (wuauserv), • Error Reporting Service (ERSvc/WerSvc
-x	restore display of hidden system files
–a	disable auto start from all drives
–m	mode to monitor threads, tasks, services. When in this mode, the utility constantly resides in memory and will periodically perform scans of threads, services, and scheduler tasks. If an infection is detected, it will perform disinfection and continue monitoring.
-j	restore the registry branch SafeBoot (if the registry branch is deleted, computer cannot boot in safe mode)
-help	show additional information about the utility

ขอให้แน่ใจได้เลยว่า หากเครื่องคอมพิวเตอร์ติด conficker แล้ว แสดงว่าเครื่องนั้น ไม่ได้ทำการอุดช่องโหว่ตามที่ได้แจ้งก่อนหน้านี้ ดังนั้น ให้ทำการดาวน์โหลดจาก บทความ แจ้งเตือนการระบาดของไวรัส Kido , Conficker ได้ครับ (หรือจะเอาจากเว็บไซต์

[illegible])