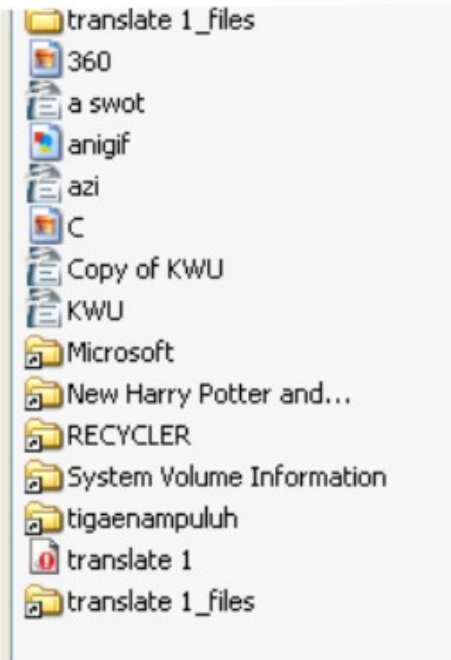


Mengatasi Virus Shorcut



translate 1_files	File Folder	12/31/2008 4:38 AM	
360	61 KB JPEG Image	12/27/2008 9:28 AM	12/
a swot	16 KB OpenDocument Text	12/30/2008 7:56 PM	
anigif	1,161 KB GIF Image	12/25/2008 10:23 AM	
azi	32 KB OpenDocument Text	12/26/2008 1:54 PM	
C	379 KB JPEG Image	12/25/2008 10:04 AM	5/1
Copy of KWU	15 KB OpenDocument Text	12/26/2008 4:12 PM	
KWU	15 KB OpenDocument Text	12/26/2008 4:12 PM	
Microsoft	1 KB Shortcut	12/31/2008 4:38 AM	
New Harry Potter and...	1 KB Shortcut	12/31/2008 4:38 AM	
RECYCLER	1 KB Shortcut	12/31/2008 4:38 AM	
System Volume Information	1 KB Shortcut	12/31/2008 4:38 AM	
tigaenampuluh	1 KB Shortcut	12/31/2008 4:38 AM	
translate 1	2 KB Opera	12/30/2008 8:17 PM	
translate 1_files	1 KB Shortcut	12/31/2008 4:38 AM	

Itu adalah varian baru dari VBScript..

Ciri - Ciri :

Membuat file induk database.mdb di My Documents

Membuat file autorun.inf di setiap drive, flash disk, dan folder

Membuat file Thumb.db (hati2 tanpa huruf s) di setiap folder

Membuat file Microsoft.Ink dan New Harry Potter and....Ink di setiap folder

Membuat duplikat setiap folder dengan ekstensi .Ink

Pada task manager terdapat services wscript.exe

Langkah - Langkah :

Matikan System Restore.. >> MY Computer >> klik kanan pilih Properties >> pilih tab System Restore

>> aktifkan (centang) Turn Of System Restore on All Drive

Matikan proses virus wscript.exe (C:\WINDOWS\System32\wscript.exe), bisa menggunakan Process Explorer atau misc. tool pada HijackThis..

Hapus file virus database.mdb di My Documents..

Hapus file duplikat virus..

Gunakan fasilitas search pada Windows..

Pada "More advanced options", pastikan option "Search system folders" dan "Search hidden files and folders" keduanya terpilih..

Search file dengan nama autorun.inf ukurannya 8 KB

Search file dengan nama Thumb.db ukurannya 8 KB

Search file dengan ekstensi .lnk.lnk ukurannya 1 KB

Hapus semua file yang ditemukan..

Hapus registry Autorun yang dibuat virus dengan menggunakan HijackThis (program Hijack This bisa anda ambil di folder Tools)

>> Do A System Scan Only >> pilih Scan >> Cari di bagian HKCU\..\Run: yang berhubungan dengan file database.mdb >> klik Fix Checked