

6 Langkah Membersihkan Virus 'JeNGKol'

Kontribusi Dari detikinet.com
 Saturday, 06 December 2008
 Pemutakhiran Terakhir Saturday, 06 December 2008

Salah satu ciri komputer terinfeksi virus JeNGKol adalah komputer akan logoff jika user menjalankan file .INF dan saat user mengedit file VBS.

Virus ini akan menyembunyikan file berekstensi .DOC, dengan cara membuat file duplikat sesuai dengan nama file yang disembunyikan untuk mengelabui user. Bagaimana cara membersihkan virus ini? Ikuti langkah berikut ini:

1. Putuskan komputer yang akan dibersihkan dari jaringan (LAN).
2. Nonaktifkan "System Restore" selama proses pembersihan (Windows XP).
3. Matikan proses virus. Untuk mematikan proses virus ini dapat menggunakan tools pengganti task manager seperti "Process explorer". Silahkan download tools tersebut di: <http://download.sysinternals.com/Files/ProcessExplorer.zip>.
4. Hapus registri yang dibuat oleh virus. Untuk mempermudah proses penghapusan silahkan salin script di bawah ini pada program notepad kemudian simpan dengan nama repair.vbs, kemudiai Jalankan file tersebut (klik 2x).

```
Dim oWSH: Set oWSH = CreateObject("WScript.Shell")
on error resume Next
oWSH.Regwrite "HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command", """"%1"" %*"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command", """"%1"" %*"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command", """"%1"" %*"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\Software\CLASSES\pifffile\shell\open\command", """"%1"" %*"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\AlternateShell", "cmd.exe"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Control\SafeBoot\AlternateShell", "cmd.exe"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell", "cmd.exe"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Shell", "Explorer.exe"
oWSH.Regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Edit\Command", "C:\Windows\System32\notepad.exe
%1"
oWSH.Regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\DefaultIcon", "C:\Windows\System32\WScript.exe,2"
oWSH.Regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Classes\inffile\shell\Install\command", "C:\windows\System32\rundll32.exe
setupapi,InstallHinfSection DefaultInstall 132 %1"
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFind")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFolderOpt
ions")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFileAssoci
ate")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegist
riTools")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTask
Mgr")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCMD"
)
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRege
dit")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\RunLogonScr
iptSync")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\HideLegacyL
ogonScripts")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\HideLogoffSc
ripts")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\HideStartupSc
ripts")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\RunStartupSc
```

```

riptSync")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\run\JeNGKoL")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\NeverShowExt")
oWSH.Regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile","VBScript Script File"
oWSH.Regwrite "HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\FriendlyTypeName","VBScript Script File"
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegis
triTools")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTask
Mgr")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRege
dit")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\RunLogonSc
riptSync")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFolderOp
tions")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NOFind")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NORun")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveAut
oRun")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\WinOldApp")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\Msconfig.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\regedit.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\cmd.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\taskmgr.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\cmd.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\regedit32.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\rstrui.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\attrib.exe")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\command.com")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\install.exe\debugger")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\setup.exe\debugger")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\explorer\DisallowRun
")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\explorer\Run")
oWSH.RegDelete("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\ActiveDesktop")
oWSH.RegDelete("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run")

```

5. Hapus file duplikat yang dibuat oleh virus dengan ciri-ciri:

- Menggunakan icon JPEG atau VBS
- Ukuran 14 KB
- Type file JPEG Image atau VbScript Script File

Untuk mempermudah proses pencarian virus, silahkan gunakan fungsi Search windows.

6. Untuk pembersihan optimal dan mencegah infeksi ulang, lindungi komputer Anda dengan anti virus yang sudah dapat mendeteksi dan membasmi virus ini.

sumber : detikinet