CÁCH GỠ BỎ THỦ CÔNG SYMANTEC ANTIVIRUS AN TOÀN

Symant

Symantec Antivirus hay Norton Antivirus là chương trình chống virus được sử dụng rất phổ biến. Tuy nhiên, khi người dùng gỡ bỏ (Uninstall) thì thường hệ thống sẽ bị lỗi và đôi khi dẫn đến việc cài đặt lại toàn bộ hệ điều hành.

Đối với các phiên bản khác nhau thì ta cũng có cách gỡ bỏ khác nhau. Do đó, bạn cần kiểm tra kỹ phiên bản mình đang sử dụng là phiên bản mấy bằng cách vào phần About và xem số phiên bản (version). Bài viết sẽ hướng dẫn bạn cách gỡ bỏ các phiên bản mới.

Symantec AntiVirus 10.1 Client

Phiên bản này dành cho các máy trạm, thường được dùng trên các hệ thống sử dụng phiên bản hệ điều hành 2000/XP/2003. Cách gỡ bỏ bao gồm 5 bước:

Khóa Tamper Protection: bạn cần phải khóa Tamper Protection trước khi khóa các dịch vụ của Symantec AntiVirus.

- Mở Symantec AntiVirus, ở phần menu cấu hình (Configure), chọn Tamper Protection.

- Bỏ chọn “Enable Tamper Protection” rồi nhấn OK.

Khóa các chương trình của Symantec AntiVirus: Những chương trình đang được thực thi cần được khóa là: ccApp.exe, Vpc32.exe, Vptray.exe. Để tắt các “process” này, bạn chọn Start - Run, trong hộp thoại gõ “taskmgr.exe” và Enter hoặc phải chuột lên khay hệ thống và chọn “Task Manager”. Trong cửa sổ “Windows Task Manager”, chọn thẻ “Processes” rồi lần lượt chọn ccApp.exe, phải chuột “End Process”, tiếp tục với 2 process còn lại.

Khóa các dịch vụ Symantec AntiVirus: Ta cần ngưng hoạt động các dịch vụ của Symantec AntiVirus trước khi tiến hành xóa giá trị registry. Nhấn chọn Start - Run, gõ "services.msc" trong hộp thoại Run rồi OK. Tìm và chọn các dịch vụ sau rồi phải chuột lên chúng, chọn "Stop" để ngưng hoạt động: SAVRoam, Symantec AntiVirus, Symantec AntiVirus Definition Watcher, Symantec Event Manager, Symantec Settings Manager.
Đối với phiên bản Symantec AntiVirus 10.2 Client thì 2 bước trên sẽ được thu ngắn lại như sau:

Khóa các dịch vụ của Symantec AntiVirus trong Services

- Không có process: Vpc32.exe

- Phần dịch vụ, sẽ bao gồm: SavRoam, Symantec AntiVirus, DefWatch, ccEvtMgr, ccSetMgr.

Gỡ bỏ khóa Registry: Đây là thao tác quan trọng và phức tạp nhất. Tốt nhất, bạn cần sao lưu lại toàn bộ registry trước khi thực hiện các bước dưới đây.
Chọn Start - Run, gõ "regedit" rồi OK. Trong cửa sổ Registry Editor, tìm đến khóa HKEY_CLASSES_ROOT*\Shellex\ContextMenuHandlers, ở khung bên trái, phải chuột chọn LDVPMenu và chọn Delete.

Tìm đến khóa HKEY_CLASSES_ROOT\Installer\Features. Tại đây, có rất nhiều khóa là các ký tự số dạng 32F36B64A4B252548A72860862EBE504. Click chọn lên từng khóa và đồng thời nhìn ở khung bên phải. Khóa nào có "SAVMain" thì xóa toàn bộ khóa đó.

Mở tiếp đến HKEY_CLASSES_ROOT\Installer\Products, và ta lại bắt gặp nhiều khóa mang ký tự số chữ hỗn hợp như ở "Features". Cũng thực hiện thao tác dò tìm từng khóa và nhìn bên khung phải xem giá trị nào có dạng "ProductName - Symantec AntiVirus" thì xóa cả khóa (bên trái) đó đi.

Mở rộng khóa HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products, khóa này cũng bao gồm các khóa ký tự số. Tại khung trái, mở rộng từng khóa bằng cách nhấn vào dấu (+) trước tên khóa, chọn khóa InstallProperties. Nếu bên phải có phần "DisplayName - Symantec AntiVirus" thì xóa toàn bộ khóa đó đi.

Mở rộng khóa HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall, thực hiện tìm từng khóa và lưu ý bên khung phải có Symantec AntiVirus thì xóa toàn bộ khóa đó đi.

Xóa các khóa sau:

HKEY_CLASSES_ROOT\Installer\UpgradeCodes\20A7FB42A06BB49448A397B3CB77ED4D
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\UpgradeCodes\20A7FB42A06BB49448A397B3CB77ED4D
HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\DllUsage\VP6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UpgradeCodes\20A7FB42A06BB49448A397B3CB77ED4D
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SPBBC
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec AntiVirus
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\SymNetDrv
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System\SAVRT

Mở rộng khóa HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features, tìm trong các khóa và lưu ý khung bên phải, khóa nào có "SAVMain" thì xóa toàn bộ khóa đó. Tiếp theo, tìm khóa HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products và cũng giống như trên, tìm đến khóa nào mà bên khung phải có Symantec AntiVirus thì xóa toàn bộ khóa đó.

Tìm khóa HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, trong khung bên phải, xóa giá trị vptray. Tiếp tục với khóa HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\InstalledApps, ở khung phải, xóa các giá trị sau: AVENGEDEFS, Common Client, Common Client Data, Common Client Decomposers, NAVNT, SAV Install Directory, SAVCE, Savrt, SPBBC, SymNetDrv, VP6ClientInstalled, VP6UsageCount.

Tìm khóa HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services, xóa các khóa phụ sau: ccEvtMgr, ccSetMgr, DefWatch, NAVENG, NAVEX15, SavRoam, SAVRT, SAVRTPEL, SNDSrvc, SPBBCDrv, SPBBCSvc, Symantec AntiVirus, SYMREDRV, SYMTDI.

Tìm khóa HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application, xóa các khóa phụ sau: ccEvtMgr, ccSetMgr, DefWatch, LiveUpdate, SavRoam, Symantec AntiVirus.

Gõ từ khóa cần tìm để có thể kiếm chính xác và nhanh chóng hơn trong Registry Editor

Bên khung trái của Registry Editor, bạn tìm đến phần trên cùng là My Computer, trên thanh menu Edit, chọn Find, bạn gõ "VirusProtect6", xóa tất cả các khóa chứa chuỗi này. Tiếp tục thao tác trên với từ khóa tìm là "933187C5788574F4889B3B1FBB35638A".

Tiếp theo thao tác xử lý trong Registry trên, ta tiến hành các bước còn lại để gỡ bỏ Symantec AntiVirus 10.1 Client. Tuy nhiên, 2 bước bên dưới đây có thể sẽ làm ảnh hưởng đến các chương trình khác của Symantec cùng được cài đặt trên hệ thống. Do đó, bạn phải kiểm tra lại xem có ứng dụng nào khác của Symantec ngoài AntiVirus 10.1 Client hay không.

1. Mở Registry Editor, xóa các khóa:

- HKEY_LOCAL_MACHINE\Software\Symantec\SharedDefs
- HKEY_LOCAL_MACHINE\Software\Symantec\Common Client
- HKEY_LOCAL_MACHINE\Software\Symantec\SymEvent
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SymEvent

2. Tìm đến khóa HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, trong khung bên phải, xóa giá trị ccApp. Khởi động lại máy tính.

Symantec AntiVirus đã được khóa hoàn toàn các giá trị, dịch vụ lẫn chương trình. Bước tiếp theo sẽ là xóa bỏ trong menu Start và trên ổ cứng. Phải chuột lên Start trên thanh tác vụ, chọn "Explorer All Users". Cửa sổ Windows Explorer sẽ xuất hiện, đường dẫn sẽ là C:\Documents and Settings\All Users\Start Menu\Programs (C là partition cài đặt hệ điều hành). Chọn Programs - Symantec Client Security. Nếu đang dùng nhiều ứng dụng của Symantec thì bạn chỉ xóa Symantec AntiVirus. Nếu chỉ có Symantec AntiVirus trong thư mục này thì bạn xóa Symantec Client Security.

Thao tác tiếp theo sẽ là xóa các tập tin trên ổ cứng bằng cách nhấn phím Windows + E hoặc Start - Programs - Accessories - Windows Explorer để mở Windows Explorer. Mở partition cài đặt hệ điều hành, ở đây là ổ C:\Program Files\Symantec, xóa thư mục này. Tiếp tục tìm thư mục Program Files\Common Files\Symantec Shared, nếu Symantec AntiVirus là ứng dụng Symantec duy nhất trên hệ thống thì xóa các thư mục sau: Decomposers, SPBBC, SPManifests, SSC, VirusDefs.

Cuối cùng, tìm đến thư mục C:\Documents and Settings\All Users\Application Data\Symantec và xóa 2 thư mục con là Common Client và Symantec AntiVirus Corporate Edition. Ta hoàn tất quá trình gỡ bỏ thủ công cho Symantec AntiVirus 10.1 Client hay Symantec Client Security 3.1.

Các hệ thống cài đặt Symantec AntiVirus 10.2 Client hay Symantec AntiVirus 10.1 và Symantec Client Security 3.1 server có thể tham khảo tại đây.

Norton Removal Tool 2007.2.02.14
Đối với các máy đã gỡ bỏ các phiên bản Norton 2003/2004/2005/2006/2007 mà bị lỗi hệ

thống, gỡ bỏ không hoàn tất, có thể dùng tiện ích miễn phí của Symantec là Norton Removal Tool tùy theo phiên bản hệ điều hành là Me/98 hay 2000/XP/Vista mà tải về tại đây. Sau khi tải về, thực thi, tiện ích sẽ tự dò tìm các chương trình thuộc Symantec trên máy và đưa ra giải pháp, bạn sẽ làm theo các bước mà tiện ích yêu cầu cũng như sẽ phải khởi động lại hệ thống nhiều lần theo từng bước tiến hành.

Thanh Trực