VPScan.exe

Usage:

```
   VPSCAN [X Options] [ScanTarget]


[Scan Options]
   /UI              UI mode, all other options ignored.
   /INI             Use scan options from the INI file.
                    INI options can apply only to /USER and /ADMIN scans.

   These options apply to /USER and /ADMIN scan types. You can combine these
   options.

   /GREYWARE        Enable scanning for greyware on machine. For SAV Version
                    9.x and above.
   /PROCESSES       Enable scanning for infected process loaded in memory on
                    machine. For SAV Version 9.x and above.
   /SECURITYRISKS   Enable scanning for security risks on machine. For SAV
                    Version 10.x and above.
   /LOADPOINTS      Enable scanning for generic load points on machine. For SAV
                    Version 10.x and above.
   /KILLSERVICE     Enable automatic termination of infected services. For SAV
                    Version 10.x and above.
   /KILLPROCESS     Enable automatic termination of infected processes. For SAV
                    Version 10.x and above.
   /SHOWSCAN        Shows scan progress dialog.

ScanType:
   /USER            Run a client user's scan (default, no need to specify)
   /ADMIN           Run an admin scan
   /SWEEP           Run virus sweep, requires a location of a GRC.DAT


[ScanTarget]
   For /USER or /ADMIN scans, specify a directory path or filename to scan.
   For /SWEEP scans, specify the GRC.DAT to use, as C:\TEMP\GRC1.DAT


Do not use the options below with the options above.

[INI Option]
   /CREATEINI       To Create a simple INI from the current user settings.
                    INI file is placed in the same directory as VPSCAN.EXE.
   /ALLOPTIONS      Use with /CREATEINI, Adds options that are available for
                    users in the UI.
```

Samples:

To create a sample INI file to modify and use for scans run the following command at the command prompt:

- **vpscan.exe /createini**

To run a user scan (on a machine with SAV 9.x or above on it) that will scan for greyware and in-memory infections, run the following command at the command prompt:

- **vpscan.exe /user /greyware /processes "c:\program files"**

To run a sweep scan, run the following command at the command prompt:

- **vpscan.exe /sweep c:\temp\grc.dat**

To run a user scan (on a machine with SAV 10.x or above on it) that will scan for in-memory infections, generic load points, security risks, and have the action of terminating infected processes, run the following command:

- **vpscan.exe /user /processes /securityrisks /loadpoints /killprocess c:**

Notes:

- The /KILLPROCESS and /KILLSERVICE options can be impact the user who is currently working on the machine being scanned. Use these options with care as they will not prompt the user before terminating the process or service. For example, if the infected process is Internet Explorer and the user has it currently open, then the process will be terminated without any way for the user to stop it.

- You can use 10.x options on previous versions of Symantec AntiVirus. The previous version will just ignore the options that it does not understand. This allows you to have a batch file or VBScript that can be run on any version of Symantec AntiVirus and you only have to maintain that one file instead of one file per Symantec AntiVirus version.