One quick trick prevents AutoRun attacks

Scott Dunn By Scott Dunn

The AutoRun function in Windows can launch installers and other programs automatically when you insert a CD or flash drive, but this convenience poses a serious security risk.

Unfortunately, simply turning off AutoPlay, a separate feature, isn't enough to prevent AutoRun from introducing a rogue program into your system.

The real solution is to globally block autorun.inf files from executing (see procedure in next page)

AutoRun starts Windows programs automatically

Every recent version of Windows has features known as AutoPlay and AutoRun. These functions are designed to launch applications automatically from a external device containing the necessary AutoRun information. This is what causes an installer window to pop up when you insert a software disc into your CD or DVD drive, for example, or makes a pop-up menu icon appear in the taskbar tray when you insert a USB flash drive. (In some cases, the action doesn't occur until you double-click the flash drive icon in Windows Explorer.)

When a disc is inserted or a drive is connected to your system, **Windows looks in the root directory** of the new disc or drive for a file named **autorun.inf**. If found, Windows executes the instructions in that file.

For example, an autorun.inf file on a CD might contain a line that reads open=setup.exe. This tells your computer to launch a setup program as soon as the CD is inserted into the drive.

However convenient this might be, unfortunately, **AutoRun also opens a huge door for viruses, Trojan horses, and worms**. All it takes is a USB flash drive with an autorun.inf file and an executable in its root. **Once inserted, a worm launched in this manner can infect every disk partition it finds, jumping from computer to computer as network users connect to an infected drive**.

Shutting down AutoPlay is not a fix

In both Windows XP and Vista, the default for USB flash drives is to prompt the user for a decision if autorun.inf tries to launch a program. Inserting a CD or DVD into a drive, however, defaults to running any autorun.inf file that may be present.

In XP, you can change the defaults for AutoPlay on a given drive by right-clicking the drive in Windows Explorer and choosing Properties. Click the AutoPlay tab and use the controls there to change the settings for different types of media. Making changes in this dialog box, however, has no effect in preventing autorun.inf from being executed.

In Vista, end users can choose one of several options, even for software programs that use autorun.inf: (1) always launch the program, (2) always open a listing of the disc in a Windows Explorer window, (3) always prompt for a choice, or (4) take no action.

Unfortunately, none of the above steps can safeguard you against a malicious autorun.inf on removable media. I'm no hacker, but I was able in just a few minutes to make an AutoRun file that would run, even with AutoPlay disabled in XP and "take no action" selected in Vista.

The exploit involves creating an autorun.inf file that adds a new default command to a USB flash drive's context menu. If you have "take no action" selected in Vista, the flash drive doesn't automatically launch any programs when first inserted. But double-clicking the flash drive icon in My Computer, for example, is all it takes to launch whatever commands are in autorun.inf (which the attacker has made the default command, in place of Open). The steps are documented at Daily Cup of Tech.

A clever hacker could make a worm that (1) spreads itself to all your drives when launched in this manner and then (2) displays the drive contents in a window, as expected. This would make it appear that nothing unusual had happened.

Block AutoRun for all devices all the time

You might think that you could proect yourself from AutoRun by using two keys in the Registry known as NoDriveAutoRun and NoDriveTypeAutoRun.

However, self-described "low-budget hacker" Nick Brown points out that these keys can be overridden because of a **Registry key named MountPoints2 that stores information about all USB flash drives and other removable media that have ever been connected to your computer. Brown says this cache overrides the Registry settings that turn off AutoRun**.

The solution is to globally block autorun.inf files from executing, without trying to use the dialog boxes in XP and Vista to do this.

Here's the procedure: How to **Block AutoRun for all devices all the time**

Step 1. Start Notepad or another text editor.

Step 2. Copy the following text from this page and paste it into your text editor (everything between the square brackets should be all on one line):

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

Step 3. Save the file on the desktop with a name like **`NoAutoRun.reg`**, taking care to include the .reg extension.

Step 4. Right-click **`NoAutoRun.reg`** file and choose ***Merge o Unisci***. Confirm any warning prompts to add the information to the Registry.

Step 5. Reboot the system

The next time you insert a flash drive, CD, DVD, or other removable disc into your system, Windows will not execute the information in any autorun.inf file that may be present.

Naturally, taking these steps means that the next time you put a game or installer disc into your CD or DVD drive, its software won't launch automatically. You'll have to open a Windows Explorer window or use a command line to launch the desired executable.

The benefit is a big one: a rogue program that you never intended to launch won't silently take over your system if you happen to insert a Trojan-carrying disc into a drive.

Note added by Robert @ FAsTec http://fastec.eu http://hc.no-ip.biz/wordpress

If you want restore the Autorun.inf execution, create a file with the above procedure but change the content in the Step 2 with the following one and save the file as **`RestoreAutoRun.reg`**

```
REGEDIT4
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

The only difference is the '**-**' symbol before the **`HKEY_LOCAL_MACHINE`** . This will remove the modification added with the **`NoAutoRun.reg`** file.