ScripTrap
Script File Trapper

Scripts are small programs that are written in a variety of simple computer languages. They can perform useful functions but they can also be used for less useful and sometimes damaging purposes, the prime examples being computer viruses and trojan-horse programs.

The worst thing about many types of scripts is that they can operate without warning as a legitimate part or extension of another program. Most damaging of all are email attachments that contain scripts. If you open them in an email program that allows scripting they may execute before you even realize what you have done.

ScripTrap traps scripts when they attempt to run on your computer and provides the option of blocking them or letting them continue to run. You can also check the intercepted script with your anti-virus program before you decide to run it or not. This provides you with a chance of catching possibly malicious code before it causes damage. *ScripTrap* is particularly useful for trapping scripts that arrive in email attachments.

As always, having a good anti-virus program installed on your computer is highly recommended. Even if you do not have one installed there are several free anti-virus applications that can run from over the Web. Try http://www.antivirus.com/pc-cillin/.

This is the list of file types that *ScripTrap* intercepts:

.DOC	Microsoft Word© Document
.HTA	HTML Applications
.INS	Internet Communication Settings
.ISP	Internet Communication Settings
.JS	Script® File
.JSE	JScript Encoded Script File
.REG	Registration Entries
.SHS	Shell Scrap Object
.VB	VBScript File
.VBE	VBScript Encoded Script File
.VBS	VBScript Script File
.WSF	Windows Script File
.WSH	Windows Scripting Host Settings File
.XLS	Microsoft Excel© document

Although *Microsoft Word* and *Microsoft Excel* documents are not scripts as such, they can contain macros, short script-like programs that are potentially just as dangerous as standalone scripts and so I chose to include ***.doc*** and ***.xls*** files in the list.

I have intentionally not included the ability to add extra file types. Programs can execute using many different techniques and intercepting the execution of certain poorly chosen file types can cause unexpected behavior and problems with the normal operation of the computer. The list above should suffice for practically all of your needs and covers most if not all of the malicious script types encountered.

Starting ScripTrap

This is simple. Just run the program!

When run for the first time, *ScripTrap* will place a convenient shortcut in your **Start menu > Programs** section under the heading **ScripTrap**.

All *ScripTrap* operations are contained in the one executable file, *ScripTrap.exe*. This single file takes care of the installation, interception of scripts, configuration options and uninstalling. There are no extra files involved to clutter up your disk and the program will add and remove all registry entries as needed. You may safely place *ScripTrap* anywhere you like on your hard drive; it will run from any location.

You can access this help information from within *ScripTrap* by clicking the **Help** button.

How to use ScripTrap

The first time you run the program you will see a window with a message on a red background telling you that *ScripTrap* is currently disabled. When the program is in this state no scripts will be intercepted and your system will operate as if *ScripTrap* were not there at all.

Before you enable *ScripTrap* for the first time you should disable or uninstall any similar products (I do not mean virus scanners). Failure to do this may result in incorrect operation of the program!

To enable *ScripTrap*, click the **Enable** button. The display will change to show **Enabled** on a green background. *ScripTrap* is now ready to intercept the running of script files. Click **OK** to close the window.

Note that *ScripTrap* does not need to be running to intercept scripts. Once you have clicked the **Enable** button and closed the window by clicking **OK** you are ready to continue using your computer as normal. You only need run *ScripTrap* again if you want to change the program options that are detailed later on in this document.

When ScripTrap intercepts a script

ScripTrap will bring up a warning window whenever it intercepts a script. The warning window will show the full path name of the script that is attempting to run and ask you if you want to allow it to execute.

You now have three options:

- You can click **Yes** and the script will execute as normal
- You can choose **No** and the script will be blocked. It will not run.
- You can click **Scan first** to have your anti-virus program scan the script and then decide to click **Yes** or **No**.

.

(This last option will only be available if you have configured an anti-virus program. See Configuring ScripTrap below).

. . . . . .

Obviously, if you choose **Yes** to let the script run you should be absolutely certain that it is safe. You should configure an anti-virus program and scan the file first if you have any doubts. You should never run a script (or any program) that came from an uncertain origin and even then it is wise to run a virus check on the file before you let it go about its business.

You may find yourself wanting to always allow a particular script to run or perhaps always prevent one from running. If this is the case you should click in the checkbox where it says ***Add this file name to my list and don't ask me about it again*** so that the checkmark is visible. Then, after you choose **Yes** or **No** you will never again be prompted when that particular script file is run. *ScripTrap* adds the script file name to its internal list together with your choice of whether you are allowing it to run or blocking it. To change items in this list you should choose the **More...** button on the warning window or select the **Program options...** button from the main window.

There is an exception to the rule of when you can add items to your auto accept/reject list. If the script file that has been intercepted is located in a *temporary* directory (usually your *Windows\Temp* directory) you will not be given the chance to add it to your list. This is because scripts in your temporary directory are most likely to have been placed there after having been opened directly from an email attachment. By their nature these script files are likely to be named in some unique obscure manner typical of temporary files but more importantly these scripts opened from email attachments are the most likely files to contain viruses and so you wouldn't want to always accept these files.

Configuring ScripTrap

From the *ScripTrap* main window select the **Program options...** button. You will be presented with the program options window.

The first option you will see is a checkbox asking if you only want to intercept *temporary* scripts. As mentioned above, *temporary* scripts are saved in to a temporary folder on your hard drive (usually *Windows\Temp*) and are most likely to have been placed there after having been opened from an email attachment. For this reason they are obviously more likely to contain viruses. If your primary concern is to trap scripts that you inadvertently run from email attachments this is a good option to activate.

In the middle of the options window it shows the contents of *ScripTrap's* auto accept/reject

list, the list of scripts that you have chosen to allow to run or block without prompting. If there are any items in this list, script files that you chose to allow to run will have a green check mark next to them and scripts you chose to always block will have a red cross next to them. Note that if you have chosen to only intercept *temporary* scripts you cannot change this list.

You can change whether a script runs or is blocked by double-clicking the item in the list.

If you want to remove a script from the list, select it so that it is highlighted then click the **Remove selected item** button.

At the bottom of the options window is where you can specify the location of your anti-virus program, if you have one. If you don't you can leave these entries blank.

In the **Anti-virus program** box enter the full path name to your anti-virus program. You can click the **...** button to browse for the file or simply type the name into the box. Here are the default locations for two of the most common anti-virus applications:

McAfee Virus Scan:
C:\Program Files\Network Associates\McAfee VirusScan\scan.exe

Norton Anti-virus:
C:\Program Files\Norton AntiVirus\navw32.exe

The **Options** box next to the anti-virus location box is where you can enter any additional options for your anti-virus application. Most of the time this can be left blank. Consult the documentation for your anti-virus program if you require further information.

Permanent changes to the configuration of *ScripTrap* won't be made until you click the **OK** button to confirm them or click **Cancel** to abandon your changes.

Uninstalling

To uninstall *ScripTrap* you should either use the uninstall shortcut placed in your **Start menu > Programs** section under **ScripTrap**, or use the **Add/Remove Programs** option in the **Control Panel**. This can be reached by clicking the **Start** button, selecting **Settings** then **Control Panel**. Select **Add/Remove Programs**, find *ScripTrap* in the list then click on **Add/Remove**.

ScripTrap leaves no trace of itself in the registry after uninstalling and there are no other files it uses other than the main executable file *ScripTrap.exe* that will be removed automatically.

Attempting to uninstall ScripTrap by using a method other than those just described will result in your script files being unable to run. You must uninstall ScripTrap this way to ensure all script file interceptions are removed.

Written by Robin Keir, June 2000
http://keir.net/
mailto:robin@keir.net