How to add script analysis to a profile to detect suspicious code and autoruns

Click ‘Configuration Templates’ > ‘Profiles’ > open a Windows profile > Click ‘Add Section’ > ‘Script Analysis’

- Script analysis improves endpoint protection by analyzing the code of a program to detect zero-day and file-less malware.

  Comodo Client Security (CCS) uses the following two methods to analyze code:

  - **Heuristic command line analysis** - Identifies files which have virus-like attributes. This lets CCS detect new, previously unknown malware.

  - **Embedded Code Detection** – Detects non-compiled, file-less code loaded to your system memory. File-less malware allows malicious actors to directly execute commands on your system.

  - See the background infromation at the end of this section if you want to know more about these technologies.

- This article explains how to add a script analysis section to a profile.

Add script analysis to a profile

Configure script analysis

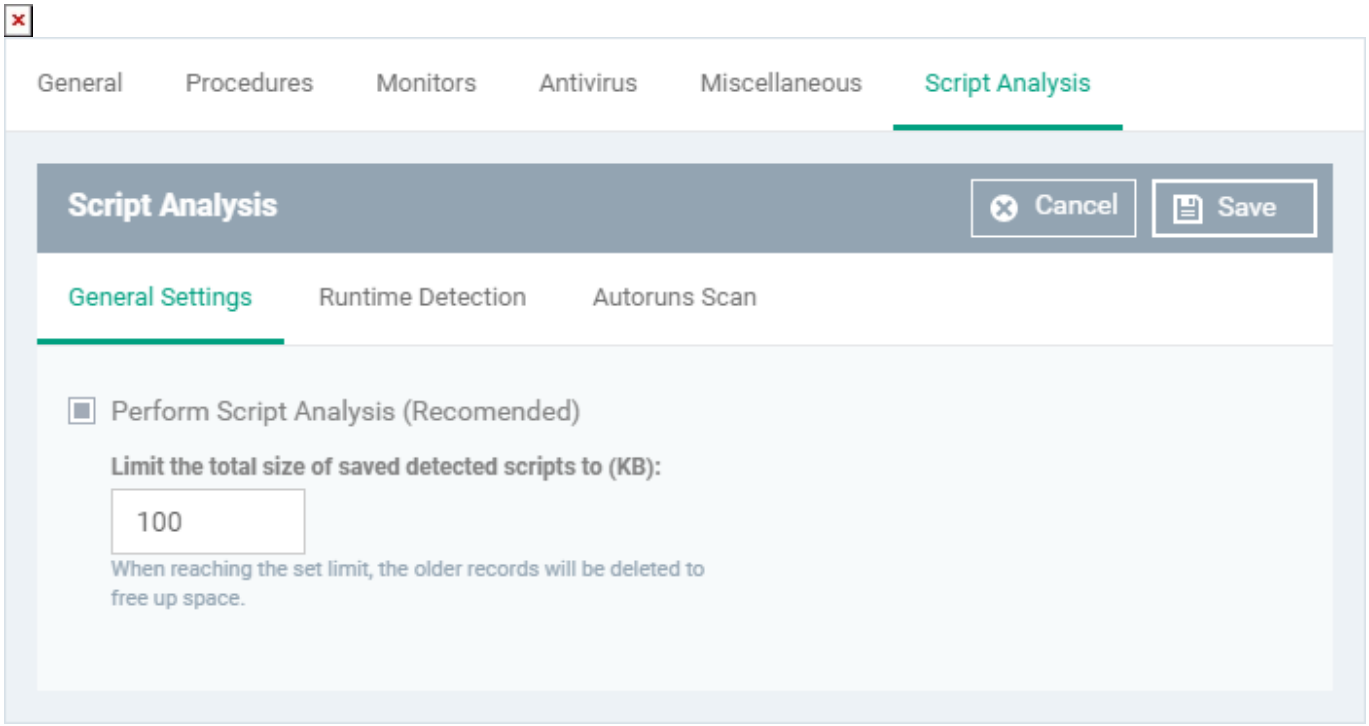
Background information

Add script analysis to a profile

- Login to Comodo One / Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Click the ‘Profiles’ tab
- Open the Windows profile applied to your target devices
  - Open the 'Script Analysis' tab

    OR

  - Click 'Add Profile Section' > 'Script Analysis', if it hasn't yet been added
- Enable script analysis under the 'General Settings' tab
- Click 'Save'



Configure script analysis

The script analysis screen has three tabs:

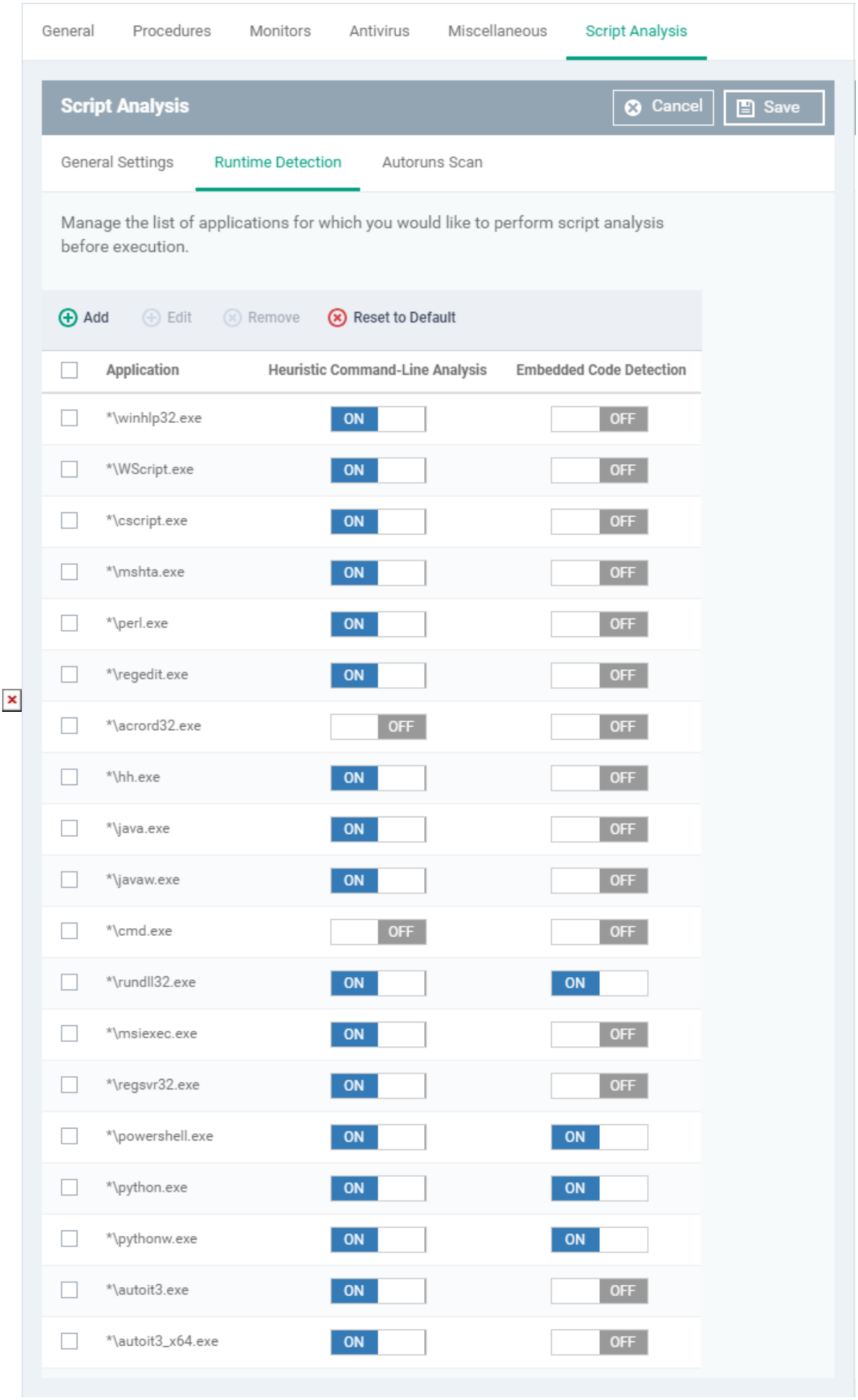
- General Settings - Enable script analysis and set the maximum file size which should be checked.
- Runtime Detection - Select which programs are monitored.
- Autoruns Scan - Choose programs that you want to monitor to see if they make changes to auto-run entries, Windows services and scheduled tasks.

General Settings

- **Perform Script Analysis** - Enable/Disable script analysis. An alert is generated if malicious code is found in any item. (Default = Enabled)
- **Limit the total size of saved detected scripts to** - CCS stores scripts run by managed applications for analysis. This option lets you specify the total size of stored scripts. When the set limit is reached, the older scripts are deleted automatically. (Default = 100 KB)

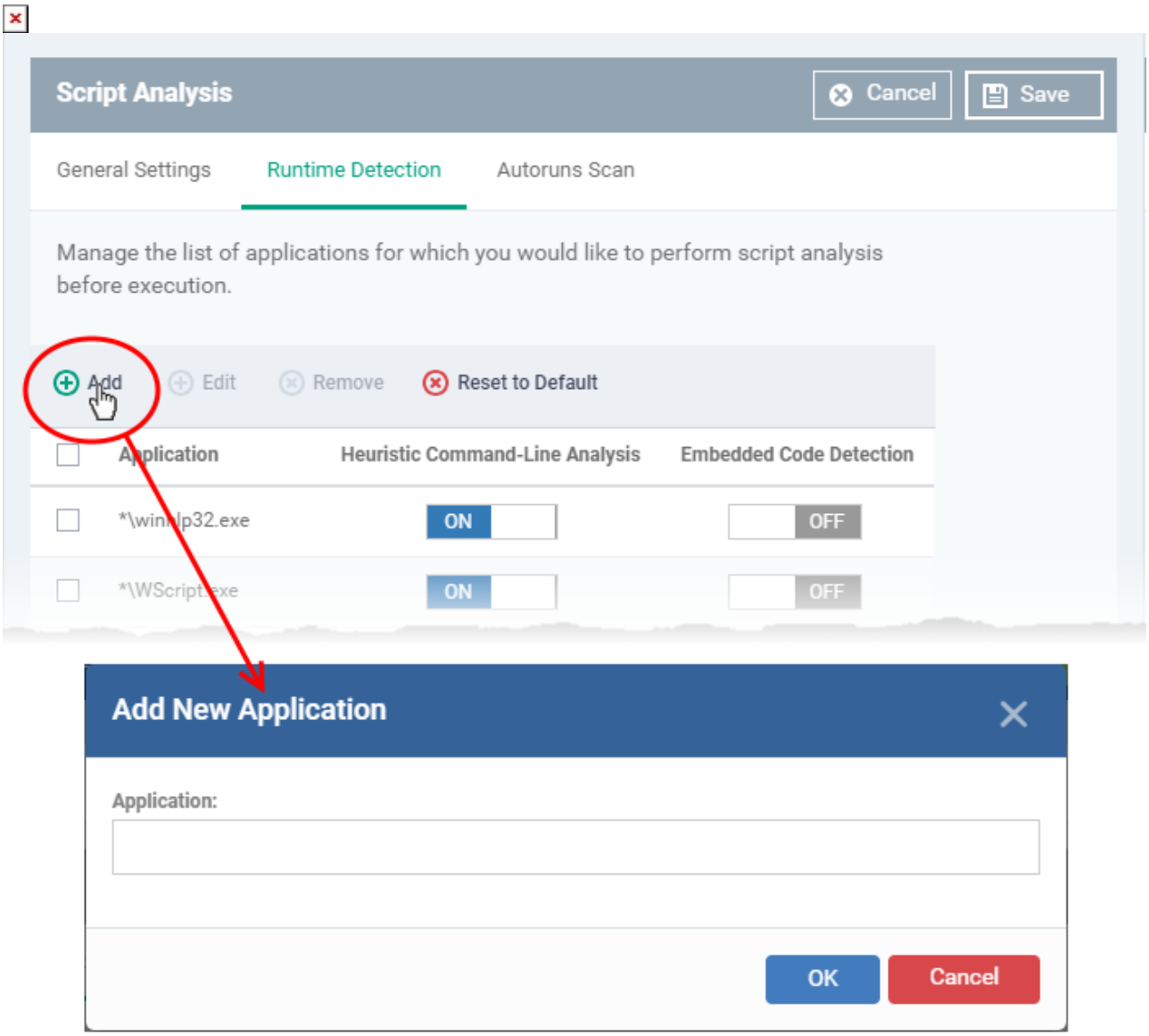
Runtime Detection

- Lets you select executables which should be analyzed throughout their runtime.
- You can also add custom applications that you want to protect.


General
Procedures
Monitors
Antivirus
Miscellaneous
Script Analysis
Script Analysis
Cancel
Save
General Settings
Runtime Detection
Autoruns Scan
Manage the list of applications for which you would like to perform script analysis before execution.
Add
Edit
Remove
Reset to Default
Application
Heuristic Command-Line Analysis
Embedded Code Detection
*\winhlp32.exe ON OFF
*\WScript.exe ON OFF
*\cscript.exe ON OFF
*\mshta.exe ON OFF
*\perl.exe ON OFF
*\regedit.exe ON OFF
*\acrord32.exe OFF OFF
*\hh.exe ON OFF
*\java.exe ON OFF
*\javaw.exe ON OFF
*\cmd.exe OFF OFF
*\rundll32.exe ON ON
*\msiexec.exe ON OFF
*\regsvr32.exe ON OFF
*\powershell.exe ON ON
*\python.exe ON ON
*\pythonw.exe ON ON
*\autoit3.exe ON OFF
*\autoit3_x64.exe ON OFF

- Use the switch in the 'Heuristic Command-Line Analysis' column to enable/disable heuristic command line analysis for each application.
- Use the switch in the 'Embedded Code Detection' column to enable/disable embedded code detection for each application.

- Click 'Add' to include a new application:



- Enter the name of the application in the 'Add Application' dialog and click 'Add'.
- Repeat the process to add more applications

- Click 'OK' to apply your changes.

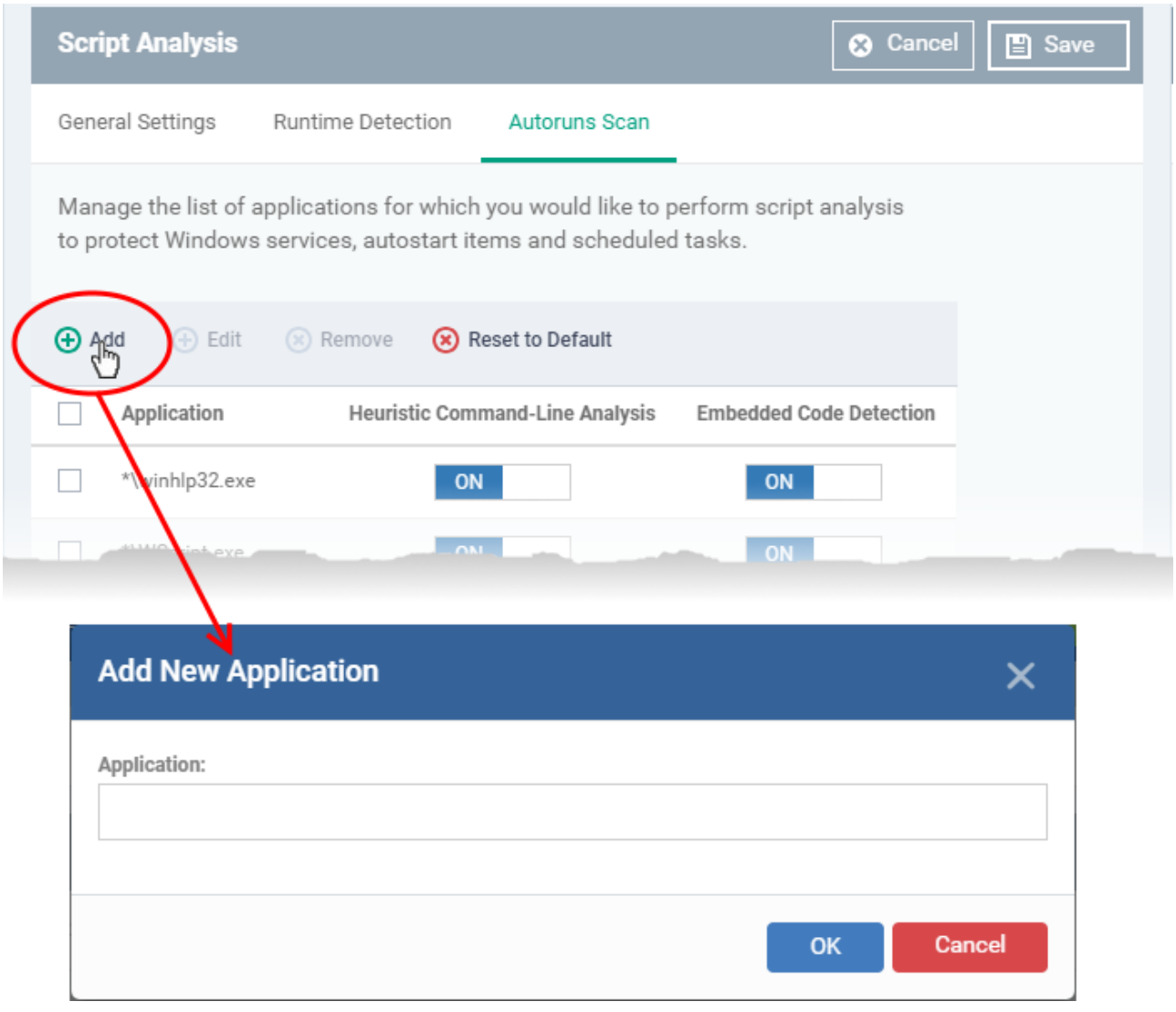
Autoruns Scan

- Select applications which should be monitored in case they make changes to autoruns, Windows services or scheduled tasks.

- You can also add custom applications which you want to monitor.
- Click the 'Autoruns Scan' tab

  - Use the switch in the 'Heuristic Command-Line Analysis' column to enable/disable heuristic command line analysis for each application.
  - Use the switch in the 'Embedded Code Detection' column to enable/disable embedded code detection for each application.

- Click 'Add' to include a new application:



  - Enter the name of the application then click 'Add'.
  - Repeat the process to add more applications

- To reset the list to the default list of applications, click 'Reset to Default' on the top

- Click 'OK' to apply your changes.

Background information

Heuristic command line analysis:

- Heuristic analysis helps identify new malware by inspecting a file’s code to see if it contains code typical of a virus.
- The system detects files which have ‘virus-like’ attributes, instead of looking for a signature that matches a signature on the blacklist.
- This allows the engine to predict new viruses - even if they are not in the current virus database.

Embedded code detection:

There are two types of executable programs:

- **Compiled** - These programs can execute on their own. Examples include .exe and .dll files.
- **Non-compiled** - These are scripts which require an interpreter program to execute them. For example, Powershell scripts (.ps1) are interpreted and executed by the Powershell program.

Embedded code detection protects you against attacks from non-compiled malware (also known as file-less malware).

- File-less malware attacks allow hackers to directly execute powershell commands on your system.
- These commands can be used to take control of endpoints, install ransomware, steal confidential data and more.
- File-less scripts reside in memory, so no trace of them remains after the computer is restarted.
- Example programs affected by these attacks are wscript.exe, cmd.exe, java.exe and javaw.exe.
- For example, the program wscript.exe can be made to execute visual basic scripts (.vbs files) via a command similar to 'wscript.exe c:/tests/test.vbs'. When script analysis is enabled, CCS detects c:/tests/test.vbs from the command-line and applies all security checks to this file.