



# **The Microsoft Office Isolated Conversion Environment (MOICE) and File Block Functionality with Office 2003**

## **Introduction**

Hackers have long been able to exploit vulnerabilities in versions of Microsoft's Office suite by getting users to open files that contain malicious content. This can allow attackers to steal files, log keystrokes, capture screenshots, or even remotely execute commands of their choosing.

Security vendors have recommended a variety of actions that system administrators can take to protect users from these kinds of attacks (limiting users' privileges, blocking certain kinds of outbound traffic, quarantining all attachments, converting all Office files to PDF files, etc.) but many of the proposed countermeasures are not implemented because they are thought to be too difficult, too expensive, or too inconvenient.

Malicious Office files often exploit vulnerabilities that exist in the parsing code used to open and save supported file types. Microsoft has responded to this type of threat by creating more robust parsers and by introducing new file formats in Office 2007. Further, the default file formats in Office 2007 (.docx, .xlsx, .pptx, etc.) are not allowed to contain embedded code or macros<sup>1</sup>.

In May 2007, Microsoft released a free tool that gives customers who cannot immediately upgrade to Office 2007 the ability to sanitize potentially-malicious Office files by converting them to the new Office 2007 file formats.

## **MOICE**

The Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats<sup>2</sup> makes it possible for users of Office 2003, Office XP, and Office 2000 to open, edit, and save their existing documents, workbooks, and presentations in the new Office 2007 file formats. An important part of the conversion from a binary Office file type to an Office 2007 file type is the removal of potentially malicious content.

The Microsoft Office Isolated Conversion Environment (MOICE) provides a framework for ensuring that supported Office 2003 file types are always converted to the corresponding Office 2007 file type<sup>3</sup>. This is accomplished by installing the Compatibility Pack and then changing the application that runs when supported Office 2003 file types are executed. The new application (Oice.exe) oversees the conversion to an Office 2007 file type and the removal of embedded code and macros. To prevent the converter itself from being exploited by malicious code, the conversion takes place inside a separate desktop that is issued a restricted security token.

---

<sup>1</sup> For more information about the new file formats in Office 2007, see "Introducing the Office (2007) Open XML File Formats" at <http://msdn2.microsoft.com/library/aa338205.aspx>. Office 2007 documents can still contain macros as long as the files are saved in a macro-enabled file format (.docm, .xlsm, and .pptm).

<sup>2</sup> For more information about the Compatibility Pack, see <http://support.microsoft.com/kb/924074>.

<sup>3</sup> The Compatibility Pack can be installed on Office 2003, Office XP, and Office 2000 but Microsoft only supports MOICE and File Block functionality on Office 2003 and Office 2007. This document focuses on Office 2003 only. For more information about MOICE, see <http://www.microsoft.com/technet/security/advisory/937696.msp>.

## Enabling MOICE

1. Install all recommended patches and updates for Office 2003 (including [Office 2003 Service Pack 3](#)). Then deploy the Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats. Finally, install all recommended patches and updates for the Compatibility Pack (including [Service Pack 1](#)).
2. Make MOICE the registered handler for supported file types. The commands that do this can be typed at a command prompt (see Table 1), executed in a batch file, or pushed via Group Policy.

File type	Command to enable MOICE	Command to disable MOICE
.doc	ASSOC .doc=oice.word.document	ASSOC .doc=Word.Document.8
.xls	ASSOC .xls=oice.excel.sheet	ASSOC .xls=Excel.Sheet.8
.xlt	ASSOC .xlt=oice.excel.template	ASSOC .xlt=Excel.Template
.xla	ASSOC .xla=oice.excel.addin	ASSOC .xla=Excel.Addin
.ppt	ASSOC .ppt=oice.powerpoint.show	ASSOC .ppt=PowerPoint.Show.8
.pot	ASSOC .pot=oice.powerpoint.template	ASSOC .pot=PowerPoint.Template.8
.pps	ASSOC .pps=oice.powerpoint.slideshow	ASSOC .pps=PowerPoint.SlideShow.8

**Table 1: Enabling or Disabling MOICE for supported file types**

## Bypassing MOICE

Users can bypass the MOICE file format conversion by right-clicking on a file type that has become associated with Oice.exe, choosing Open With, and selecting the application originally associated with that file type (ie, Word, Excel, or PowerPoint). File Block functionality can prevent users from bypassing MOICE in this manner.

## File Block Functionality

File Block functionality allows administrators to keep Office 2003 users from opening or saving particular file types in Excel, PowerPoint, and Word. File Block functionality is not supported with previous versions of Office. With the appropriate settings enabled, it is no longer possible for users to bypass MOICE in the manner described above. Thus, when File Block functionality is used in conjunction with MOICE, administrators can force users to convert all supported Office 2003 file types to the new Office 2007 file formats. If some users have a legitimate need to work with macro-enabled files, administrators can create a trusted directory to which File Block settings do not apply. Users can then place their macro-enabled files in the trusted directory and open them directly with the appropriate Office 2003 application.

## Enabling File Block Functionality

File Block functionality is enforced by setting values in the registry. An Administrative Template that can be used to easily deploy the appropriate registry settings via Group Policy is available for download at <http://www.nsa.gov/snac/>.

## Additional Information about MOICE and File Block Functionality

For more information about MOICE and File Block functionality, see the companion deployment guide – it gives recommended File Block settings, offers some comments on possible usability issues, and lists references that can be used to further research these technologies.

Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation in the United States and other countries. This document is an independent publication and is not affiliated with, nor has it been authorized, sponsored, or otherwise approved by Microsoft Corporation.