

StripIT® identifies macros and active code in OpenOffice and Microsoft Office documents and removes these sources of risk, allowing the modified document to be delivered to the intended recipients.

Document based macros and other active code have long been seen as a source of security risk. There are few limits to what this embedded active code can do when run.

Microsoft Office applications provide an environment that uses ActiveX/COM DLLs already installed on your system to extend functionality. Visual Basic for Applications (VBA) was included in Microsoft Office to provide automation support in and between documents. VBA can access and use ActiveX/COM DLLs available in the office environment plus it can load others. VBA also has direct access to the file system and shell. The power of combining VBA macros with the office environment can pose a significant risk.

OpenOffice provides access for scripts running in a number of languages including its own version of Basic. These languages are feature-rich and could similarly be used for malicious purposes. OpenOffice can even run some VBA code imported from Excel, provided this capability is enabled.

There is general concern about what is downloaded when web browsing. That same concern should apply to what is running from inside your Office applications. Macro's are potentially dangerous and can run automatically.

Malicious use of VBA could provide access to confidential files or could disable the computer's operating system. VBA code has the same access rights as the user, which could be at administrator level.

Typically, documents attached to e-mail messages are scanned for virus content only, and if clear, are passed through. Anti-virus programs only look for known virus signatures. There is no reason for them to detect macros or other active code. Alternatively keyword searching may be used to identify the presence of active content and such documents might be quarantined.

StripIT provides a higher level of control, allowing macros and other active code to be identified and optionally stripped out of documents before they are delivered to the intended recipients.

StripIT identifies macros and active code in OpenOffice (Writer, Calc, Impress) and Microsoft Office 2003, 2007 and 2010 documents (Word, Excel, PowerPoint) and optionally removes these sources of risk, allowing the modified document to be delivered to the intended recipients free of macros and active code.

StripIT processes documents inside ZIP, 7Z, TAR, CAB, MIME & BZIP containers. Modified documents are returned to the archive container for delivery. **StripIT** also reads RAR containers and writes another supported format if necessary.

StripIT identifies nominated file types and can strip them off messages before transmission. It also allows identification of Information Rights Management (IRM) access permissions and the presence of orphaned data structures in some documents.

StripIT operates as an SMTP relay when operating stand-alone or as a content scanner when **StripIT** is integrated with MIMESweeper for SMTP.

StripIT can process OpenOffice and Microsoft Office word processor, spreadsheet and presentation documents and can be configured to **detect and report** via an appropriate classification or **detect and clean**, again reporting its action via an appropriate classification.

StripIT detects:

- * Openoffice.org Basic, Javascript, BeanShell and Python scripting languages.
- * Microsoft Office 97-2003, 2007-2010 Macros and Microsoft Office 2003 XML.

Some Microsoft Office documents may contain orphaned data structures. This can occur as a result of using fast save, which adds new data to the end of a document, without removing old data. Although this data is not directly accessible, it can contain anything, and it may be possible for the recipient to reactivate it. **StripIT** provides a way to remove these orphaned data structures.

StripIT identifies the presence of IRM access permissions in Microsoft Office documents. It allows these to be classified as "Not Checked" and quarantined by MIMESweeper for SMTP. **StripIT** uses file type signatures and file name masks to identify files to strip.



Who to Contact

Scientific Software and Systems Limited
Telephone +64 4 917-6670
e-mail: info@sss.co.nz
web: <http://www.sss.co.nz>

Licensing

StripIT is licensed on a per user basis.

Software prerequisites

MAILsweeper for SMTP version 5 and above.

StripIT is a product of:

Scientific Software and Systems Limited
New Zealand
Telephone +64 4 917-6670
e-mail: info@sss.co.nz
web: <http://www.stripit.co.nz>

