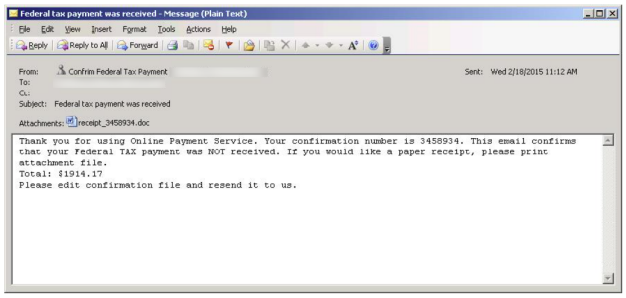
Microsoft Malware Protection Center (MMPC) is now Windows Defender Security Intelligence (WDSI). Watch out for even more info about threats and protecting you and your Windows computer.

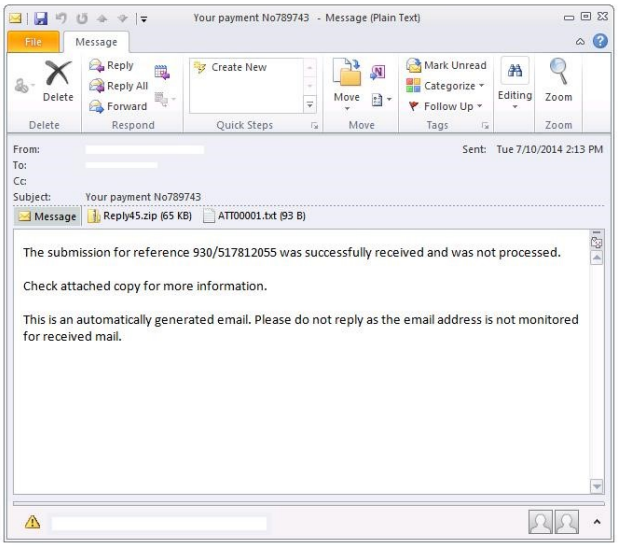
Macro malware

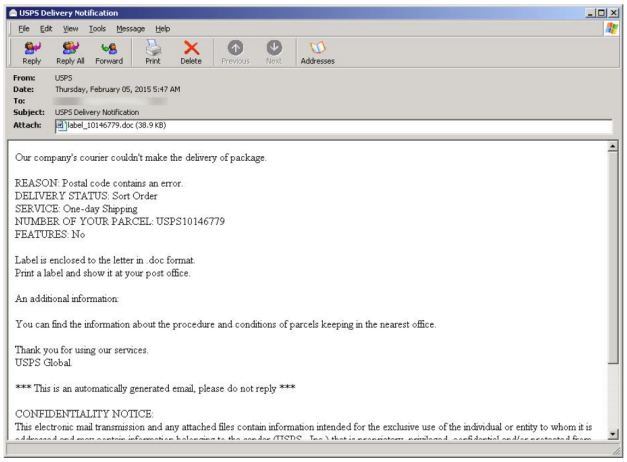
What is macro malware?

Macros are a legitimate way to automate some common tasks in Microsoft Office. However, malware can also use this functionality to download threats onto your PC.

Macro malware usually hides in Microsoft Word or Microsoft Excel documents. These malicious documents are sent as spam email attachments, or inside ZIP files attached to spam emails. They use files names designed to entice you into opening them. Some examples of the spam emails used to spread macro malware are shown below:





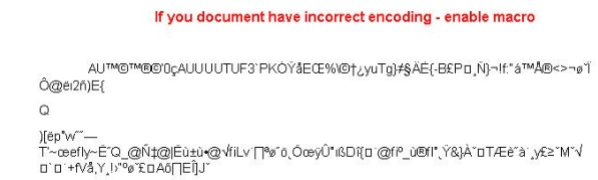


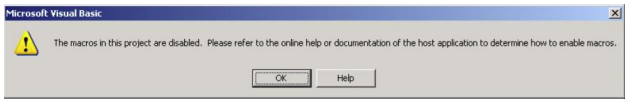
Some other attachment names we have seen imitate invoices, receipts, and other important documents, for example:

- *case number.doc*
- *e-ticket_79010838.doc*
- *fax_msg896-599-5459.doc*
- *invoice_723961.doc*
- *legal_complaint.doc*
- *logmein_coupon.doc*
- *receipt_3458934.doc*

Macro malware was fairly common several years ago because macros ran automatically whenever you opened a document.

However, in recent versions of Microsoft Office, macros are disabled by default. This means malware authors need to convince you to turn on macros so that their malware can run. They do this by showing you fake warnings when you open a malicious document. Some examples of this are shown below:





If you follow these prompts and enable macros, the malware can run. We have seen macro malware download threats from the following families:

- Ransom:MSIL/Swappa
- Ransom:Win32/Teerac
- TrojanDownloader:Win32/Chanitor
- TrojanSpy:Win32/Ursnif
- Win32/Fynloski
- Worm:Win32/Gamarue

Preventing macro malware infection

Stop macros running on your PC

Check if macros are disabled in your Microsoft Office applications. In enterprises, your system administrator can set the default setting for macros.

- Enable or disable macros in Office documents.

Don’t open suspicious emails

If you get an email from someone you don’t know, or an invoice for something you don’t remember buying, delete it. Spam emails are the main way macro malware spreads.