National Cyber Security Centre
Ministry of Security and Justice

Office macros

Old threat in new disguise

Fact sheet FS-2014-01
version 1.0 | 30 January 2014

In the 1990s, a lot of malware was developed that abused a function in the Microsoft Office software suite: macros. Macros offered users the possibility of task automation, but were a great weakness for virus writers through which they attacked their victims and spread their malware. Microsoft learned lessons from this and adjusted the default configuration of Office. As a result, users who did not adjust the default settings were no longer vulnerable and large-scale attacks by macro viruses were put to a halt.

Nowadays, home users in particular are no longer vulnerable, but large organisations sometimes use macros and have therefore adjusted the settings for this, deviating from the recommendation. This has drawn the renewed attention of malware authors and has gradually led to the return of macro viruses. These macro viruses are actually no longer viruses in the form of mass outbreaks, but a different type of malware for the purpose of customised and targeted attacks on individual organisations. The solution, however, is simple.

The most important facts

- Macros are given renewed attention; instead of the virus outbreaks of the 1990s, they are now being abused during targeted attacks on individual organisations.
- The settings of Microsoft Office are often made unsafe in order to enable the continued legitimate use of macros.
- Trusted file locations allow for the co-existence of a safe configuration and legitimate use of macros.

What are macros?

Macros can be active in some office applications (almost always Microsoft Office in practice). A macro consists of a series of automated commands that can be called by users with a certain combination of keystrokes or a mouse click. Macros can also be executed automatically, for example, when opening or closing a certain document. Macros are used by many organisations to create a correspondence layout or house style.

Software that supports macros often has an internal scripting language for this purpose. In Microsoft Office, it is possible to create a macro in the Microsoft Visual Basic (VBA) editor, which can be accessed from Word, Excel and PowerPoint. A user does not have to program VBA code, but can also use the recording function. In doing so, the user can perform a number of mouse movements or keystrokes and place them in a macro. Macros created with the recording function also consist of a VBA code, but this is generated by Office based on the user's actions.

A macro can be saved in the relevant document itself or in a separate document, for example, a document template. A macro can be called by name; if the same name is used several times, the closest macro will be executed. So if a macro name is called which is defined both in the document itself and in a template, the macro in the document will be executed.

A macro can only be executed if the security settings allow for this. This is determined by two aspects:

- the macro settings in the Trust Center and
- the trusted locations in File Locations.

What are the risks of macros?

Attackers can write macros that contain malicious codes and are executed automatically. As Office enables access to operating system resources, a macro constitutes a powerful tool for placing malware that infects a user's entire system. This is traditionally called a macro virus, although other forms of malware are used as there is renewed attention for it. It is even possible to place a complete program (for example a remote access tool) in an Office document that is then extracted and accessed from the macro.

Many organisations have changed the security settings to allow macros to be executed, because macros are used, for instance, to support the use of the house style. Sometimes, users within an organisation develop macros themselves - without the knowledge of the IT department - which are then used throughout the organisation. This creates an unknown dependency with respect to business processes, some of which are may be critical.

A file containing malware hidden in macros can be spread by attackers through e-mail attachments, web pages and removable devices such as USB disk drives. As the infected file behaves like a normal document, the infection often goes unnoticed. Anti-virus programs can recognise known malware on the basis of a unique 'fingerprint', but are often unable to recognise malicious behaviour in individually adjusted (and therefore unknown) malware.

Who are the victims?

As the current, standard settings of Microsoft Office no longer enable macros, many home users are not vulnerable to malware in macros. This method of attack is therefore no longer suitable for spreading viruses on a large scale.

Automatic macros

Macros can be executed automatically for certain events if the security settings allow this. These events are linked to certain macro names with differences between Word, Excel and PowerPoint. Word has the following options:

- **AutoExec** only works in templates and is started when the template is loaded (for the default template this will be immediately when Word is started).
- **AutoNew** is started when a new document is created.
- **AutoOpen** is started when a document is opened.
- **AutoClose** is executed before a document is closed.
- **AutoExit** is executed before Word is closed or when a template is closed.

Old news

Macro viruses have existed since the mid-1990s. The first self-spreading macro virus was WM.Concept in 1995. This virus did not cause any damage, but probably was just an experiment of the maker to demonstrate the technical possibility.

A more well-known outbreak was that of Melissa in 1999. Melissa spread through a Word document attached to an e-mail with a short text that had to persuade users to read the attachment. Once opened, the virus spread to other documents and changed those by inserting quotes from *The Simpsons* in them. Some documents were e-mailed without a user noticing. The virus also e-mailed itself via Outlook to the first fifty contacts in the user’s address book.

Melissa caught some media attention because it was the fastest spreading virus to date. It was discovered in the morning, and many organisations reported large numbers of infections that same night. Even Microsoft was forced to suspend all their internal e-mail communications to stop the virus from spreading.

Nowadays, macro viruses can no longer cause such large outbreaks. But if a malicious person is targeting a specific organisation, for instance, for the purpose of industrial espionage, unsafe macro settings could often prove to be the weakest link in the chain.

Over the past few years, a few incidents have occurred in which macros were used for targeted attacks on individual organisations, the so-called Advanced Persistent Threats.[1] Some of these targeted attacks started with an employee of the organisation opening an e-mail attachment. It is impossible to get a complete picture of how often these attacks occur; individually used malware goes unnoticed by anti-virus companies and organisations are very reluctant in communicating when such attacks took place.

There are no practical examples of malware hidden in macros for applications other than those from the Microsoft Office package, although it is also possible for specific malware to be customised for a target as part of an Advanced Persistent Threat.

[1] More information about Advanced Persistent Threats can be found in the NCSC fact sheet ‘De aanhouder wint’ (Dutch version) at https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-de-aanhouder-wint-advanced-persistent-threats.html.

Am I vulnerable?

You can consult the settings in the Trust Center in order to check if Microsoft Office enables macros.

Is my Microsoft Office set properly?
Instructions apply to versions 2007, 2010 and 2013

- Start a Microsoft Office application.
- Go to:
  - the Office button or File menu (top left);
  - Options (bottom right (2007) or in the left menu (2010, 2013));
  - Trust Center (last menu item);
  - Trust Center Settings;
  - Macro Settings.
- Check if macros are disabled, or if a notification is given.
- The last option enables all macros and is not recommended. If this option is selected, this Office application will be vulnerable to malicious macros.

Bear in mind that each Office application has its own settings. You should therefore repeat the above check for all Office applications (Word, Excel, PowerPoint, etc.).

There are other applications that support macros besides Microsoft Office. Consult the manual or the website of those applications to check if safe settings have been selected.

What can I do?

The following measures are required in order to prevent malware infection via macros. See the box 'How to proceed' for more details of the proposed measures.

- **Identify and list legitimate macro use** in your organisation. Some security measures could hinder business processes. To prevent sudden complaints of users leading to measures being reversed, it is important to first have a proper overview of all possible dependencies.

- **Use trusted file locations** or digital signatures for documents with legitimate macros. Block the execution of all other macros in all applications supporting it.

- **Configure the server for incoming e-mail** such that incoming e-mails containing macros in attachments are blocked. Bear in mind that legitimate documents may also be blocked in this case. Inform the addressee so that the sender can be instructed to deliver a file without any macros.

Besides these specific measures, general recommendations for malware prevention still stand. Train users not to open any unsolicited files, even if they seem to be coming from familiar senders.

How to proceed

1 Make all users aware of the risk of malware in files and how malware is spread.
2 Identify and list legitimate macro use. Be critical of the need for their use and see if alternatives are possible.
3 Adjust the macro settings in the Trust Center of Microsoft Office. The following settings are possible:
  - In the first option “Disable all macros without notification”, the macros are not executed without the user being informed of it or given the opportunity to deviate from this.
  - The second option “Disable all macros with notification” is the standard setting of Microsoft Office. If a user wants to execute a macro (or if an automatic macro is going to be executed), the user will receive a warning, but is given the opportunity to execute the macro.
  - The third option only enables macros that are digitally signed by a “Trusted publisher”, causing macros from other parties to be blocked.
  - The fourth option “Enable all macros (not recommended, potentially dangerous code can run)” allows all macros to be executed without any restrictions or warnings.
4 Consider the security level required for each application. It is, for instance, not likely for PowerPoint that macros are used in it. They can therefore be switched off completely.
5 Replace macros in individual documents by document templates and transfer all these files to central locations.
6 Set the central locations as trusted locations. If (some) users still want to use documents with macros, you should create a special trusted location for them where they can store these documents and from where they can start them.
7 Have suppliers of macro applications sign the documents digitally so that this publisher can be set as trusted publisher.
8 Configure the e-mail server or the virus scanner filtering the e-mails to block attachments with macros in them, possibly with a warning to the addressee.
9 Consider banning Excel files with macros if they do not have a specific extension for this (.xlsm).[2]
10 Block files with specific macro extensions (.docm, .pptm, .xlsm) for external sources (e-mail, internet, CD-ROM, etc.).

[2] See http://support.microsoft.com/kb/948615/ for this.

Finally

There are plenty of examples of targeted attacks on large organisations. In many cases, unfortunately, few details of the attack are released; technical information in particular is not published. This makes it difficult to get a good idea of the extent of this specific problem and the scope of the actual threat. There is still a clear reason for proper macro settings: if an attacker is looking for the weakest link, he will easily find it in macro vulnerability.

This fact sheet was made possible with the help of
prof. dr. E.R. Verheul, Radboud University Nijmegen.

Publication of **National Cyber Security Centre**
Turfmarkt 147 | 2511 DP The Hague
P.O. Box. 117 | 2501 CC The Hague
www.ncsc.nl | info@ncsc.nl | T +31 70-751 55 55 | F +31 70-322 25 37
Publication no: FS-2014-01 1.0 | No rights can be derived from this information.