Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Microsoft Office Macro Security

APRIL 2019

Introduction

Microsoft Office applications can execute macros to automate routine tasks. However, macros can contain malicious code resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion.

This document has been developed to discuss approaches that can be applied by organisations to secure systems against malicious macros while balancing both their business and security requirements.

The names and locations of Group Policy settings used in this document are taken from Microsoft Office 2016 and are equally applicable to Microsoft Office 365 ProPlus and Microsoft Office 2019. Some differences however may exist for earlier versions than Microsoft Office 2016.

Background

An increasing number of attempts to compromise organisations using malicious macros have been observed. In particular, adversaries have been observed using social engineering techniques to entice users into executing malicious macros in Microsoft Office files. The purpose of these malicious macros can range from cybercrime to more sophisticated exploitation attempts.

By understanding the business requirements for the use of macros, and applying the recommendations in this document, organisations can effectively manage the risk of allowing macros in their environments.

Macros explained

What are macros?

Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications (VBA) programming language.

A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity. However, an adversary can also create macros to perform a variety of malicious activities, such as assisting in the compromise of workstations in order to exfiltrate or deny access to sensitive information.

How are macros verified and trusted?

Microsoft Office has both trusted document and trusted location functions. Once trusted documents or trusted locations are defined, macros in trusted documents or macros in Microsoft Office files in trusted locations automatically

execute when the files are opened. While the use of trusted documents is discouraged, trusted locations when implemented in a controlled manner can allow organisations to appropriately balance both their business and security requirements.

Microsoft Office applications allow developers to include information about themselves by digitally signing their macros. The signing certificate that is used to create a signed macro confirms that the macro originated from the signatory, while the signature itself confirms that the macro has not been altered. Digital signing certificates can be self-generated by users, obtained from a commercial Certificate Authority or obtained from an organisation's security administrator if they operate their own Certificate Authority.

How can I determine which macros to trust?

To manage the use of macros within an organisation, all macros created by users or third parties should be reviewed by an independent party to the developer and assessed to be safe before being approved for use within the organisation.

When assessing whether macros are safe or not, assessors should ask themselves the following questions:

- Is there a business requirement for a particular macro?
- Has the macro been developed or provided by a trusted party?
- Has the macro been validated by a trustworthy and technically skilled party?

Securing systems against malicious macros

The following table displays the security benefit, business impact and implementation difficulty of different approaches to managing macros in Microsoft Office files.

Approach	Security Benefit	Business Impact	Implementation Difficulty
All macros are disabled	Very high	High	Low
Only macros from trusted locations are enabled	High	Medium	Medium
Only digitally signed macros are enabled (hardened implementation)	High	Medium	High
Only digitally signed macros are enabled (standard implementation)	Medium	Medium	High
Users decide which macros to enable on a case-by-case basis	Low	Low	Low
All macros are enabled	None	None	Low

All macros are disabled

If organisations do not have a business requirement for macro use, support for their use should be disabled across the Microsoft Office suite.

To prevent users or an adversary from bypassing macro security controls, all support for trusted documents and trusted locations should be disabled.

To ensure users cannot knowingly or unintentionally alter macro security controls via a Microsoft Office application's Trust Center interface, organisations should apply macro security controls using Group Policy settings.

Only macros from trusted locations are enabled

If organisations have a business requirement for macro use, approved macros in Microsoft Office files in trusted locations can be allowed to execute. However, only specific Microsoft Office applications for which there is a business requirement for macro use should be allowed to execute approved macros. All other Microsoft Office applications should have support for macros disabled.

To prevent users or an adversary from bypassing macro security controls, support for trusted documents should be disabled while trusted locations should prevent all users, except for approved users, from adding or modifying macros in Microsoft Office files in these locations. Using an appropriately secured network path as a trusted location can assist in the centralised management and control of macros in Microsoft Office files.

To ensure users cannot knowingly or unintentionally alter macro security controls via a Microsoft Office application's Trust Center interface, organisations should apply macro security controls using Group Policy settings.

Only digitally signed macros are enabled (hardened implementation)

If organisations have a business requirement for macro use, digitally signed macros can be allowed to execute. However, only specific Microsoft Office applications for which there is a business requirement for macro use should be allowed to execute digitally signed macros. All other Microsoft Office applications should have support for macros disabled.

To prevent users or an adversary from bypassing macro security controls, support for trusted documents and trusted locations should be disabled.

To further reduce the likelihood of an adversary signing a malicious macro and it being executed by users, organisations should restrict their use of trusted publishers to digital signing certificates belonging to their organisation. In addition, the ability to enable macros signed by a non-trusted publisher, or add additional trusted publishers, should be disabled for users. This includes via the trust bar, backstage view, Internet Options control panel and the use of certificate management tools.

Organisations should take care to sufficient test this approach before implementation to ensure that there are no unintended consequences of implementing the above restrictions on Microsoft Office and certificate management functionality within their environment.

To ensure users cannot knowingly or unintentionally alter macro security controls via a Microsoft Office application's Trust Center interface, organisations should apply macro security controls using Group Policy settings.

Only digitally signed macros are enabled (standard implementation)

If organisations have a business requirement for macro use, digitally signed macros can be allowed to execute. However, only specific Microsoft Office applications for which there is a business requirement for macro use should be allowed to execute digitally signed macros. All other Microsoft Office applications should have support for macros disabled.

To prevent users or an adversary from bypassing macro security controls, support for trusted documents and trusted locations should be disabled.

To reduce security warning fatigue for users, organisations should consider recognising their digital signing certificates as trusted publishers. Note, however, that users will still be prompted to enable or disable other digitally signed macros even if they don't originate from a trusted publisher.

To ensure users cannot knowingly or unintentionally alter macro security controls via a Microsoft Office application's Trust Center interface, organisations should apply macro security controls using Group Policy settings.

Users decide which macros to enable on a case-by-case basis

If organisations have a business requirement for macro use, they should manage the use of macros in their environment using one of the recommended approaches discussed below. Relying on users to make correct security decisions one hundred percent of the time is not a realistic expectation considering the sophistication of many spear phishing attempts. As such, allowing users to decide which macros to enable on a case-by-case basis presents a significant risk and should not be implemented.

All macros are enabled

If organisations have a business requirement for macro use, they should manage the use of macros in their environment using one of the recommended approaches discussed below. Allowing unrestricting execution of all macros presents a serious risk and should never be implemented.

Recommended approach

To protect themselves against malicious macros, organisations should implement one of the following recommended approaches:

- all macros are disabled
- only macros from trusted locations are enabled
- only digitally signed macros are enabled (hardened implementation).

In addition to implementing one of the recommended approaches above, organisations should:

- implement application whitelisting to mitigate a malicious macro running unauthorised programs
- implement email and web content filtering to inspect incoming Microsoft Office files for macros, and block or quarantine them as appropriate
- implement macro execution logging to verify only authorised macros are used (e.g. by logging the execution of known file extensions such as dotm, docm, xlsm, pptm and ppsm)
- ensure users assigned to assessing the safety of macros have appropriate VBA training.

Group Policy settings

The following Group Policy settings can be implemented depending on an organisation's desired approach to managing macros in Microsoft Office files.

Microsoft Windows

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
Computer Configuration\Policies\Administration Templates\Windows Components\Internet Explorer\Internet Control Panel			
Disable the Content page	N/A	N/A	Enabled
User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\ Restricted/Permitted snap-ins			
Certificates	N/A	N/A	Disabled

Microsoft Office 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings			
Automation Security	Enabled Set the Automation Security level: Disable macros by default	Enabled Set the Automation Security level: Use application macro security level	Enabled Set the Automation Security level: Use application macro security level
Disable all Trust Bar notifications for security issues	N/A	N/A	Enabled
Disable VBA for Office applications	Enabled	Disabled	Disabled
User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings\Trust Center			
Allow mix of policy and user locations	Disabled	Disabled	Disabled

Microsoft Access 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Access 2016\Application Settings\Security\Trust Center			
Turn off trusted documents	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros
User Configuration\Policies\Administration Templates\Microsoft Access 2016\Application Settings\Security\Trust Center\Trusted Locations			
Allow Trusted Locations on the network	Disabled	Enabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled
User Configuration\Policies\Administration Templates\Microsoft Access 2016\Disable Items in User Interface\ Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092

Microsoft Excel 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Disable Items in User Interface\ Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092

User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center			
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled
Trust access to Visual Basic Project	Disabled	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros
User Configuration\Policies\Administration Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\ Trusted Locations			
Allow Trusted Locations on the network	Disabled	Enabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled

Microsoft Outlook 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Outlook 2016\Disable Items in User Interface\ Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092
User Configuration\Policies\Administration Templates\Microsoft Outlook 2016\Security\Trust Center			
Apply macro security settings to macros, add-ins and additional actions	Enabled	Enabled	Enabled

Security settings for macros	Enabled Security Level: Never warn, disable all	Enabled Security Level: Never warn, disable all	Enabled Security Level: Warn for signed, disable unsigned

Microsoft PowerPoint 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\Disable Items in User Interface\Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center			
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled
Trust access to Visual Basic Project	Disabled	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros
User Configuration\Policies\Administration Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Trusted Locations			
Allow Trusted Locations on the network	Disabled	Enabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled

Microsoft Project 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Project 2016\Project Options\Security\Trust Center			
Allow Trusted Locations on the network	Disabled	Enabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros

Microsoft Publisher 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Publisher 2016\Disable Items in User Interface\ Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092
User Configuration\Policies\Administration Templates\Microsoft Publisher 2016\Security			
Publisher Automation Security Level	Enabled High (disabled)	Enabled High (disabled)	Enabled By UI (prompted)
User Configuration\Policies\Administration Templates\Microsoft Publisher 2016\Security\Trust Center			
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros

Microsoft Visio 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Visio 2016\Disable Items in User Interface\ Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092
User Configuration\Policies\Administration Templates\Microsoft Visio 2016\Visio Options\Security\Macro Security			
Enable Microsoft Visual Basic for Applications project creation	Disabled	Disabled	Disabled
Load Microsoft Visual Basic for Applications projects from text	Disabled	Disabled	Disabled
User Configuration\Policies\Administration Templates\Microsoft Visio 2016\Visio Options\Security\Trust Center			
Allow Trusted Locations on the network	Disabled	Enabled	Disabled
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled
Disable all trusted locations	Enabled	Disabled	Enabled
Turn off trusted documents	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros

Microsoft Word 2016

Group Policy Setting	All Macros Disabled	Only Macros from Trusted Locations	Only Digitally Signed Macros (Hardened)
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Disable Items in User Interface\ Custom			
Disable commands	N/A	N/A	Enabled Enter a command bar ID to disable: 19092
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Word Options\Security\Trust Center			
Block macros from running in Office files from the Internet	N/A	Enabled	Enabled
Trust access to Visual Basic Project	Disabled	Disabled	Disabled
Turn off trusted documents	Enabled	Enabled	Enabled
Turn off Trusted Documents on the network	Enabled	Enabled	Enabled
VBA Macro Notification Settings	Enabled Disable all without notification	Enabled Disable all without notification	Enabled Disable all except digitally signed macros
User Configuration\Policies\Administration Templates\Microsoft Word 2016\Word Options\Security\Trust Center\Trusted Locations			
Allow Trusted Locations on the network	Disabled	Enabled	Disabled
Disable all trusted locations	Enabled	Disabled	Enabled

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).