How to protect your organization from malicious macros

January 2024 **ITSAP.00.200**

Macros are written sequences that automate processes, data flows, and repetitive tasks in applications, such as in some Microsoft Office Suite documents. These written sequences, sometimes referred to as embedded code, allow the user to create shortcuts for specific tasks like sorting worksheets alphabetically, unmerging all merged cells, or making all rows and columns visible. Users can apply a signed certificate on the macros they create to confirm where the macro originated from. They can also be verified by your organization to offer users trustworthy macros to use as needed.

Your users, administrators, and service providers can write macros **but so can threat actors**. Threat actors can create malicious macros and include them in documents which are then transmitted throughout your organization, such as through phishing attacks. Malicious macros can compromise applications and affect programs throughout your systems. When opening a file, you may be prompted by a notification asking if you would like to activate or deactivate macros. On some newer versions of Microsoft Office applications, macros from the internet, such as those in email attachments, are blocked by default. This document outlines the risks related to using macros and some measures you can take to protect your systems from malicious intrusions.

Potential threats

An application may appear to be safe, but threat actors can embed malicious macros in the script of the application that are set to execute when opened. Threat actors can also send you an email with an attachment or file containing malicious macros. If your organization uses macros from internal and external sources, your systems and information may be at risk to some of the following threats.

Macro viruses

Macro viruses are made up of malicious code and disguised as legitimate macros embedded in an application. Macro viruses can automatically run when documents are open and infect your files, damaging the contents of documents. Macro viruses can also spread to other software and files that they come in contact with, such as disk files, network files, and email attachments, and infect your entire system.

Unauthorized access

Threat actors use malicious macros to bypass security controls, like allow lists, and gain access to your systems and network. These macros can be used to execute malicious content and steal or destroy sensitive information. Phishing attempts often use malicious macros in the attached files of their messages, disguised as legitimate attachments. A threat actor may be able to convince you to activate macros in an attachment, allowing the malicious content to spread throughout your systems and network.

Insider threats

Anyone who has knowledge of or access to your infrastructure and information can cause harm, either knowingly or accidentally.

Insider threats can exist if someone is able to:

- create macros that contain sensitive information, such as passwords, or code that has been copied from unverified external sources
- spread macros throughout the organization by sharing documents
- forward documents from external sources that are not verified by your organization's policies
- spread documents with malicious macros through cloud components

AWARENESS SERIES

Cat. No. D97-1/00-200-2023E-PDF
ISBN 978-0-660-68427-7

Security measures

To protect your systems from malicious macros, you should implement the following security measures:

- Deactivate default macros that are not required
- Ensure users cannot re-activate macros that have been deactivated
- Enforce the principle of least privilege to assign administrative privileges and account access
- Use organization-developed or signed macros that are verified by technical authorities
- Ensure macros cannot contain any sensitive information like personal credentials
- Audit actions made by users developing macros in the organization, such as administrative changes
- Train your organization's users and provide guidance on macro security and phishing to support awareness
- Update and patch applications and systems frequently
- Scan your devices regularly with an antivirus program from a reputable vendor

Trustworthy macros

Your organization and users can often trust macros in the following circumstances:

- Your organization develops and owns the macros and they are maintained internally
- Your organization has set policies to activate only signed and verified macros such as those developed by your organization
- Your documents are from known senders, are sourced internally and have not been externally forwarded

Alternatives to macros

If you deactivate the use of macros, there are other ways to automate tasks, including:

- using off-the-shelf, commercially available applications from office productivity suites
- using software as a service (SaaS) alternatives to automate data flow
- building custom applications to support business processes

Reminder:

We recommend that you deactivate macros from external sources. Although there are trusted ways of using macros and protecting your systems from malicious macros, there are still risks. Macros from external sources open up your organization to unintended consequences.

Learn more

Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)

Application allow list (ITSAP.10.095)

How to protect your organization from insider threats (ITSAP.10.003)

Managing and controlling administrative privileges (ITSAP.10.094)

Network security auditing (ITSAP.80.086)

Offer tailored cyber security training to your employees (ITSAP.10.093)

How updates secure your device (ITSAP.10.096)

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Canadian Centre for Cyber Security (Cyber Centre) website at **cyber.gc.ca**