HOW TO PROTECT YOUR ORGANIZATION FROM MALICIOUS MACROS

SEPTEMBER 2020 **ITSAP.00.200**

Macros are written sequences that imitate user keystrokes and mouse commands to automatically repeat tasks in applications. Macros are used in many Office suite documents to automate processes and data flows. They are embedded in the code of the files, enabling users to create shortcuts for specific tasks (e.g. sort worksheets alphabetically, unmerge all merged cells, unhide all rows and columns). When opening a file, you may be prompted by a notification asking if you would like to enable or disable macros. Users can use a signed certificate on the macros they create to confirm where the macro originated from. Macros can also be verified by your organization to offer users trustworthy macros to use in applications 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 to be transmitted through your organization. Malicious macros can compromise applications and affect programs throughout your systems. This document outlines the risks related to using macros and some measures you can take to protect your systems from malicious intrusions.

POTENTIAL THREATS

A file may appear to be safe, but threat actors can embed malicious macros in the script of the application to activate when the file is opened. A threat actor may send you an email with an attachment 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

Malicious code that is disguised as a legitimate macro and embedded in an application. Macro viruses can automatically run when documents are open and infect your files. Infected files can damage the contents of documents and spread to other software and files that it comes in contact with (e.g. disk files, network files, email attachments), infect your entire system.

UNAUTHORIZED ACCESS

Threat actors use malicious macros to bypass security controls (e.g. allow list) 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.

INSIDER THREATS

Anyone who has knowledge of or access to your infrastructure and information can cause harm, either knowingly or accidentally. Regarding the use of malicious macros, insider threats can exist if someone has the ability to perform the following functions:

- Create macros (e.g. copying code from unverified external sources), including macros containing sensitive information (e.g. passwords).
- Spread macros throughout the organization (e.g. sharing documents).
- Forward documents from external sources (e.g. not verified by your organizations policies).
- Spread documents with malicious macros through cloud components.

For more details on insider threats, see *ITSAP.10.003 How to Protect Your Organization from Insider Threats* on **cyber.gc.ca**

SECURITY MEASURES

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

- Disable default macros that are not required.
- Enforce the principle of least privilege to assign administrative privileges and account access.
- Ensure users cannot re-enable disabled macros.
- Use organization-developed or signed macros that are verified by technical authorities.
- Ensure macros cannot contain any sensitive information (e.g. personal credentials).
- Audit actions made by users developing macros in the organization (e.g. administrative changes).
- Train your organization's users and provide guidance on macro security to support awareness.
- Update and patch applications and systems frequently.

ALTERNATIVES TO MACROS

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

- Using off-the-shelf (i.e. a commercially available product that is not customized) applications from office productivity suites.
- Using software as a service (SaaS) alternatives to automate data flow.
- Building custom applications to support business processes.

TRUSTWORTHY MACROS

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

- Your organization develops and owns the macros (e.g. maintained internally).
- Your organization has set policies to enable only signed and verified macros (i.e. organization-developed macros).
- Your documents are from known senders and are sourced internally (e.g. not externally forwarded).

Remember

We recommend that you disable 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.

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**