M

Macro Virus and Macro Malware: Detection, Removal, and Prevention

Learn how malicious Office macros spread, which file types can contain VBA, what to do after enabling content, and how organizations should restrict macros.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is a macro virus?

02 How macro malware spreads

03 Which Office files can contain macros?

04 Warning signs

05 What to do after enabling a suspicious macro

06 How to remove macro malware

07 Macro protection for individuals

08 Macro controls for organizations

09 Macro virus vs. ordinary document exploit

A **macro virus** is malicious code written in an application's macro language and stored in a document or template. The broader term **macro malware** includes downloaders and scripts that use macros to install ransomware, information stealers, or remote-access tools.

A malicious script sent by email is not necessarily a macro virus. The ILOVEYOU worm, for example, used a VBScript attachment; the file type and execution mechanism matter more than the fact that it arrived in a message.

Legitimate macros automate repetitive work. A macro-enabled file is not automatically malicious, but a document received unexpectedly should never require you to disable security controls or click "Enable Content" merely to read it.

01 What is a macro virus?

A macro virus is a computer virus implemented in the macro language of an application such as Word or Excel. It can run when the infected document or template is opened in a trusted context or when the user enables its macros. Traditional macro viruses copy themselves into other documents or templates; many modern malicious macros act as downloaders instead, so **macro malware** is often the more accurate term.

02 How macro malware spreads

Attackers send an Office document directly or inside an archive, often using invoice, delivery, payroll, or urgent-business themes. The document may claim that content is blurred, protected, or created in an older version and instruct the recipient to enable macros. Once permitted, the macro can start other tools, download malware, or alter user settings.

Modern Microsoft 365 Apps block VBA macros by default in many files marked as originating from the Internet. Attackers therefore try to convince users to remove that mark, copy files into trusted locations, or use alternate delivery methods.

03 Which Office files can contain macros?

- `.docm` and `.dotm` for Word.
- `.xlsm`, `.xltm`, and `.xlam` for Excel.
- `.pptm`, `.potm`, and `.ppam` for PowerPoint.
- Some older binary Office formats can also contain macro code.

A renamed extension does not change a file’s real format. Show file extensions and verify documents through the expected sender.

04 Warning signs

Be cautious when a document arrives unexpectedly, asks to enable content, contains instructions to change Trust Center settings, launches a command window, creates a process such as PowerShell, or contacts unfamiliar domains. Grammar and visual quality are weak signals; a convincing document can still be malicious.

05 What to do after enabling a suspicious macro

1. Disconnect the device from networks when practical and stop using it for sensitive accounts.
2. Do not forward the document to colleagues.
3. Record the message, sender, filename, time, and actions taken.
4. Notify the security team and run approved endpoint scans.
5. Review processes, persistence, downloads, and network connections.
6. Change exposed credentials from a known-clean device if theft is possible.

06 How to remove macro malware

Quarantine the document and any payloads, remove persistence, and update the affected applications. If privileged malware ran or system integrity is uncertain, rebuild from a known-good source. Deleting the original document is insufficient when it already downloaded or launched another program.

07 Macro protection for individuals

Keep Office and Windows updated, leave macros blocked unless there is a verified business need, and download templates only from trusted sources. Do not add a folder to Trusted Locations just to bypass a warning. When a legitimate macro is required, verify the publisher and file through a separate channel.

08 Macro controls for organizations

Block macros from Internet-origin files, permit only trusted or signed macros where feasible, control trusted locations, and apply attack-surface-reduction rules after testing. Filter risky attachments, restrict script interpreters, and monitor Office applications spawning unusual child processes. Provide an approved workflow for business macros so users do not invent bypasses.

09 Macro virus vs. ordinary document exploit

A macro requires the application’s macro engine and normally some form of permission or trusted context. A document can also exploit a software vulnerability without a macro. Keep document readers patched and treat both enabled code and crafted files as potential risks.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com