New feature in Office 2016 can block macros and help prevent infection | Microsoft Security Blog

By Microsoft Defender Security Research Team

Published: 2016-03-22 · Archived: 2026-04-05 18:25:29 UTC

Macro-based malware infection is still increasing

Macro-based malware continues its rise. We featured macro-based malware in our Threat Intelligence report last year, but infections are still increasing.

Despite periodic lulls, infections for the top 20 most detected macro-based malware were high over the past three months.

In the enterprise, recent data from our Office 365 Advanced Threat Protection service indicates 98% of Office-targeted threats use macros.

Note these are detections and not necessarily successful infections. To learn more about Advanced Threat Protection and other security features in Office 365, check out this blog and video.

> *Office 365 client applications now integrate with AMSI, enabling antivirus and other security solutions to scan macros and other scripts at runtime to check for malicious behavior.*
>
> *This is part of our continued efforts to tackle entire classes of threats. Learn more:*
>
> ***Office VBA + AMSI: Parting the veil on malicious macros***

The enduring appeal for macro-based malware appears to rely on a victim's likelihood to enable macros. Previous versions of Office include a warning when opening documents that contain macros, but malware authors have become more resilient in their social engineering tactics, luring users to enable macros in good faith and ending up infected.

Block the macro, block the threat

In response to the growing trend of macro-based threats, we've introduced a new, tactical feature in Office 2016 that can help enterprise administrators prevent the risk from macros in certain high risk scenarios. This feature:

1. Allows an enterprise to selectively scope macro use to a set of trusted workflows.
2. Block easy access to enable macros in scenarios considered high risk.
3. Provide end users with a different and stricter notification so it is easier for them to distinguish a high-risk situation against a normal workflow.

This feature can be controlled via Group Policy and configured per application. It enables enterprise administrators to block macros from running in Word, Excel and PowerPoint documents that come from the Internet. This includes scenarios such as the following:

1. Documents downloaded from Internet websites or consumer storage providers (like OneDrive, Google Drive, and Dropbox).
    - NOTES:
      The macro will not be blocked under the following conditions:
        - When the file is opened from the OneDrive location of the user signed into the client, i.e., your own OneDrive location
        - When the file is opened from within the tenant (OneDrive for Business or SharePoint Online) of the user signed into the client, i.e., your own tenant.
2. Documents attached to emails that have been sent from outside the organization (where the organization uses the Outlook client and Exchange servers for email)
3. Documents opened from public shares hosted on the Internet (such as files downloaded from file-sharing sites).

Let's walk through a common attack scenario and see this feature in action.

Claudia is an enterprise administrator at Contoso. After a rash of macro-based malware attacks targeting her organization, she learns of this new feature in Office 2016 and has rolled out a Group Policy update to all Office clients on the network.

Stewart is a cybercriminal looking to attack and penetrate the Contoso network. Stewart uses macro-based malware because he's had recent successes using it. He launches his attack campaign against Contoso by targeting James, an employee there.

James receives an email from Stewart in his inbox that has an attached Word document. The email has content designed to pique James's interest and influence him to open the attachment.

When James opens the Word document, it opens in Protected View. Protected View is a feature that has been available in Word, Excel, and PowerPoint since Office 2010. It is a sandboxed environment that lets a user read the contents of a document. Macros and all other active content are disabled within Protected View, and so James is protected from such attacks *so long as he chooses to stay in Protected View*.

However, Stewart anticipates this step and has a clear and obvious message right at the top of the document designed to lure James into making decisions detrimental to his organization's security. James follows the instructions in the document, and exits Protected View as he believes that will provide him with access to contents of the document. James is then confronted with a strong notification from Word that macros have been blocked in this document by his enterprise administrator. There is no way for him to enable the macro from within the document.

James's security awareness is heightened by the strong warning and he starts to suspect that there is something fishy about this document and the message. He quickly closes the document and notifies his IT team about his suspicions.

This feature relies on the security zone information that Windows uses to specify trust associated with a specific location. For example, if the location where the file originates from is considered the Internet zone by Windows, then macros are disabled in the document. Users with legitimate scenarios that are impacted by this policy should work with their enterprise administrator to identify alternative workflows that ensure the file's original location is considered trusted within the organization.

Use Group Policy to enforce the setting, or configure it individually

Administrators can enable this feature for Word, Excel, and PowerPoint by configuring it under the respective application's Group Policy Administrative Templates for Office 2016. For example, to enable this setting for Word:

1. Open the Group Policy Management Console, right-click the Group Policy Object you want to configure and click **Edit**.
2. In the **Group Policy Management Editor**, go to **User configuration**.
3. Click **Administrative templates** > **Microsoft Word 2016** > **Word options** > **Security** > **Trust Center.**
4. Open the **Block macros from running in Office files from the Internet** setting to configure and enable it.

You can read more about this Group Policy setting at Plan security settings for VBA macros in Office 2016.

Final tips

For end-users, we always recommend that you don't enable macros on documents you receive from a source you do not trust or know, and be careful even with macros in attachments from people you do trust – in case they've been hacked.

For enterprise administrators, turn on mitigations in Office that can help shield you from macro based threats, including this new macro-blocking feature. If your enterprise does not have any workflows that involve the use of macros, disable them completely. This is the most comprehensive mitigation that you can implement today.

More info for end-users: Learn how to enable or disable macros in Office files

More info for admins and IT professionals: Learn about security and compliance in Office 365

Related blog entry: **Machine learning vs. social engineering**

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.

Follow us on Twitter @WDSecurity.

Source: https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/