Microsoft disables Excel 4.0 macros by default to block malware

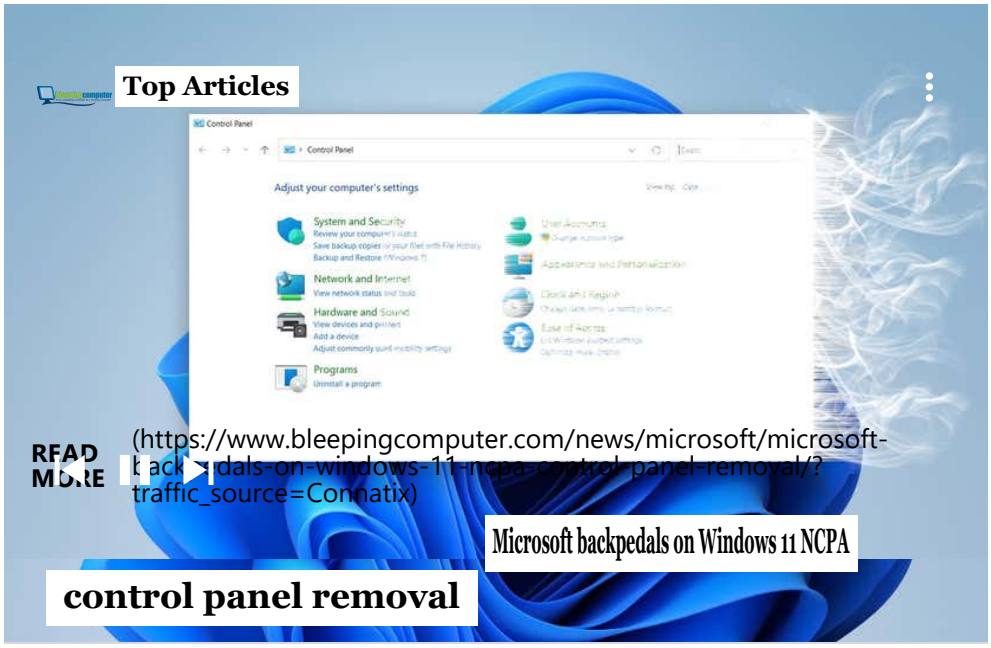
By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** January 21, 2022 10:56 AM **0**

Microsoft has announced that Excel 4.0 (XLM) macros will now be disabled by default to protect customers from malicious documents.

In October, the company first revealed in a Microsoft 365 message center update that it would disable XLM macros in all tenants (https://www.bleepingcomputer.com/news/microsoft/microsoft-is-

disabling-excel-40-macros-by-default-to-protect-users/) if the users or admins hadn't manually toggled the feature on or off.

Starting July 2021 (https://techcommunity.microsoft.com/t5/excel-blog/restrict-usage-of-excel-4-0-xlm-macros-with-new-macro-settings/ba-p/2528450), Windows admins could also use group policies and users the 'Enable XLM macros when VBA macros are enabled' setting from the Excel Trust Center to disable this feature manually.



"In July of 2021, we released a new Excel Trust Center setting option to restrict the usage of Excel 4.0 (XLM) macros," said (https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905) Catherine Pidgeon, a Principal Program Manager Lead at Microsoft, earlier this week in a Tech Community blog post.

"As planned, we have now made this setting the default when opening Excel 4.0 (XLM) macros. This will help our customers protect themselves against related security threats."

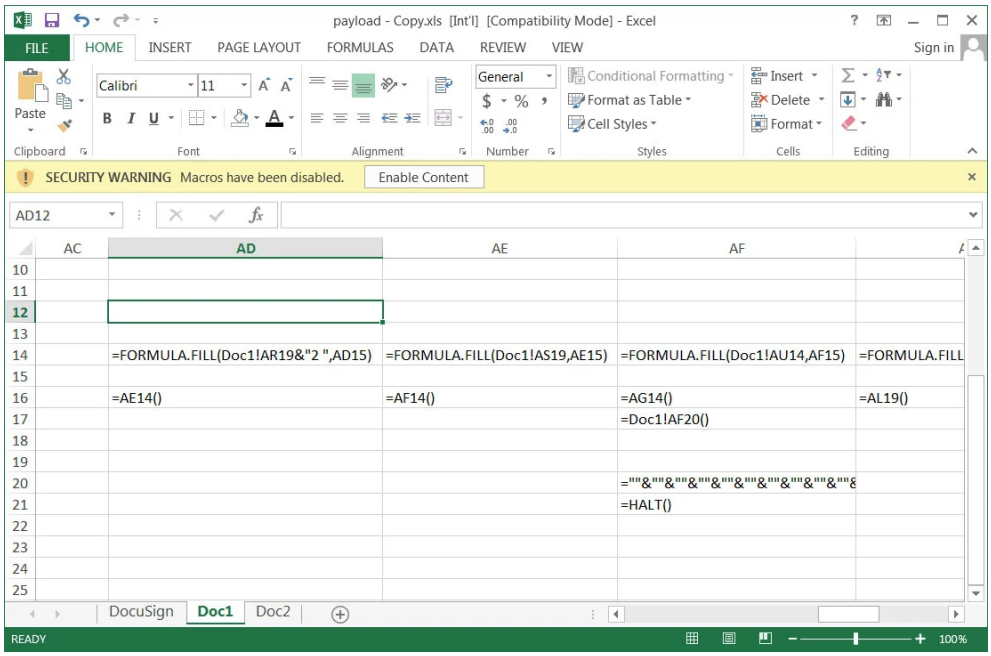
Admins can configure how Excel macros are allowed to run using Group Policy settings, Cloud policies, and ADMX policies.

They can also block all Excel XLM macro use in their environments (including new user-created files) by toggling on the "Prevent Excel from running XLM macros" Group Policy, configurable via Group Policy Editor or registry key.

Right now, XLM macros are disabled by default in the September fork, Excel version 16.0.14527.20000 and newer available in the:

- Current Channel builds 2110 or greater (first released in October)
- Monthly Enterprise Channel builds 2110 or greater (first released in December)

- Semi-Annual Enterprise Channel (Preview) builds 2201 or greater (first ships in March 2022)
- Semi-Annual Enterprise Channel builds 2201 or greater (will ship July 2022)



XLS document with obfuscated Excel 4.0 macro

XLM (aka Excel 4.0) macros (https://support.microsoft.com/en-us/office/working-with-excel-4-0-macros-ba8924d4-e157-4bb2-8d76-2c07ff02e0b8) were the default Excel macro format until Excel 5.0 was released in 1993 (https://www.kb.cert.org/vuls/id/125336) when Microsoft first introduced VBA macros (https://support.microsoft.com/en-us/office/automate-tasks-with-the-macro-recorder-974ef220-f716-4e01-b015-3ea70e64937b) which are still the default format.

However, despite being discontinued, threat actors are still using XLM three decades later to create documents that deploy malware or perform other malicious behavior manipulating files on the local filesystem because current Microsoft Office versions still come with support for XLM macros.

Malicious campaigns using this type of macros to push malware have been observed downloading and installing TrickBot (https://twitter.com/h2jazi/status/1331342523462258696), Zloader (https://twitter.com/elceef/status/1392177026078056455), Qbot (https://twitter.com/elceef/status/1396916046188195849), Dridex (https://twitter.com/jcarndt/status/1260998505541353472), and many other strains on victims' computers.

Microsoft also silently added a Group Policy in October 2019 (https://www.bleepingcomputer.com/news/microsoft/office-365-admins-can-now-block-malicious-microsoft-query-iqy-files/) that allows admins to block Excel users from opening untrusted (and potentially malicious) Microsoft Query files with IQY, OQY, DQY, and RQY extensions.

Such files have been weaponized in numerous malicious attacks to deliver remote access Trojans (https://www.bleepingcomputer.com/news/security/malspam-campaigns-using-iqy-attachments-to-bypass-av-filters-and-install-rats/) and malware loaders (https://www.bleepingcomputer.com/news/security/necurs-botnet-pushing-new-marap-malware/) since early 2018.

Related Articles:

Microsoft offers 50% subscription discounts to Office pirates (https://www.bleepingcomputer.com/news/microsoft/microsoft-offers-50-percent-subscription-discounts-to-office-pirates/)

OceanLotus hackers turn to web archive files to deploy backdoors (https://www.bleepingcomputer.com/news/security/oceanlotus-hackers-turn-to-web-archive-files-to-deploy-backdoors/)

Microsoft fixes critical Office bug, delays macOS security updates (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-critical-office-bug-delays-macos-security-updates/)

Dive into data with this Excel, Power BI, and Alteryx learning bundle (https://www.bleepingcomputer.com/offer/deals/dive-into-data-with-this-excel-power-bi-and-alteryx-learning-bundle/)

Microsoft: KB5008212 Windows security update breaks Outlook search (https://www.bleepingcomputer.com/news/microsoft/microsoft-kb5008212-windows-security-update-breaks-outlook-search/)