Microsoft allows users to reactivate Windows App installer

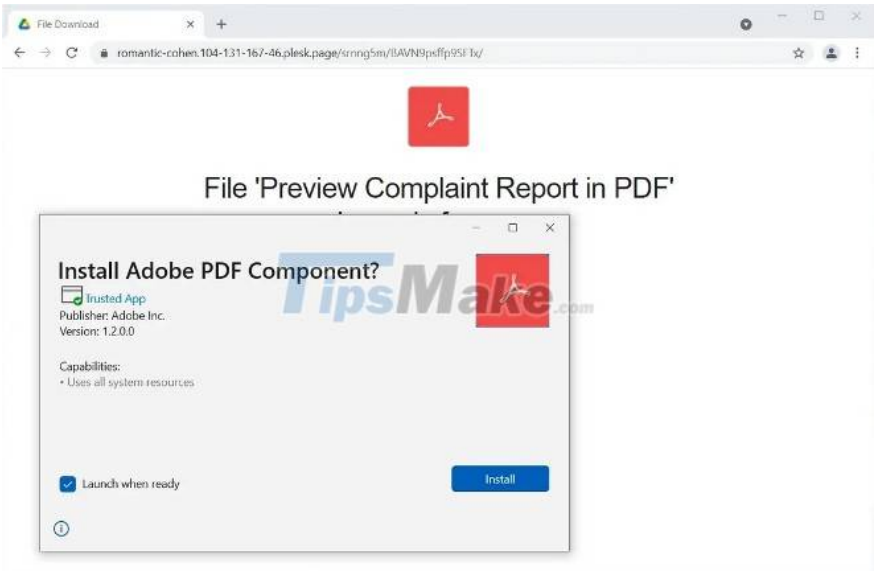
Microsoft has just allowed enterprise administrators to re-enable the MSIX ms-appinstaller protocol handler. Windows App Installer used to be disabled to avoid being abused by the Emotet malware.

App Installer (also known as AppX Installer) allows users to install applications directly from a web server using an MSIX package or an App Installer file without downloading the installer to their computer first.

Microsoft has disabled the ms-appinstaller map in response to reports that the Emotet malware is exploiting a zero-day vulnerability that impersonates Windows AppX Installer, forcing users to download application packages to their devices before they can. install them using App Installer.

"We recognize that this feature is very important to many organizations and businesses. We are taking the time to conduct thorough testing to ensure that re-enabling this protocol can be done without delay. safely," said Dian Hartono, program manager at Microsoft.

"We are looking at rolling out a Group Policy that will allow IT admins to re-enable the protocol and control its use within their organization."



How to re-enable the ms-appinstaller . protocol

According to an update from Hartano, Microsoft has finally figured out how to fix the problem and now they've allowed administrators to re-enable the ms-appinstaller protocol handler. To do this, you need to update to the

latest App Installer version (1.17.10751.0) and enable a group policy.

On systems that cannot update the App Installer using the internet-connected installer, you can also download the offline version from the Microsoft Download Center site.

The App Installer feature will be re-enabled after downloading the update and implementing the Desktop App Installer policy and selecting "Enable App Installer ms-appinstaller protocol".

You can do this via the Group Policy Editor by going to Configuration > Administrative > Templates > Windows Components > Desktop App Installer.

ms-appinstaller misused to spread malware

Since the beginning of December 2021, the Emotet malware has started using Windows AppX Installer packages containing malicious code disguised as Adobe PDF software to infect Windows computers.

Phishing botnets spread emails into reply strings they steal. The phishing email instructs victims to open PDFs designed to look related to the previous chat thread.

However, instead of opening the PDF file, the link will Windows App Installer and ask the user to install "Adobe PDF Component" containing the malicious code. After the victim presses the Install button, the App Installer downloads and installs a malicious apk hosted on Microsoft Azure.