How to avoid dual attack and vulnerable files with double extension? - Blogs on IT, Network, and Cybersecurity

By Seqrite

Archived: 2026-04-05 19:19:13 UTC

The dual extension or double extension is one of the oldest forms of cyber-attacks but continues to be extremely effective. The reason for the continued effectiveness of this type of attack lies in its simplicity.

File extensions are so familiar with us that we don't even give them a second thought. A .doc or a .docx extension is a Microsoft Word document, and .xlsx file is from Microsoft Excel, .ppt/.pptx is from PowerPoint, .jpeg/.gif is an image file and so on. We work with these file formats so much that we hardly spend even a second thinking about them.

A double extension can be hidden in plain sight

It's exactly that familiarity that cybercriminals look to exploit. In Microsoft Windows operating systems, there is an option to "Hide file extensions for known file types" which is turned on by default. Malware writers can use this feature to get unsuspecting users to download files that look genuine but are actually executable.

For example, a file that ends in .exe is an executable file and most email providers will block the download or installation of such a file. A user would also be wary of downloading a .exe file without knowing where it came from. However, a malware actor can easily disguise the extension through a dual extension. The file can be renamed to an official-sounding "Sales Report Q4 FY21". Then, to hide the .exe extension, the file could be given a dual extension like "Sales Report Q4 FY21.doc.exe".

Tricked into running an executable file

Because Windows by default hides known extensions, the file will show to the user as a .doc document without the .exe extension. The user will consider it a Word document and open it, inadvertently downloading malware on their systems. This is exactly how many types of ransomware and malware have spread in the last few years. A good example is the CryptoLocker Ransomware which encrypted files and demanded a hefty ransom if users wanted to recover their files.

It's a very simple method of attack but can be very effective. Even if one user downloads and runs a malware executable, it can easily spread to other systems on the network and shut down the entire enterprise network. Ransomware can spread extremely fast and shut down entire networks.

Cybersecurity 101: Don't open attachments from unknown people

The key method to prevent dual extension attack is to be extremely vigilant about opening files, especially from unknown sources. Users should turn off the option to hide file extensions—this will ensure that the entire file extension can be viewed. While even opening emails from unknown sources is a strict no-no, there's no guarantee

that an email from someone known is safe. They could well be compromised. It should be first nature to check the entire file extension and open it only it seems genuine.

Seqrite's state-of-the-art Endpoint Security (EPS) is equipped with Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS) that proactively detects and prevents malicious activity through known signatures. EPS also has a Ransomware Protection feature which uses Seqrite's behaviour-detection technology to detect and block ransomware threats. Using an updated security solution like EPS is highly recommended for protection against malware attacks such as dual-extension type attacks.
