Issued 2/8/18

Hacker Easily Bypasses Windows 10 Anti-ransomware Protection with this Trick

The Controlled Folder Access (CFA) in Windows 10—which Microsoft promoted as protection against ransomware—can be easily bypassed with the use of 'boobytrapped' Office files, according to work from security researcher Yago Jesus. CFA was added to Windows Defender in the Windows 10 Fall Creators Update in late 2017. Essentially, CFA keeps suspicious apps from augmenting or editing any files stored in a particular protected folder. Normally, a user must approve an app's ability to edit files stored in these protected CFA folders by whitelisting the app, as noted by Bleeping Computer. But Office files are automatically whitelisted, which provides a workaround. "By default, Office executables are included in the whitelist so these programs could make changes in protected folders without restrictions," Jesus wrote in the report. Edit access is granted even to users working with Object Linking & Embedding (OLE) objects, which can programatically drive Office executables. This means that a ransomware developer could modify their software to use OLE objects, allowing them to change, edit, or delete a victim's files without detection. The hacker showed a few examples of Python scripts that could use OLE objects to bypass the CFA folder protections. And that doesn't only affect Office files. "Notice that Office could be used to edit PDF files, Image files and others type of files not strictly related to Office documents," Jesus wrote.