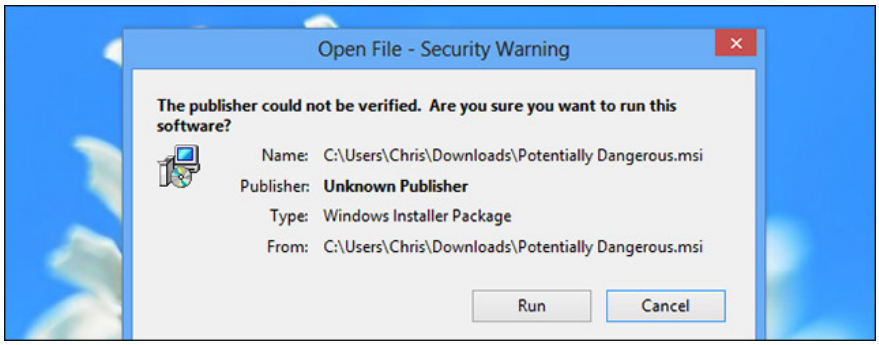
List of some types of files that are potentially dangerous on Windows

Not only does a new .exe file contain security risks for Windows computers, but many other file extensions also carry hidden dangers.

Most people know that files with .exe extensions are potentially dangerous to the system, but not only each .exe contains security risks for Windows computers, but also Many other file extensions also carry hidden dangers.In this article, we will mention the list of file extensions you need to pay attention to (this list may be much longer than you imagine), but first we will work together to clarify some issues.



So why do we need to know which file types are dangerous?

It is important to know which file extensions may contain potential dangers before deciding to open the file.This may be the files that are attached to your email or downloaded from the web and your task is to determine if it is safe enough to open.Even screen saver files can be dangerous on Windows.

When you encounter one of these types of files, you should be more careful to ensure that your system is fully protected.Scan these files with your favorite antivirus software or even upload them to services like VirusTotal to make sure there are no viruses or malware hidden in them.

Why is the file extension capable of indicating hidden dangers?

These file extensions are potentially dangerous because they can contain code or execute arbitrary commands.For example, an .exe file can be dangerous because it is a program that can perform settings on the system (within theUser Account Controlfeature (WindowsUser Account Control). For example, .JPEG files and .MP3 music files are not dangerous because they do not have the ability to contain code (although there are some cases where manually created images contain malicious code or other media files can exploit vulnerabilities in viewer applications, but these cases are rare and patched very quickly).

Overall, it is important that we know what file types can contain code, scripts and other potentially dangerous things.

Below is a list of a file type that is potentially dangerous on Windows:

Program file extensions

.EXE: Program executable files.Most applications running on Windows are .exe files.

.PIF: Program Information File,a file type that contains program information for MS-DOS programs.Although .PIF files do not contain executable code, Windows will still process the .PIF files just as they do for .EXE files if they contain executable code.

.APPLICATION: The application installer is deployed with Microsoft's ClickOnce technology.

.GADGET: A utility file for Windows desktop utility technology that was first introduced in Windows Vista.

.MSI: Microsoft installer file (Windows Installer).These files can be used to install other applications on your computer, although applications can also be installed by .exe files.

.MSP: This is the patch file of the Windows installer.Used to patch applications deployed with .MSI files.

.COM: The type of program file originally used by MS-DOS.

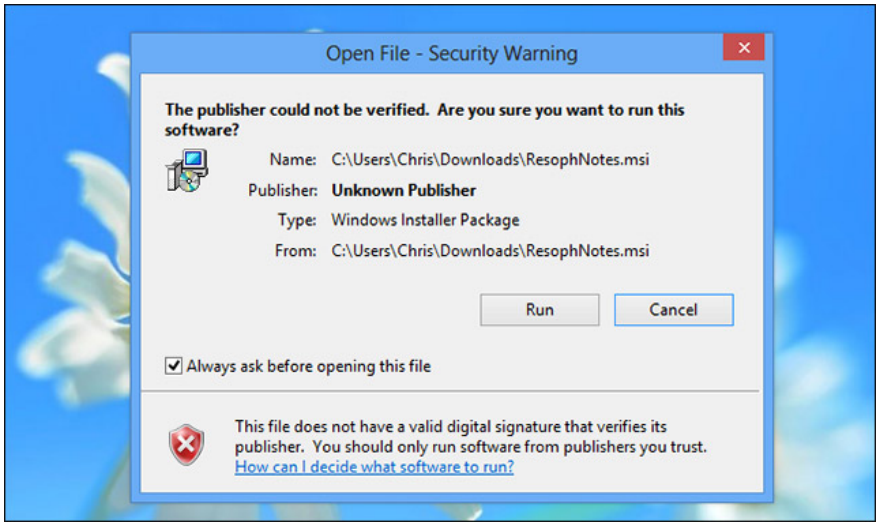
.SCR: File Windows screen saver.Windows screensaver may contain executable code.

.HTA: Is an HTML application.Unlike HTML applications running in the browser, the .HTA files are run as trusted applications without the sandbox.

.CPL: Control Panelfile (Control Panel), including all utilities found in the Windows Control Panel.Double clicking on this file will launch the linked control panel.

.MSC: Microsoft Management Console file.Applications like group policy editor and disk management tool (disk management tool) are .MSC files.

.JAR: .JAR files contain Java executable code.If you have the runtime installed for Java, the .JAR files will be run as programs.



Script file extensions

.BAT: The batch file is a text file containing a series of commands.When starting the batch file these commands will be executed.This type of file was originally used by MS-DOS.

.CMD: An executable file type.Similar to .BAT, but this file extension was introduced from Windows NT.

.VB, .VBS: A VBScript file.This file will execute the attached VBScript code if you run it.

.VBE: A type of VBScript file that is encrypted.Similar to a VBScript file, but it is not easy to determine what the file will actually do when you run it.

.JS: JavaScript file..JS files are often used by websites, they are completely safe if they are run on Web browsers.However, Windows will run .JS files outside of the browser without the sandbox.

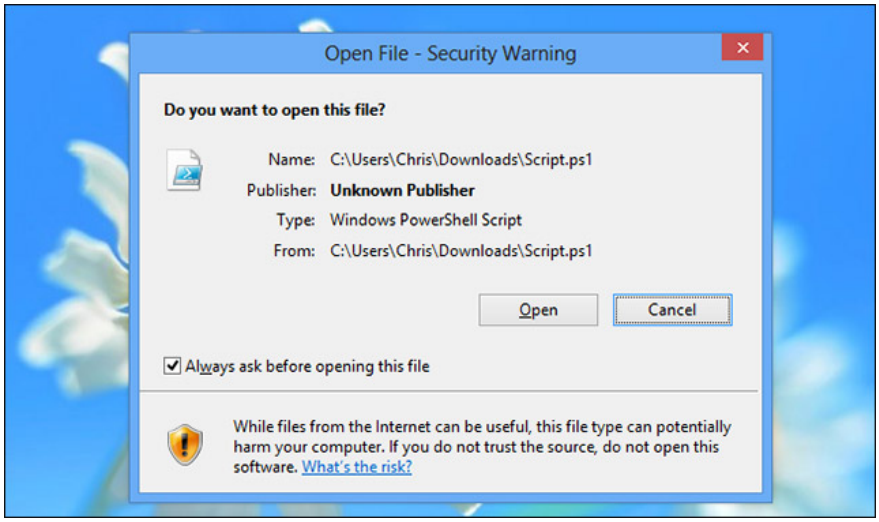
.JSE: Encrypted JavaScript file.

.WS, .WSF: Windows Script File.

.WSC, .WSH: Windows Script Component files and Windows Script Host, they are used together with Windows Script files.

.PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2: Windows PowerShell script files.The task is to run the PowerShell command in the order specified in the file.

.MSH, .MSH1, .MSH2, .MSHXML, .MSH1XML, .MSH2XML: Monad script files.Monad is then renamed to PowerShell.



The extension c file shortcut

.SCF: Windows Explorer command file.Can infect potentially dangerous commands for Windows Explorer.

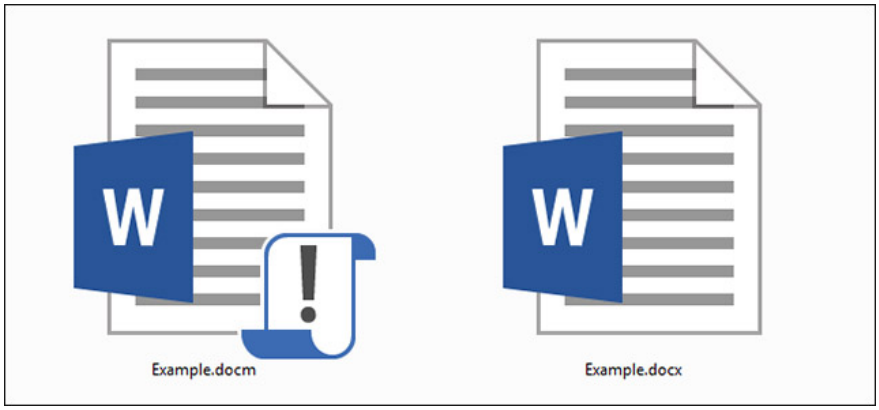
.LNK: File has not yet linked to a program on your computer.These linked files may contain command line attributes for malicious content, such as deleting files without first asking.

.INF: A type of text file used by AutoRun.If run these files are capable of launching dangerous applications that come with it or infecting dangerous options for programs in Windows.

Other file types extensions

.REG: The Windows Registry file is a file that can be used to make modifications to the Windows Registry.The .REG files contain a list of registry entries that will be added or deleted if you run them.Malicious .REG file can delete important information.You should never double click on these files unless you are sure what you are doing.

Extensions of office application files and text files



.DOC, .XLS, .PPT: Microsoft Word, Excel and PowerPoint document files.They may contain malicious macro codes.

.DOCM, .DOTM, .XLSM, .XLTM, .XLAM, .PPTM, .POTM, .PPAM, .PPSM, .SLDM: These are the new file extensions introduced in Office 2007. The M character at the end File extension indicates documents containing Macro.For example, the .DOCX file does not contain macros, while the .DOCM file may contain macros.

summary

This is not a complete list of file extensions that can hide malicious code.There are other types of file extensions - like .PDF, that have been involved in scandals about security incidents.However, for most of the above files, paying more attention to them is what you should do because these files exist to run arbitrary code or commands on your computer.

See more:

1. What is file extension?
2. What is sandboxing and how to sandbox a program?
3. Website synthesis of file formats
4. 8 ways to identify strange format files