Why don't the file timestamps on an extracted file match the ones stored in the ZIP file?

devblogs.microsoft.com/oldnewthing/20110504-00

May 4, 2011

Raymond Chen

A customer liaison had the following question:

> My customer has ZIP files stored on a remote server being accessed from a machine running Windows Server 2003 and Internet Explorer Enhanced Security Configuration. When we extract files from the ZIP file, the last-modified time is set to the current time rather than the time specified in the ZIP file. The problem goes away if we disable Enhanced Security Configuration or if we add the remote server to our Trusted Sites list. We think the reason is that if the file is in a non-trusted zone, the ZIP file is copied to a temporary location and is extracted from there, and somehow the date information is lost. The customer is reluctant to turn off Enhanced Security Configuration (which is understandable) and doesn't want to add the server as a trusted site (somewhat less understandable). Their questions are
>
> - Why is the time stamp changed during the extract? If we copy the ZIP file locally and extract from there, the time stamp is preserved.
> - Why does being in an untrusted zone affect the behavior?
> - How can we avoid this behavior without having to disable Enhanced Security Configuration or adding the server as a trusted site?

The customer has an interesting theory (that the ZIP file is copied locally) but it's the wrong theory. After all, copying the ZIP file locally doesn't modify the timestamps stored inside it. Since the ZIP file is on an untrusted source, a zone identifier is being applied to the extracted file to indicate that the resulting file is not trustworthy. This permits Explorer to display a dialog box that says "Do you want to run this file? It was downloaded from the Internet, and bad guys hang out there, bad guys who try to give you candy." And that's why the last-modified time is the current date: Applying the zone identifier to the extracted file modifies its last-modified time, since the file on disk is not identical to the one in the ZIP file. (The one on disk has the "Oh no, this file came from a stranger with candy!" label on it.) The recommended solution is to add the server containing trusted ZIP files to your trusted sites list. Since the customer is reluctant to do this (for unspecified reasons), there are some other alternatives, though they are considerably riskier. (These alternatives are spelled out in KB article 883260: Description of how the Attachment Manager works.) You can disable the saving of zone information from the Group Policy Editor, under Administrative Templates, Windows Components, Attachment Manager, *Do not preserve zone information in file attachments*. This does mean that users will not be warned when they attempt to use a file downloaded from an untrusted source, so you have to trust your users not to execute that random executable they downloaded from some untrusted corner of the Internet. You can use the *Inclusion list for low, moderate, and high risk file types* policy to add ZIP as a low-risk file type. This is not quite as drastic as suppressing zone information for all files, but it means that users who fall for the “Please unpack the attached ZIP file and open the XYZ icon” trick will not receive a “Do you want to eat this candy that a stranger gave to you?” warning prompt before they get pwned.

But like I said, it’s probably best to add just the server containing the trusted ZIP files to your trusted sites list. If the server contains both trusted and untrusted data (maybe that’s why the customer doesn’t want to put it on the trusted sites list), then you need to separate the trusted data from the untrusted data and put only the trusted server’s name in your trusted sites list.

Raymond Chen

Follow