The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- What is Metadata?
- Identifying & Removing Metadata
- Protecting Yourself

Metadata

GUEST EDITOR

James Tarala is the guest editor for this issue. He is a senior instructor with the SANS Institute and a principal consultant with Enclave Security (www.enclavesecurity.com). He is also the author of numerous SANS training courses, including SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls and SANS Audit 407: Foundations of Auditing Information Systems.

OVERVIEW

Every day computer users share photos, word processing documents, spreadsheets, presentations, audio clips, and other types of digital files with people around the world. What you may not know is that these files may inadvertently include private or sensitive information about you or your organization in the form of metadata. To help you maintain both your privacy and security, we will explain what metadata is, how you can find and remove it, and some steps to take to protect yourself.

WHAT IS METADATA?

Metadata is data that defines or describes another piece of data. Metadata by itself is not evil, but it may reveal more about you, your organization, or your devices than you realize. Many devices, such as your computer, camera, or smartphone, automatically embed metadata in any digital files they create. In addition, most software programs or file formats include placeholders or standards for specific types of metadata. A common example is Microsoft Word, which by default is likely to include information about the author, the date when the document was created, and any embedded comments or revisions. Some examples of metadata include:

- File creation date and time
- The address or geographic location where the file was created
- Your name, your organization's name, and your computer's name or IP address
- The names of any contributors to the document or comments they have inserted

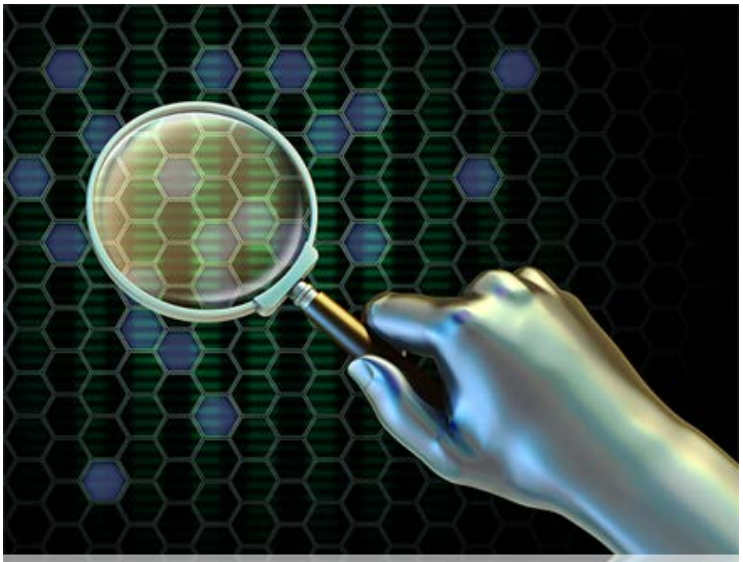
Metadata

- Type of camera you are using and its settings when the photo was taken
- Type of audio or video recording device you are using and its settings when a recording was taken
- Make, model, and service provider of your smartphone

IDENTIFYING AND REMOVING METADATA

Unfortunately, many devices and software make it difficult to remove metadata from the files they create or edit. Many times the metadata is embedded in places that are not easy to reach by ordinary computer users. One common way to view and remove metadata on a Windows computer for any file you are working with is to right-click on the file, and then view its *Properties*. From there, you can remove the metadata by selecting the *Details* tab and clicking on *Remove Properties and Personal Information*. Another way to view metadata is to open the file in special applications. For example, the Mac OS X application Preview can show you the metadata of any photo you open.

Some applications include tools specifically for removing metadata. For example, Microsoft Office 2007 and 2010 come with a built-in tool called Document Inspector which will identify metadata in an Office document and give you the option of selectively removing some or all of it. While Microsoft Office for Mac does not have this tool, it does give you the ability to remove metadata from an Office document by going into Preferences/Security/Privacy and selecting Remove personal information from this file on save. Finally, there are a variety of both open source and commercial applications designed to identify and edit or remove metadata in files.



Metadata is not evil, but it may reveal more than you planned. Check before sharing your digital files.

PROTECTING YOURSELF

Much of this metadata by itself may not be damaging. In fact you may deliberately make metadata freely available, such as embedding your name in an image for copyright purposes. However, especially when dealing with sensitive or confidential pieces of information, you should be aware of the metadata that you are revealing to others. When you create a file that includes metadata, there is no telling where that information might find itself in the future. Therefore, some best practices for dealing with metadata include:

Metadata

1. Consider saving the file in a format that does not store or has very limited metadata. For example, instead of sharing a Word document, convert the document into .rtf or .txt file format. For images, use the PNG file format instead of JPEG images.
2. Consider running a metadata cleaner, such as Microsoft Office's Document Inspector or special software tools designed to identify and remove metadata.
3. Check the preferences or settings for any application or device you are using. You may be able to limit the amount of metadata they store by changing the default configuration options. For example, you can disable geo-location tracking for your smartphone camera.
4. Before you send or post a file, consider the impact if the file contains metadata . This is especially true when posting files such as photos or videos to social networking sites, like Flickr, Twitter, or Facebook.

By following these simple steps, you can help to ensure that only information you intend to share with others is actually shared. Private data should stay private.

RESOURCES

Some of the links shown below have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Document Inspector : http://preview.tinyurl.com/3996c2a

EXIF Metadata Explanation:
http://preview.tinyurl.com/775mbxc

Free Metadata Extraction Tool:
http://meta-extractor.sourceforge.net
or http://preview.tinyurl.com/aueb4

Disabling Geo-location for Smartphone Cameras
http://preview.tinyurl.com/3v4xznm

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org

OUCH! is published by the SANS Securing The Human program and is distributed under the Creative Commons BY-NC-ND 3.0 license. Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Cara Mueller

© The SANS Institute 2012