

FCW Makes Hidden Data Front Page News

The cover story in today's Federal Computer Week makes hidden data in electronic documents front page news. Michael Arnone gives a good top-level description of the hidden data threat in his story called, "Accidental Publicist." The article appears in both the print edition and the online edition.

We would like to expand on a couple of issues mentioned in this article. Michael mentions that experts disagree on how well Microsoft's Remove Hidden Data (RHD) plug-in works, and there is a statement that the RHD Plug-in removes Tracked Changes data from PowerPoint. SRS has demonstrated many times that Microsoft's RHD plug-in fails to remove Tracked Changes from PowerPoint documents, and there are a lot of other hidden data types that are not removed by the RHD plug-in.

The Microsoft representative quoted in this article claims that all users can terminate an Ad Hoc Review by using the Reviewing toolbar under the Tools menu. This is not correct. Neither the "End Review" button nor the Tracked Changes in PowerPoint are visible to anyone other than the originator of the review. You can look at the Reviewing pane as mentioned in the article, but nothing will show up. Similar problems have been observed in Word and Excel.

In the article, Microsoft admits that there are problems with the Ad Hoc Review, and they indicate it will be removed from Office 2007, which is currently scheduled for release in January. This is a good first step, but that will not fix the problem. There are already a large number of documents in circulation with the Ad Hoc Review enabled. Many more Ad Hoc Reviews will be triggered before Office 2007 is available to the public. Not everyone will upgrade to the new Office when it is released, and even if they did, there is no evidence that Office 2007 can stop reviews already in progress. None of the security features added in recent editions (i.e. "Remove personal information on file save," Compress Pictures, and RHD Plug-in) have worked well or addressed the depth of the hidden data threat.

<http://www.fcw.com/article93983-04-10-06-Print>

Center for Army Lessons Learned Using Document Detective

The Center for Army Lessons Learned (CALL) at Fort Leavenworth, Kansas receives sensitive information from around the world that it must quickly convert into instructional materials for military personnel. Their pressing need to transfer documents in native format, especially Microsoft PowerPoint, led them to try our Document Detective software. With the approval of US Army NETCOM, CALL began using Document Detective in June 2006. Dan Cindrich, a security specialist for CALL,

discussed the results of this successful pilot program with Ann Bednarz in a Network World magazine article. You can read this article yourself at:

<http://www.networkworld.com/news/2006/032106-srs-document-detective.html>

Washington Post Meta Data Incident Exposes Source

The Washington Post published an article recently about an interview with a 21-year-old hacker who admits he hacked into thousands of personal computers and turned them into 'bots.' The article described the hacker's physical attributes, but stopped short of providing information that would directly identify this source or his location. Unfortunately for the Washington Post, the Meta data contained in a picture included with the original article identified his location as a small town in Oklahoma. The town has a population of a few thousand people, which would make it fairly easy to find this individual when combined with the other information in the article. The photograph was removed from the Washington Post website shortly after the Meta data issue was announced by Slashdot. The Meta data from the photo, which is available at Slashdot, appears below:

SLUG: mag/hacker

DATE: 12/19/2005

PHOTOGRAPHER: Sarah L. Voisin/TWP

id#: LOCATION: Roland, OK

CAPTION:

PICTURED: Canon Canon EOS 20D

Adobe Photoshop CS2 Macintosh 2006:02:16 15:44:49 Sarah L. Voisin

<http://it.slashdot.org/comments.pl?sid=177830&cid=14748871>

<http://www.eweek.com/article2/0%2C1895%2C1930342%2C00.asp>

Many people know about Meta data in Office documents, but many people may not be aware that Meta data can be found in many electronic files, including images. Some of this information is added automatically by the equipment and the software application used to process the file. Other information can be added by the user to identify the file for later use. Embedding these files into other files, such as Microsoft Office documents, does not alter the original data. This results in second level Meta data that is ignored by most commercial Meta data cleaners.

The document flatteners in the SRS Document Detective toolbars can remove second level Meta data from an electronic document. This information is automatically removed when the Document Detective flatteners compress a picture. Microsoft Office added a compress pictures feature beginning with Office XP, but that feature may not work for all of the images in a document. Only the Document Detective flattener can

successfully remove second level Meta data from all images and other embedded files in Microsoft Office documents.

Bitform Finds Hidden Data in Fortune 100 Survey

Bitform recently surveyed the public Office documents of the Fortune 100 companies and published their report to the Internet. They found over 8000 Word, PowerPoint and Excel documents. One of the categories of information they reported was called "Outlook Properties." Based on the description of Outlook Properties, we realized they were talking about one of the tell tale signatures of the Ad Hoc Review. Therefore, based on the Bitform report, we can conclude that nearly one in five documents in this survey (17.1%) are in an Ad Hoc Review cycle. This means that these documents are actively tracking changes. It also shows how most experts in the field of "Meta data" are unaware of the Ad Hoc Review.

These results closely parallel a similar survey that we conducted of Word documents on the White House website in December 2005. The Whitehouse had just suffered several embarrassing "Tracked Changes" incidents, and we wanted to know how extensive the problem was. We used Google's advanced search feature to locate and download all of the Word documents from www.whitehouse.gov. Nearly a third (29%) of those documents were in an Ad Hoc Review. That means that at least 29% of the Word documents on the White House website could contain Tracked Changes. The Tracked Changes feature is automatically enabled by the Ad Hoc Review feature. The Ad Hoc Review tags are removed when the review cycle is complete, but that does not automatically remove the Tracked Changes data. It is also possible to enable Tracked Changes without enabling the Ad Hoc Review, so the actual incidence of Tracked Changes in White House documents could be even higher.

Bitform reported that 6.5% of the documents contained Tracked Changes, but they only checked Word and Excel documents for this condition. Like most people, Bitform is not aware that PowerPoint has a Tracked Changes feature. We can probably assume that PowerPoint has about the same incident rate as Word and Excel. The actual number of documents with Tracked Changes is not necessarily equal to the number of documents in an Ad Hoc Review. In some cases, the Ad Hoc Review is enabled, but no changes have been made to the document. In this case, there will be no Tracked Changes. It is also possible to enable Tracked Changes without enabling an Ad Hoc Review, but you can not enable an Ad Hoc Review without enabling Tracked Changes.

The Bitform survey also reported that 24.8% of the documents contained embedded objects. This is probably low because of the way they defined an embedded object. They did not account for pictures inserted using the Insert --> Picture --> method or other types of objects that are not created using the Insert --> Object method.

The report is not dated, but the Meta data in the PDF shows that it was last modified on 29 Nov 2005. Obtain a copy of that report from the following URL:

<http://www.bitform.net/products/f100/>

Document Detective Version 2.0 Released

SRS Officially announced the release of Document Detective version 2.0 on 20 March 2006. After nearly a year in the field, version 1.0 had proven to be reliable and robust. With the many improvements added to the software, SRS decided to designate the new software as version 2.0.

PDF review capability was improved significantly in version 2.0, and users can now recover deleted text and pages from PDF documents. Deleted pages and deleted text occur when the PDF document is edited in its PDF form after it has been converted from another application, like Microsoft Word. Neither the recent NSA guidance on redaction or the official DOD policy on public release procedures mentions this vulnerability.

The Word flattener feature of Document Detective was also improved for version 2.0. The flattener used in version 1.0 software was based on Government recommended procedures endorsed by NSA. While this procedure successfully removed Meta data, Tracked Changes and Macros, it also removed a lot of extended document formatting. As a result, users needed to spend a lot of time reformatting the document after flattening it. SRS developed new procedures that remove the undesirable information while leaving the document format intact for version 2.0.

Even with the flattener improvements, there could still be some formatting problems. Security is paramount, and occasionally the flattening process does alter the look of a document, so we added a side-by-side review capability to version 2.0. Displaying the flattened document beside the original document makes it easy to detect and to correct any problems caused by the flattening process.

The press release announcing Document Detective version 2.0 and an article by Grant Gross in Info World Magazine are available at the following URLs.

http://www.freshnews.com/news/orange-county/article_30589.html

http://www.infoworld.com/article/06/03/20/76614_HNdocumentcleaning_1.html?source=NLC-TB2006-03-20

SRS Technologies is committed to continuing research and product development. While no process or procedure is perfect, Document Detective is the best available solution for reviewing and sanitizing electronic documents, especially when National Security Information is at stake.

Please feel free to forward this message to anyone you believe would benefit from this information.

This newsletter is dedicated to raising awareness about the Desktop Publishing Threat to Information Security and to disseminating information that will help mitigate these risks. Our newsletter is published aperiodically when there is news to report. We will not clutter your inbox with idle chatter when there is nothing significant or useful to say. This newsletter is available free of charge. Subscriptions are at the discretion of SRS Technologies.

Suggestions and comments are always welcome. If you do not wish to receive this newsletter, please e-mail us and we will gladly remove you from the list. All EDS-related correspondence should be sent to rhackett@stg.srs.com

For a list of articles and information regarding EDS, including previous editions of this newsletter, please visit:
<http://www.stg.srs.com/eds/>

For information about Document Detective electronic document review and sanitization toolkit, please visit:
<http://www.docdet.com/>

To subscribe or unsubscribe from this newsletter, send email to:
rhackett@stg.srs.com

SRS Technologies
Systems Technology Group
500 Discovery Drive
Huntsville, AL 35806
Copyright 2006 SRS Technologies