

## **Microsoft Is a Victim of Their Own Product**

Michal Zalewski has written a very interesting report on his analysis of revision data found in Microsoft Word documents collected from Microsoft's website by using a automated spider. The following is quoted from Zalewski's article:

“I happened to be browsing aimlessly through case studies and other publications released by Microsoft as a part of their ‘Get the facts’ initiative. At one point, I stumbled upon a Word file I wanted to read - and as soon as I ran it through wvWare, I noticed there is a good deal of amusing change tracking information still recorded within the document. Naturally, publishing documents with ‘collaboration’ data is not unheard of in the corporate world, but the fact Microsoft had become a victim of their own technology, and had failed to run their own tools against these publications makes it more entertaining. On a more serious note, it serves as a good warning it is really difficult to manage this, and that inline filtering tools on SMTP gateways and in web publishing systems may be necessary in some corporate environments.”

The statistics are alarming. Mr. Zalewski collected approximately 10,000 unique Word documents from Microsoft. Ten percent of those documents contained revision data, and 5% of those documents contained deleted text. That's approximately 500 potential security compromises. Revision data and Meta data are supposedly well known problems, yet they are still commonly overlooked. Those of you who have seen my presentation and read my report know the problem is much more extensive. You also know the problem is not limited to Microsoft documents. All electronic documents, including text based formats like HTML and XML, can contain hidden data. Think about how many documents your organization is “sharing.” This is also the second article I have seen that talks about using automated methods (spiders and search engines) for collecting this data.

This article implies that Microsoft's Remove Hidden Data (RHD) plug-in will fix the problem. The RHD plug-in will remove the revision data from Word, but there are many more serious problems that the RHD plug-in does not fix. There are other commercial tools available, but they are also limited and will not meet Government standards for reviewing and sanitizing electronic documents that could possibly contain National Security Information. The article also suggests that filtering tools and gateways are a potential solution, but again, they will not meet Government standards. Even guard technology, a gateway designed to mediate communications between different security domains, is inadequate for the task. The SRS tools are being designed to meet rigorous Government standards, and they could be available soon with Government support. Contact us for more information.

Please feel free to forward this message to other Government personnel you believe would benefit from this information.

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 to Government personnel and to certain contractors responsible for the generation and protection of National Security Information. Contractor 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](mailto:rhackett@stg.srs.com).

For a list of articles and information regarding EDS, please visit our web page: <http://www.stg.srs.com/eds>.

To subscribe or unsubscribe from this newsletter, send email to: [rhackett@stg.srs.com](mailto:rhackett@stg.srs.com)

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

Copyright 2004 SRS Technologies