

## Security Review of DidTheyReadIt.com

by: Rob Slade, 08/24/2004

<http://www.securitydocs.com/library/2467>

DidTheyReadIt is a new service on the net. It has garnered some attention from the privacy community already: I will deal with some of that later. I would like to examine the actual operations of the service. The discussion surrounding it has been marked by assumptions and lack of knowledge. Some assertions have been made that are at odds with the actual operations. DidTheyReadIt is both less, and more, dangerous than has been made out.

As the name implies, it provides a kind of "return receipt" for email. It does this, of course, using Web bugs. A "single pixel" image file is called from the central host, using a hash that presumably corresponds to the sender, subject, and receiver, looking like the following:

```
img src="http://didtheyreadit.com/b906148b2edfdab9e7de03a23f59687eworker.jpg" width="1"  
height="1" /
```

(I have removed the surrounding angle brackets: hopefully this will prevent any mailers from trying to render the HTML.)

Having obtained an account from DidTheyReadIt (and paid for the privilege), there are two ways to use the service.

### **RISK 1**

If you have WinXP or W2K (and a "standard" mailer) you can run a background program on your computer. I have downloaded the installation program and made a cursory examination of it, but I have strong reservations about actually running it on my system. One can assume that the process runs in the background, adds the Web bugs to outgoing email traffic, and sends information to the central computer. However, even a brief analysis of the code indicates it can do more than that. Among other things it calls the kernel, uses the Registry, and obtains information on privileges within your system. These may be valid activities within the context of the operation of the program, but, given what the program must be doing, what else is it doing? There is a significant possibility for information leakage here.

### **RISK 2**

You can use the program without running the background process. To do this, you append "didtheyreadit.com" to the email address. If I wanted to send a message to my rslade@isc2.org address, I would send it to rslade@isc2.org.didtheyreadit.com. The central computer then reformats the email in HTML and adds the Web bug. In this way, obviously, DidTheyReadIt gets to read all the email I send.

When email is opened using a mailer that automatically calls for information from the Web, the URL is requested, and the central computer has confirmation that the individual actually read the email. DidTheyReadIt promises that they can tell you how long the email remained open. (In the tests that I've done so far this information has been available in slightly under half of the cases.)

(When the URL is requested, a series of packets each containing a single byte is sent. Lauren Weinstein [see below] has noted that this may be the way the Rampell measures how long the message remains open. In tests the file transfer time seems to vary, but has always been shorter than the longest time that I've been "informed" a message has remained open. Others have theorized that the material transferred may be scripting that remains active as long as the message is open, passing information back to

Rampell. This does not seem to be the case. When downloaded manually, the file is 302 bytes, has the internal structure of a JPEG file, and displays as a one [or possibly two] pixel black dot. A refresh tag could be used, but this has been observed neither in the coding seen nor the activity of browsers. At this point I don't know what the basis of the "read duration" is.)

### **RISK 3**

The central computer actually has rather a lot of information from that URL request. There is information about the time it was opened. There is purported information about the location and organization, but this is obviously obtained from a whois lookup from the IP address. There is information about the browser application, and the language used. In the case of Windows software running under emulation on a non-Windows system, there was enough information to indicate that this was so.

### **RISK 4**

The amount of information that DidTheyReadIt could build up is quite staggering. As well as simple lists of valid email addresses, they can tie address information to browsers and other applications, and the language of the user. They can, of course, build maps of connections between correspondents. The hash seems to also be linked to the subject line, so that even if email is not being sent through the central computer itself a database of topics and interests can be built. I'm rather surprised that Rampell Software (the company behind DidTheyReadIt) is even trying to sell their service: make it free, get the masses on board, and they have a gold mine of marketing information.

Rampell is presumably well aware of the marketing possibilities. Each and every confirmation message from them carries at least two marketing messages: one pushing you to buy an upgrade to the version you have, and another promoting some other Rampell product.

The system is not perfect, of course: send a message to me and you will probably not get acknowledgement that I read it, since my mailer does not (automatically) render HTML and go to the Web. However, prevailing upon some friends with more "standard" mailers, such as Outlook and Eudora, the system does seem to work (at least partially) with a wide variety of systems, including Macs, and Macs running Outlook under PC emulation. Cookie filters that prevent you from going to an "outside" site might limit the susceptibility of Web based mail systems, but otherwise these should all return the tracking URL.

The system has interesting limitations with regard to mailing lists, and copies. When sent to a mailing list, and even to a number of people copied on the "To:" and "Cc:" lines, only one hash is generated. Although the confirmation message from Rampell mentions the possibility of further confirmations whenever someone subsequently reads the message, in testing that does not appear to happen. Each hash appears to be good for one use, and one use only. Sending a message to a mailing list gets you a response from the first person (or the first \*susceptible\* person) to read it.

As noted at the beginning, there has already been some interest in the system and the privacy considerations. There have been two mentions of the system in the RISKS-FORUM Digest.

<http://catless.ncl.ac.uk/Risks/23.41.html#subj2>

In the first, Lauren Weinstein gave a reasonable account of the system and the potential problems, noting the possible solutions. The use of text-only email is the best solution, and blocking the Rampell server would work as well. Turning off image display may alleviate privacy problems, but that does depend upon how different applications handle that option. Some may submit the URL to the Rampell server, and simply not display the image.

<http://catless.ncl.ac.uk/Risks/23.44.html#subj11>

A second posting noted that DidTheyReadIt is illegal in France, and speculated that travellers to France might find themselves in legal trouble if they were subscribers. In practical terms, having the Rampell software installed on your system could be evidence against you. In which case, using the modified email addresses would leave you free and clear, so long as you didn't send any modified mail while in France. France might, of course, want to block Rampell's IP addresses.

A marketing consultant did an article on the errors that Rampell made in promoting the service. He suggested that an opt-out approach or option would have avoided the bad press. Unfortunately, this demonstrates that he doesn't understand how the system or the technology works. As Weinstein's analysis indicated, you have to change your software, or have some backend support, in order to prevent detection.

It is, of course, quite possible that Rampell has only the purest of motives in providing the service, and would never consider using the information obtained by providing it. I would not dare to impugn the integrity of the company or its principles and principals. However, I would note that historically:

- a certain delivery company stated that it would never sell the database of digitized signatures collected when it started using electronic pads--and then, some years later, did exactly that.
- companies with very rigorous privacy policies, having collected significant amounts of personal customer data, have gone bankrupt, and the files have been offered for sale.
- it has, sadly, been known to happen that evil intruders have broken into companies and stolen personal information from computerized files--or even planted backdoors and logging/reporting software in their systems.