

From Tech Night Owl Newsletter

THE TIGER REPORT: THE GREAT DASHBOARD WIDGET FLAP

The possibility of security leaks in Mac OS X has been bubbling under the surface for a while, but it's now poised for a major flare up. Sure, Apple has released security updates from time to time, and I suppose the things the updates fix could, conceivably, cause grief if some Internet criminals decided to exploit them. The same holds true for those "proof of concept" computer viruses that have caused some of the companies that produce virus prevention software to raise warning flags.

The latest alleged threat comes from a Mac OS X feature that's supposed to make your computing experience more pleasurable. I'm talking about Dashboard, the component of Tiger that dims your screen and displays little applications, or widgets, designed to provide simple functions. Some deliver eye candy, such as dancing figures, while others serve more functional purposes, such as displaying TV listings, package tracking information, the day's weather, stock prices and other goodies.

While some are upset with Apple for producing something that so closely resembles a third party utility, Konfabulator, Dashboard should still stand or fall on its own merits. In fact, if there's anything in the Classic Mac OS that might resemble a widget, take a look at the original desk accessories. Like widgets, they were tiny single-purpose applications. In fact, up till recently I used one of those desk accessories, Easy Envelopes+, to process my envelopes. I have since switched to a Mac OS X alternative, Addressix, but I always have the hope in the back of my mind that Andrew Welch of Ambrosia Software will take the time to update Easy Envelopes+.

In any case, the real fear being raised by some is that the widgets might represent a heavy duty security risk, and that you should proceed with the utmost caution.

So, you may ask, what could a tiny application do to harm your Mac? Well, the theory goes that one of these widgets might seem to have a useful or entertaining function, but hide malicious code that could invade Mac OS X. You see, widgets directly access such system resources as Java and Apple's WebKit, and I can see at potential for mischief, although the reality argues against the fear mongers. The furor erupted when it was discovered that the original Tiger version of Safari could download a widget and install it without your express approval. That definitely seemed a recipe for trouble.

In its 10.4.1 update, Apple took the hint and revised Safari so that it would put up the same warning presented when you download an application. You have to click Download to finish the process. However, Safari will still install the widget after you give the OK, behind the scenes. You will not see any visible evidence of what's happening, but the widget is decompressed and placed in your Users/Library/Widgets folder. Other browsers leave the things on your desktop, leaving you to figure out where they're supposed to go.

Now I'm not going to take Apple to task for not providing a more user friendly method to install widgets by yourself, but I'm sorely tempted. In addition, you could, in the course of downloading lots of stuff, click the Download button without thinking, after which it's too late.

Or is it?

There's an article at CNET's News.Com

<http://news.com.com/Widget+security+worries+dog+Apple/2100-1002_3-

5715752.html?tag=nefd.hed> that claims Apple hasn't gone far enough to ensure safe use of widgets. Understand that real journalists have always been told to check and recheck a story. Mainstream newspapers generally require that you verify a story by contacting at least two sources. Clearly CNET's Joris Evers doesn't hold to such standards, for the only viewpoint mentioned in the article comes from Jonathan Zdziarski, a software engineer.

In the article, Zdziarski reportedly claims that "A malicious widget, after it is installed, can run in the background and wait until a time when the user logs in as administrator." Now before you go and dump all your widgets before they can cause any damage, pay closer attention to that claim, that a widget "can run in the background." Evidently neither Zdziarski nor CNET's reporter understands how you run or execute a widget.

Like any application, a widget has to be launched before it does anything. You do that by, naturally, clicking once on an icon in Dashboard's version of the Dock, or by double clicking the widget itself.

In other words, the widget won't actually do anything until you launch it. Don't believe me? Take a look at the Activity Viewer in Tiger's Utilities folder and see what's happening. The only widgets listed are the ones that have actually opened, the ones that appear when you press F12 to activate Dashboard. Do you see where I'm going?

There are thousands of Mac OS X applications out there. Some are designed to execute Unix command line instructions in the background to begin maintenance functions or change the look and feel of your Mac OS X desktop. Now if a using a widget can be risky, what about these other applications? Couldn't they represent even greater potential risks? Yes, most require that you enter your administrator's password to install the application, or allow a system process to run. But how many of you actually think first before entering that password? More than likely, you're so used to responding to those dialog boxes that you type your password with your mind on automatic pilot.

The real answer to potential security threats is not to raise unnecessary alarms. The truth is that any application you install on your Mac could be a Trojan Horse that masquerades as a useful utility, while doing its damage without your knowledge. It doesn't seem logical to just off half cocked and cry wolf. Instead, you should always download software from trusted sources. If you get a widget from Apple, you can depend on the fact that it's been checked before being posted. You can also feel confident in downloading a file from a software publisher or one of those well-known software update sites. Downloading stuff from a peer-to-peer network courtesy of Bit Torrent or a similar application represents the real risk. Do you really want the safety of your Mac to depend on sources you don't know?

In the end, the best route to safe computing is caution. Think about what you're downloading before you click that button to retrieve a file. Take a deep breath before you respond to a password prompt. Make sure what you're installing comes from a trusted source and you'll go a long way towards keeping your Mac safe and sound.