

Malicious Bundles on Mac OS X

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-06/0024.html>

From: Braden Thomas (braden127_at_myrealbox.com)

Date: 06/05/05

To: bugtraq@securityfocus.com

Date: Sat, 4 Jun 2005 19:21:57 -0400

I wrote some information about Malicious Bundles on Mac OS X and posted source code that you can find here:

<http://braden.machacking.net/bundle.html>

The InputManagers directory on OS X gives the user the ability to load any bundle into any application. The Obj-C runtime environment gives code the ability to dynamically change the mapping of any function at runtime. The combination of these two allows a bundle to modify the behavior of any application launched by a user. This fact is nothing new -- people have been discussing this for a while, and other people have been using this functionality to write neat software that modifies other software.

On the page, I have some proof-of-concept code that demonstrates the danger of the InputManagers directory: a malicious bundle called mailHack that automatically adds itself (or any file) to every email sent using Mail.app; a malicious bundle called iChatHack that automatically sends itself (or any file) to every online user using iChat.app.

I briefly discuss malicious bundles as a vector for spyware and viruses.

Braden

- application/applefile attachment: [viruspackage](#)