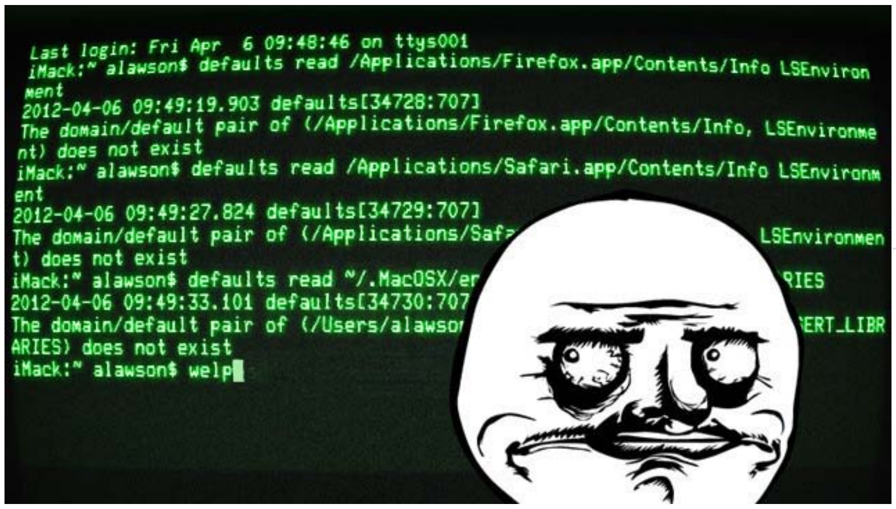
http://arstechnica.com/apple/news/2012/04/how-to-check-forand-get-rid-ofa-mac-flashback-infection.ars

How to check for—and get rid of—a Mac Flashback infection

By Jacqui Cheng | Published 18 days ago



```
Last login: Fri Apr  6 09:48:46 on ttys001
iMack:~ alawson$ defaults read /Applications/Firefox.app/Contents/Info LSEnviron
ment
2012-04-06 09:49:19.903 defaults[34728:707]
The domain/default pair of (/Applications/Firefox.app/Contents/Info, LSEnvironme
nt) does not exist
iMack:~ alawson$ defaults read /Applications/Safari.app/Contents/Info LSEnvironm
ent
2012-04-06 09:49:27.824 defaults[34729:707]
The domain/default pair of (/Applications/Safa                         LSEnvironmen
t) does not exist
iMack:~ alawson$ defaults read ~/.MacOSX/er                            RIES
2012-04-06 09:49:33.101 defaults[34730:707
The domain/default pair of (/Users/alawsor                             ERT_LIBR
ARIES) does not exist
iMack:~ alawson$ welp
```

Here's hoping you get nothing but a series of "does not exist" responses!

So you're a Mac user who has heard that more than half a million Macs have been infected by the recent Flashback malware. When the news began to spread about how the malware took advantage of a previously unpatched Java vulnerability on the Mac, the the horror stories began pouring in. "My dad heard about the Flashback malware and subsequently deleted his Java folder. Now his Mac won't boot," a friend told me.

Needless to say, this is not the way to properly nuke a possible Flashback infection or prevent yourself from catching one. Still, there is a reasonable level of concern out there. Maybe you haven't been keeping up on your antivirus software (and let's be honest, most Mac users don't), or perhaps you simply have suspicions about your Mac acting funny. How do you check if you have Flashback, and if you do, how do you (properly) get rid of it?

Head to the Terminal to check for infection

These Terminal commands will give you an easy way to find out whether you have a possible Flashback infection.

First, launch Terminal from /Applications/Utilities on your Mac. Then individually type or paste these three lines into the Terminal:

```
defaults read ~/.MacOSX/environment DYLD_INSERT_LIBRARIES

defaults read /Applications/Safari.app/Contents/Info LSEnvironment

defaults read /Applications/Firefox.app/Contents/Info LSEnvironment
```

If the Terminal returns back to you lines that look like this:

```
The domain/default pair of (/Users/jacqui/.MacOSX/environment,
DYLD_INSERT_LIBRARIES) does not exist

The domain/default pair of (/Applications/Safari.app/Contents/Info,
LSEnvironment) does not exist

The domain/default pair of (/Applications/Firefox.app/Contents/Info,
LSEnvironment) does not exist
```

Then you're home free and you're not (yet) infected by Flashback. You can proceed to the "Run Software Update" section of this post. If they *do* return results, then it's likely that you *are* infected. But worry not, as there are ways to get rid of the malware that will only hurt for a second.

How to get rid of Flashback

Here's where things might get complicated. These removal instructions are from security research firm F-Secure's removal page. Take us away, F-Secure! (Cue Keyboard Cat now.)

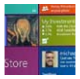
1. Run the following command in Terminal:
   ```
   defaults read /Applications/Safari.app/Contents/Info LSEnvironment
   ```
2. Take note of the value, DYLD_INSERT_LIBRARIES
3. Proceed to step 8 if you got the following error message: "The domain/default pair of (/Applications/Safari.app/Contents/Info, LSEnvironment) does not exist"
4. Otherwise, run the following command in Terminal:
   ```
   grep -a -o '__ldpath__[ -~]*' %path_obtained_in_step2%
   ```
5. Take note of the value after "__ldpath__"
6. Run the following commands in Terminal (first make sure there is only one entry, from step 2):
   ```
   sudo defaults delete
   /Applications/Safari.app/Contents/InfoLSEnvironment

   sudo chmod 644 /Applications/Safari.app/Contents/Info.plist
   ```
7. Delete the files obtained in steps 2 and 5
8. Run the following command in Terminal:
   ```
   defaults read ~/.MacOSX/environment DYLD_INSERT_LIBRARIES
   ```
9. Take note of the result. Your system is already clean of this variant if you got an error message similar to the following: "The domain/default pair of (/Users/joe/.MacOSX/environment, DYLD_INSERT_LIBRARIES) does not exist"
10. Otherwise, run the following command in Terminal:
    ```
    grep -a -o '__ldpath__[ -~]*' %path_obtained_in_step9%
    ```
11. Take note of the value after "__ldpath__"
12. Run the following commands in Terminal:
    ```
    defaults delete ~/.MacOSX/environment DYLD_INSERT_LIBRARIES

    launchctl unsetenv DYLD_INSERT_LIBRARIES
    ```
13. Finally, delete the files obtained in steps 9 and 11.
14. Run the following command in Terminal:
    ```
    ls -lA ~/Library/LaunchAgents/
    ```
15. Take note of the filename. Proceed only when you have one file. Otherwise contact our customer care.
16. Run the following command in Terminal:
    ```
    defaults read ~/Library/LaunchAgents/%filename_obtained_in_step15%
    ProgramArguments
    ```
17. Take note of the path. If the filename does not start with a ".", then you might not be infected with this variant.
18. Delete the files obtained in steps 15 and 17.

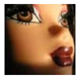
In addition to these steps, F-Secure recommends checking for another variant of Flashback, Flashback.K. The instructions can be found on another page on F-Secure's website.

Run Software Update



Why Microsoft has made developers horrified about coding for Windows 8

1,066 people recommend this.



Warning: this unrealistic image has been Photoshopped

281 people recommend this.

1Gbps fiber for $70—in America? Yup.

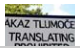
2,740 people recommend this.

Linux computer the size of a thumb drive now available for preorder

1,539 people recommend this.

Quantum decision affects results of measurements taken earlier in time

1,294 people recommend this.

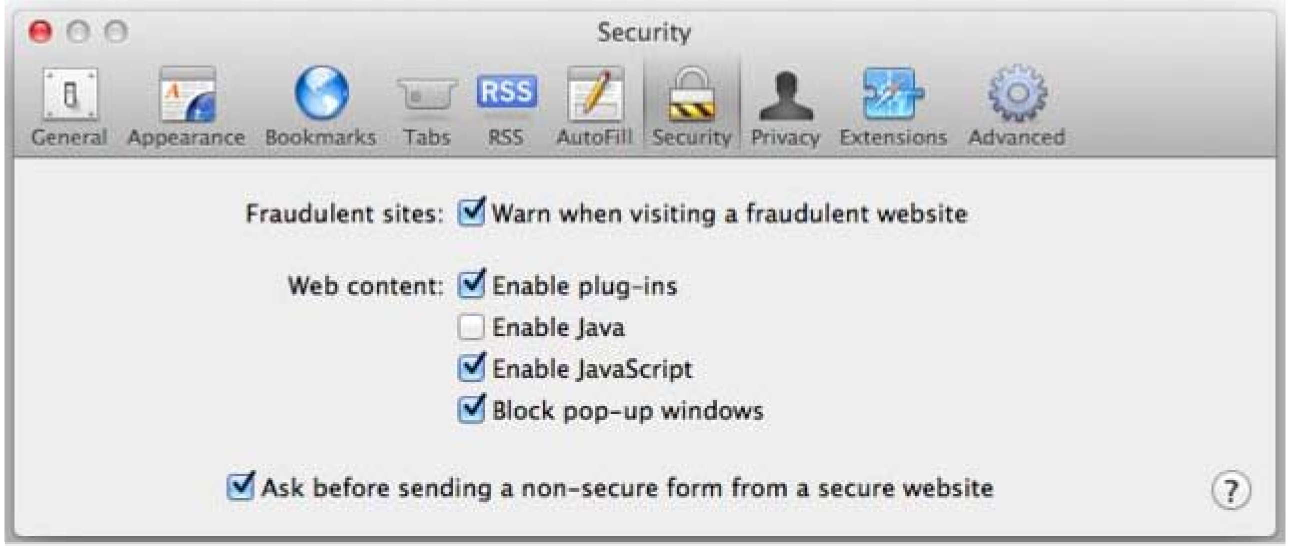


Thinking in foreign language makes decisions more rational

Apple has now released some Java updates that will patch the vulnerability targeted by the current variant of Flashback, so if you're free from infection, you can apply the patch via Software Update. (It's a mystery as to why Apple waited so long to patch Java for Mac OS X when Oracle released an update in February.) You can also manually download the update for Lion and Snow Leopard, respectively, from Apple's support site.

Do you really need Java running in your browser anyway?

This raises an important question: do you even need Java running in Safari? Some people do—my parents, for example, play bridge on a website that requires a Java applet to run, and they will not switch to another service—but many of us don't. If you don't, it could be worth turning off just to keep yourself extra secure. You can do this in Safari by going to the Safari menu and then Preferences. Then click over to the "Security" tab:



Fraudulent sites: ☑ Warn when visiting a fraudulent website

Web content: ☑ Enable plug-ins
□ Enable Java
☑ Enable JavaScript
☑ Block pop-up windows

☑ Ask before sending a non-secure form from a secure website

Unchecking Java in Safari will let you find out if you can live without it

Uncheck "Enable Java." (You can always turn it back on if you have to.) If you can live your life without it, this will be an extra step to help protect you against similar attacks in the future.

Conclusion

Once you've performed these steps and updated your installation of Java, you're inoculated against the current version of the Flashback malware, but that doesn't mean the variant won't change again sometime in the future to exploit a different vulnerability on your Mac. Stay vigilant! Keep your software up to date, don't ignore strange files that appear from strange places, and if you can, be aware of odd network behavior coming from your Mac. You can do this by installing software like Little Snitch to monitor your Mac's network activity. (And a side effect of having Little Snitch installed is that the latest variants of Flashback won't install themselves if you already installed Little Snitch!)

The files don't necessarily come from spammers, either—a Google Image Search might bring you to a malicious website, for example, that could try to execute the code once you visit the site for that cute cat picture. So it's not just about avoiding file attachments in e-mail; malware can be found lurking in all corners of the Web.

As for whether the "half a million Macs" number is accurate, Dr. Web malware analyst Sorokin Ivan said on Twitter that "BackDoor.Flashback.39 uses Hardware UUID (IOPlatformUUID) to identify bots," and Dr. Web's statistics are based on that ID. Even if the numbers aren't accurate, the latest scare is another wakeup call for Mac users who have been ignoring malware and virus threats up to this point. What steps are you taking to make sure your Mac is protected?

Photo illustration by Aurich Lawson

› User comments
Click here to view the 125 comments on this story