

THE GADGET GUIDE

TROJANS

Mac Flashback Trojan: Find Out If You're One of the 600,000 Infected

There's a new Mac trojan that's been floating around, and it's terrifying everyone. It's written in an unknown language, [doesn't even need your password](#) to compromise you, and now it's apparently infected 600,000 users. Here's how to use Terminal to check if you're one of the unlucky many.

The instructions come from [F-Secure](#), which also details how you can remove the trojan if your Mac is, in fact affected. But let's not put the cart before the virus; here's how to see if you're clean.

First, open Terminal from your Utilities folder. If you've never ever done that before, don't be scared! It's a nice way to turn your Mac into a computer you actually have some control over.

Then, once you're in, follow [these easy steps](#) to detection:

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"
```

If you don't get that error message, well, time to head to [F-Secure](#) for your fix. If you're clean so far, you can move on to step eight:

BY KYLE WAGNER APR 5, 2012 8:40 AM

Share

Like

12k

271,937

278

GET OUR TOP STORIES
FOLLOW GIZMODO



LAS VEGAS

6:40 PM

Vegas Casinos Connected by Zipline Sounds Like an *Ocean's 14* Stunt



CURRENCY

6:20 PM

Glow-in-the-Dark Dinosaur Quarter Is Actual Legal Tender



MICROSOFT

6:16 PM

Microsoft Windows Phone Designer Team Hurls Veiled Insights at Apple's Ugly, Skeuomorphic Apps



APP OF THE DAY

6:00 PM

National Geographic Today: Gander at Gorgeous Photos From Across the Globe



PHONES

5:54 PM

T-Mobile's Obnoxious Scream Tones Will Help You Find a Lost Phone

[MORE STORIES...](#)

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"
```

In other words: "does not exist" means you've got a healthy rig. Anything else, just keep following F-Secure's instructions to vanquish the intruder. And even if you get the all clear for now, don't wait on downloading the security update that patches the Java vulnerability that started this whole mess. [F-Secure via Ars]

Contact Kyle Wagner:

EMAIL THE AUTHOR

COMMENT

TWITTER

DISCUSSION THREADS

FEATURED ALL START A NEW THREAD



Arggh! there goes a...snake a snake!

Thu 05 Apr 2012 8:50 AM

"and now it's apparently infected 600,000 users"

So basically all Mac users?

/terrible attempt at joke

Edited by Arggh! there goes a...snake a snake! at 04/05/12 8:51 AM



Lunarpancake @Arggh! there goes a...snake a snake!

Looks like there's enough Mac users for people to start bothering writing viruses for them now, eh?



3pedalsgood @Arggh! there goes a...snake a snake!

1997 called, they want their Apple disparaging joke back.

promoted by FlameCell



FlameCell @3pedalsgood

1997 called, they want their comeback back.



CPD @FlameCell

1997 called. They want their lame retort to lame comebacks back.



papakep @CPD

1997 called. They are sick of everyone taking their stuff.



Dave J. @3pedalsgood

1997 called, they have this awesome band called the "Cranberries" they want you to check out.



xethor @Dave J.



1997 called, and it.... forget it.

Edited by xethor at 04/05/12 10:14 AM



SheldonPlankton @Dave J.

1997 Called...but they had to hang up.. they were too busy trying to fix the Y2K bug....

Edited by SheldonPlankton at 04/05/12 10:15 AM



michalski.26 @SheldonPlankton

1997 called, but then the call was interrupted because someone was trying to connect to AOL.

promoted by TheJaz



TheJaz @michalski.26

I'm calling the cops because these jokes are so bad, it's criminal.



snowburnt @michalski.26

1997 left a voicemail



sprouty @snowburnt

1997 sent a fax but you were out of paper.

CPD approved this comment



CPD @sprouty

1997 sent you a message on your pager. It was all numbers.



MrWheezyE @CPD

1997 is so 2000 late



smcallah @SheldonPlankton

Not in 1997 they weren't. People weren't really fixing Y2K bugs until 1999, and even then, not until the end of 1999. Procrastination reigned supreme.



r24 @smcallah

@smcallah Yes, we were. Dude, seriously? You don't patch a big blue in a weekend.



kjnutt @TheJaz

Freddy Heflin from 1997's Cop Land wants to issue a warrant for your arrest.

 FlameCell @CPD

I just asked 1997 and they said you're full of it.

 Omega117 @FlameCell

1997 called the Extreme Ghostbusters

 CPD @FlameCell

1997 knew me when. They're probably right.

 slapgun87 @3pedalsgood

1997 called, I was only 10. I remember answering on this phone:



 Zachary Jacob Zblewski @3pedalsgood

1997 called, but they had to keep it brief because they still pay by the minute for long distance.

