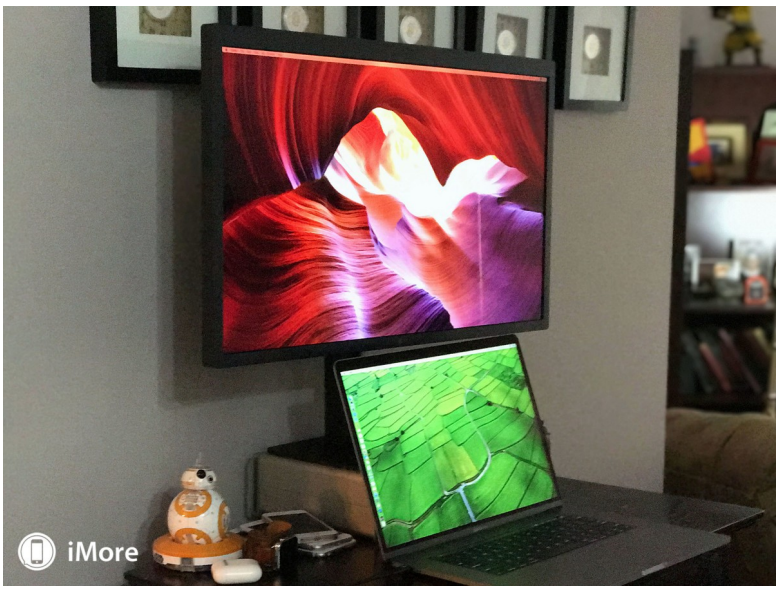
NOT AGAIN...

PSA: Again, another reason not to open attachments from strangers

BY LORY GIL Monday, May 1, 2017 at 11:25 am EDT 5 COMMENTS

Lory is a renaissance woman, writing news, reviews, and how-to guides for iMore. She also fancies herself a bit of a rock star in her town and spends too much time reading comic books. If she's not typing away at her keyboard, you can probably find her at Disneyland or watching Star Wars (or both).



The Mac malware scam, Dok, has been blocked, but you should still watch out for suspicious emails.

Update: Apple has revoked the developer certificate, so it will now trigger a notification that you are about to install a program from an unidentified developer.

Check Point Technologies has released detailed information about a new malware attack that is directed at Mac users. It's being called **Dok** and it has the potential to access a user's online communication, including secure sites. According to Check Point, it affects all versions of OS X.

> versions of OSX, has 0 detections on VirusTotal (as of the writing of these words), ~~is signed with a valid developer certificate (authenticated by Apple)~~ [strikethrough added], and is the first major scale malware to target OSX users via a coordinated email phishing campaign.

According to MacWorld, Apple has revoked the certificate, which means you'll get a notification when Dok tries to install itself on your Mac.

> Apple confirmed that Gatekeeper wasn't bypassed. That developer certificate has been revoked, which will prevent it launching in the future without a warning. Apple will likely update XProtect, its silent malware signature system, although it provided no details.

Why is Dok such a big deal?

Check Point says that Dok is the first major scale malware to target OS X users, but that's not the only reason it's a big deal. Dok also appears to have had a fake signed Apple developer certificate. Apple has revoked the certificate as of May 1.

How Dok gets in

To calm your fears, this malware isn't something you could accidentally pick up while surfing the net or if your Wi-Fi password isn't secure. For Dok to infect your Mac, *you* have to invite it into your system.

Check Point explains that the initial contact is via a phishing email (currently targeted at European users). When a person downloads an attachment (called Dokument.ZIP) from the email, it copies itself to the Mac and then displays a false message saying the file couldn't be opened because it was damaged. It will then execute itself (at this point, you'll receive a notification that you are installing a program by an unidentified developer and you can click "Cancel" to stop the installation) and send another pop-up message u there is a new update to your Mac's

message, at which point you'll be asked to enter your password to continue.

That's how Dok infects your Mac. You first have to open an attachment from an unknown source. You then have to perform an action on your computer that is completely different than how Apple does things (Apple doesn't ask you to click on "Update All" in a pop-up message). You then have to enter your password to continue, which is the point of attack. If you give away your password to Dok, it gains access to your administrative privileges, where it can quietly redirect all of your web browsing to a proxy.

How you can protect yourself against Dok

Since this is a phishing attack, it's pretty easy to avoid infection. Simply don't download attachments from unknown sources. If you aren't sure of the legitimacy of an email, you can check the file name of the attachment. If it's called Dokument.ZIP, definitely don't open it. It's always a good practice to check the sender's email address to see whether it is official. If the sender email is something like llk124@ww.edir.4.com, you should probably delete that email right away.

What if Dok has already infected your Mac?

If you did receive an email from an unknown source and have already opened the attachment called Dokument.ZIP, and then clicked on a suspicious looking update button, and then entered your password, and now think you might be infected, there are a few steps you can take to delete the malware.

First, navigate to your Proxy configuration settings and delete the rogue server.

1. Click the **Apple Menu** icon in the upper left corner of the screen.
2. Click **System Preferences** from the drop down menu.
3. Click **Network**.
4. Select your current **internet connection** (Wi-FI or Ethernet).
5. Click **Advanced** at the bottom right of the window.
6. Select the **Proxies** tab.
7. Select **Automatic Proxy Configuration**.

Dok also installed two LaunchAgents, which you'll also have to find and delete.

/Users/*%User%*/Library/LaunchAgents/com.apple.Safari.proxy.plist

/Users/*%User%*/Library/LaunchAgents/com.apple.Safari.pac.plist

Lastly, you'll need to delete the fake signed Apple Developer certificate.

1. Launch **Finder**.
2. Select **Applications**.
3. Open your **Utilities** folder.
4. Double-click on **Keychain Access**.
5. Select the **certificate** named COMODO RSA Secure Server CA 2.
6. Right or Control + click on the **Certificate**.
7. Select **Delete Certificate** fro the drop down options.
8. Select **Delete** to confirm that you want to delete the certificate.

Remember best practices for staying safe

It's very difficult to get the Dok infection. There are a number of red flags you would likely come across that would help you identify that something is wrong. Don't open attachments from unknown sources. Don't click on suspicious-looking pop-up messages. Check email addresses of senders to see if they are real. You can protect yourself from attacks if you stay aware.

If you do, however, end up with malware on your Mac, don't worry. If the steps above seem too complicated, you can call Apple support for help. Someone will be able to walk you through the necessary steps to remove the malware from your Mac.

Calls, Text and 10GB of 4G LTE | Simple Method Can "Regrow" | Seconds Before Disaster | Had Their Life Sucked Out And

Reader comments

PSA: Again, another reason not to open attachments from strangers

5 COMMENTS

SORT BY DATE SORT BY RATING

cuttheredwire

I think it's important to reiterate that the thing has to ask permission to infect your Mac. There isn't a new vulnerability here, but it is a fine example of social engineering.

To me, this highlights the problem with the Mac App Store. It would be nice if you could get by using just the store, where things are checked and at least somewhat vetted. I can't on Mac; I can on iOS.

3 days ago REPLY 0

Derrick4Real

i get like 30 attempts to auto install some flash.dmg spam daily. doesn't happen on windows on the

that. Because maybe every few weeks one gets downloaded on accident. I've never clicked on it to install but still it get's downloaded which is annoying and you have to go delete it.

0 sec ago REPLY 0

MadMax_RW

Took long enough for them to revoke it...

11 hours ago REPLY 0

Katarinabela

Thanks for this article. I generally don't open email attachments unless I'm sure of the sender but it's good to be reminded of the consequences.

10 hours ago REPLY 0

niico100

You have zero wrist support - that desk looks dangerous for your RSI!

8 hours ago REPLY 0