New OSX.Dok malware intercepts web traffic | Malwarebytes Labs

By Thomas Reed

Published: 2017-04-27 · Archived: 2026-04-05 18:46:04 UTC

Most Mac malware tends to be unsophisticated. Although it has some rather unpolished and awkward aspects, a new piece of Mac malware, dubbed OSX.Dok, breaks out of that typical mold.

OSX.Dok, which was discovered by Check Point, uses sophisticated means to monitor—and potentially alter—all HTTP and HTTPS traffic to and from the infected Mac. This means that the malware is capable, for example, of capturing account credentials for any website users log into, which offers many opportunities for theft of cash and data.

Further, OSX.Dok could modify the data being sent and received for the purpose of redirecting users to malicious websites in place of legitimate ones.

Distribution method

OSX.Dok comes in the form of a file named *Dokument.zip*, which is found being emailed to victims in phishing emails. Victims primarily are located in Europe.

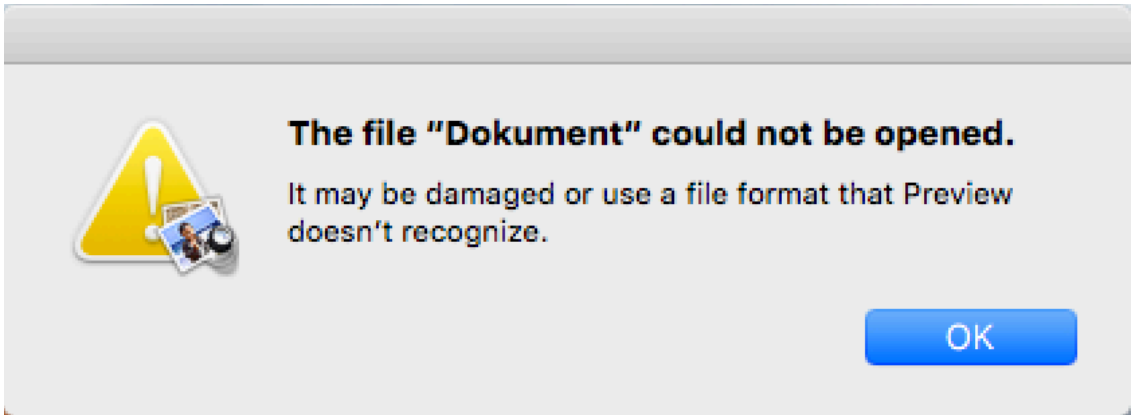
If the victim falls for the scam, the ZIP file decompresses into a file named “Dokument”, which (oddly) has been given the same icon as older versions of Apple’s Preview app. This is not the same as an icon given to a document that can be opened by Preview. Plus, the icon is oddly pixelated, which should raise some red flags among alert users.

Behavioral analysis

This “document” is, of course, actually an application. Fortunately, when the user attempts to open this app, the macOS will display a standard notification to warn the user of that fact:

Apple has already revoked the certificate used to sign the app, so, at this point, anyone who encounters this malware will be unable to open the app and unable to be infected by it.

If the user clicks past this warning to open the app, it will display a warning that the file could not be opened, which is simply a cover for the fact that no document opened:

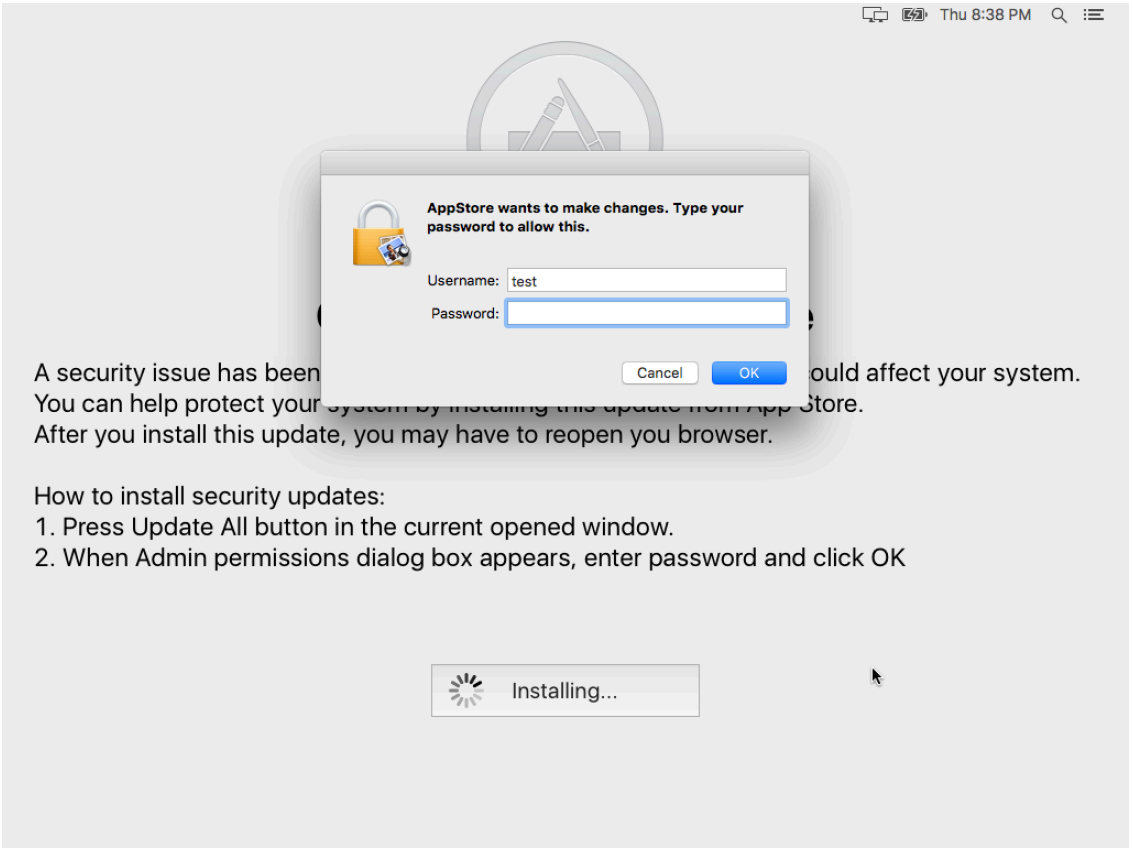


Interestingly, this window cannot be dismissed, as the OK button does not respond. Further, the app will remain stuck in this mode for quite some time. If the user becomes suspicious at this point and attempts to force quit the app, it will not show up in the Force Quit Applications window and in Activity Monitor, it will appear as "AppStore."

If the user manages to force this "AppStore" app to quit, however, all is not yet okay. The malware dropper will have copied itself onto the */Users/Shared/* folder and added itself to the user's login items so it will re-open at the next login to continue the process of infecting the machine.

After several minutes, the app will obscure the entire screen with a fake update notification.

This will remain stubbornly on the screen and will come back on restart since the malware is in the user's login items. If the user clicks the Update All button, the malware will request an admin password.



The malware will remain in this mode for quite some time, leaving the computer unusable to the user until it completes. This is quite different from any normal macOS update process and anyone who is intimately familiar with macOS will know that something is wrong, but those who don't know better could easily be fooled into thinking this is a normal procedure for an important security update.

Once the user has provided an admin password, the malware makes a change to the */private/etc/sudoers* file, which controls access to the sudo command in the Unix shell. A line like the following is added to the end of the sudoers file:

```
test ALL=(ALL) NOPASSWD: ALL
```

This line specifies that the indicated user—"test" in this case—is allowed to use sudo without the need for a password, ensuring that the malware is able to have continued root-level permission without continuing to request for an admin password.

Meanwhile, there is a very good reason for the lengthy install time: OSX.Dok will be busy using its ill-gotten root privileges to install all manner of software in the background, including macOS command-line developer tools, which are needed for the other tools it will install.

The malware will also install Homebrew, a command-line installation system. Homebrew will, in turn, be used to download and install other tools, including tor and socat. The malware will use these processes to funnel all HTTP

and HTTPS traffic through a malicious proxy server.

Two files will be installed in the user's *LaunchAgents* folder to redirect this traffic. The first of these, named *com.apple.Safari.pac.plist* has the following contents:

```
      KeepAlive    Label  com.apple.Safari.pac  ProgramArguments    /usr/local/bin/socat  tcp4-LISTEN
```

The second, named *com.apple.Safari.proxy.plist*, has the same contents, except that it uses port 5588 in place of ports 5555 and 80.

As an added kick in the pants, OSX.Dok installs a new trusted root certificate in the system with the name "COMODO RSA Extended Validation Secure Server CA 2." Using this certificate, it can impersonate any website convincingly, as part of the process of tampering with web traffic.

Once all this is complete, the malware deletes itself from */Users/Shared/*, leaving behind few obvious signs of its presence. The *LaunchAgents* folder is the only change that is likely to be noticed by some users, and many will not understand that these .plist files are not actually associated with Apple.

Removal

Removal of the malware can be accomplished by simply removing the two aforementioned *LaunchAgents* files, but there are many leftovers and modifications to the system that cannot be as easily reversed. Changes to the sudoers file should be reversed and a knowledgeable user can easily do so using a good text editor (like BBEdit), but making the wrong changes to that file can cause serious problems.

A *LaunchAgents* file named *homebrew.mxcl.tor.plist* will have also been installed. Since this is a legitimate file, it shouldn't be detected as malicious, but people who didn't have this installed already should remove it.

The bad certificate should be removed from the System keychain using the Keychain Access application (found in the Utilities folder in the Applications folder.)

The numerous legitimate command-line tools installed, consisting of tens of thousands of files, cannot be easily removed.

Update: Some subsequent variants of Dok have also modified the /etc/hosts file. That should be restored from a backup, or manually edited to revert it to the normal state.

Consumers

Malwarebytes Anti-Malware for Mac will detect the important components of this malware as OSX.Dok, disabling the active infection. However, when it comes to the other changes that are not easily reversed, which introduce vulnerabilities and potential behavior changes, additional measures will be needed. For people who don't know their way around in the Terminal and the arcane corners of the system, it would be wise to seek the assistance of an expert, or erase the hard drive and restore the system from a backup made prior to infection.

Businesses

The impact on business could be much more severe, as it could expose information that could allow an attacker to gain access to company resources. For example, consider the potential damage if, while infected, you visited an internal company page that provided instructions for how to connect to the company VPN and access internal company services. The malware would have sent all that information to the malicious proxy server.

If you have been infected by this malware in a business environment, you should consult with your IT department, so they can be aware of the risks and begin to mitigate them.

Thomas Reed

About the author

Had a Mac before it was cool to have Macs. Self-trained Apple security expert. Amateur photographer.
