New OSX/Shlayer Malware Variant Found Using a Dirty New Trick

By Jay Vrijenhoek

Published: 2018-04-24 · Archived: 2026-04-05 22:40:22 UTC

Malware

Posted on April 24th, 2018 by 

Last February, Intego researchers discovered a new variant of the OSX/Shlayer malware, disguising itself as an Adobe Flash Player update to infect systems with adware. OSX/Shlayer was also found in torrent downloads as part of (or pretending to be) software cracks.

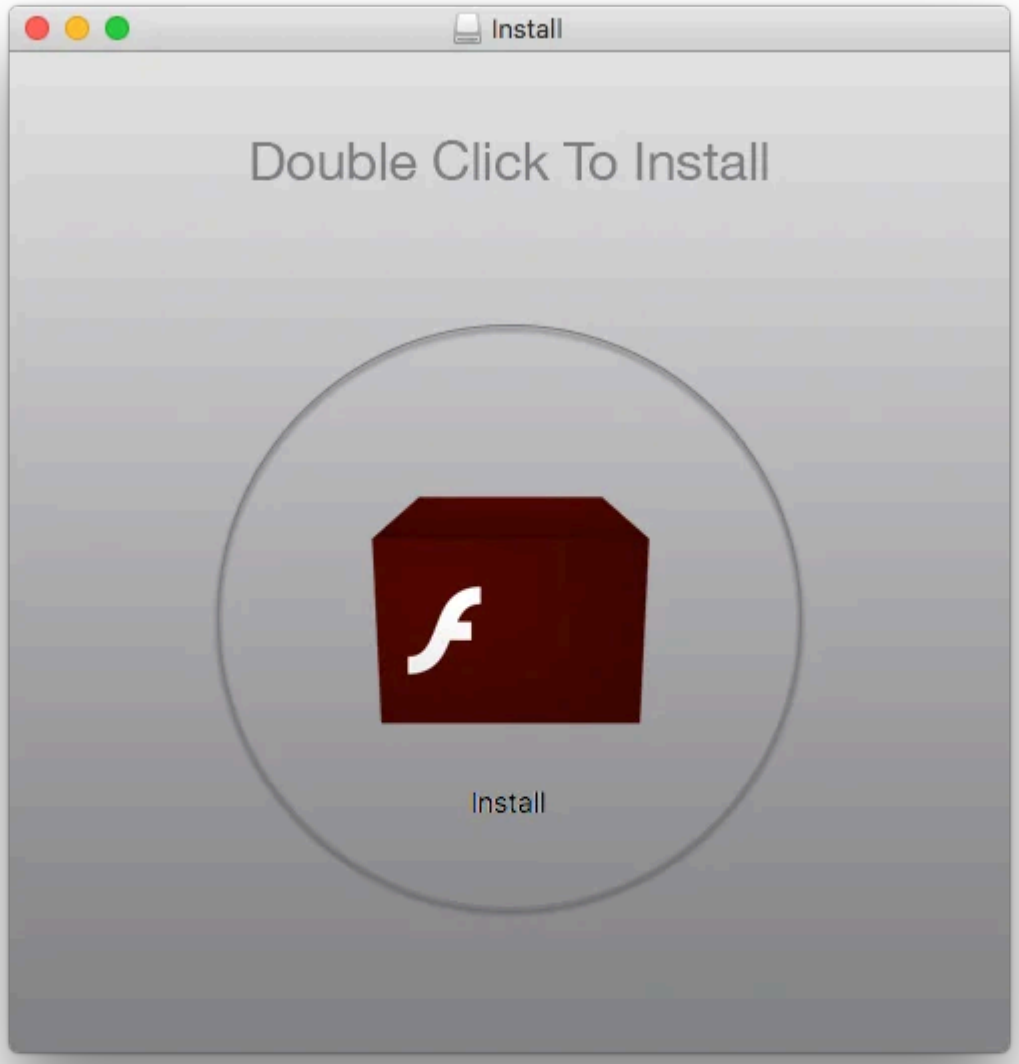
Today, Thomas Reed reported on a new variant of OSX/Shlayer that uses new tricks to get its job done. It installs a configuration profile that forces a browser's homepage to be set as "chumsearch[dot]com." This profile would take control of the homepage settings in Safari and Chrome and also set the "Open new window with" or "Open new tab with" settings to use the Chumsearch URL. While we did not observe this behavior in our tests, we did find a few other interesting things.

How are Macs getting infected?

As with the previously discovered Shlayer malware variants, this one comes as either a fake Adobe Flash Player or a crack (patch) to some kind of paid software. To pick up one of these fake Adobe Flash Player installers, one must wander around BitTorrent sites and it'll surely pop up.

To obtain Shlayer as part of a software crack, BitTorrent sites are also to blame. This is not to say that this malware variant, or any other variants, can't be found on other possibly legit websites, but we have yet to spot Shlayer there.

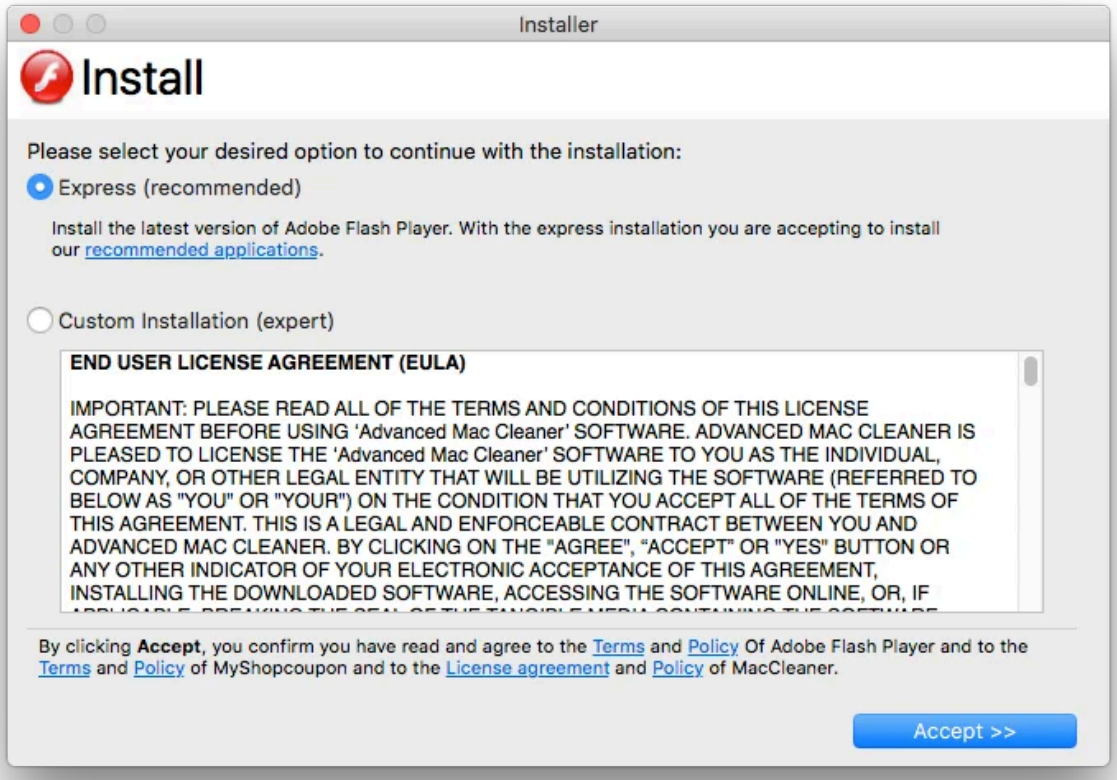
Once a user is tricked into downloading the fake Adobe Flash Player (or a site downloads it automatically), the result is typically a self mounting disk image. The user is then presented with a window that looks mostly like this:



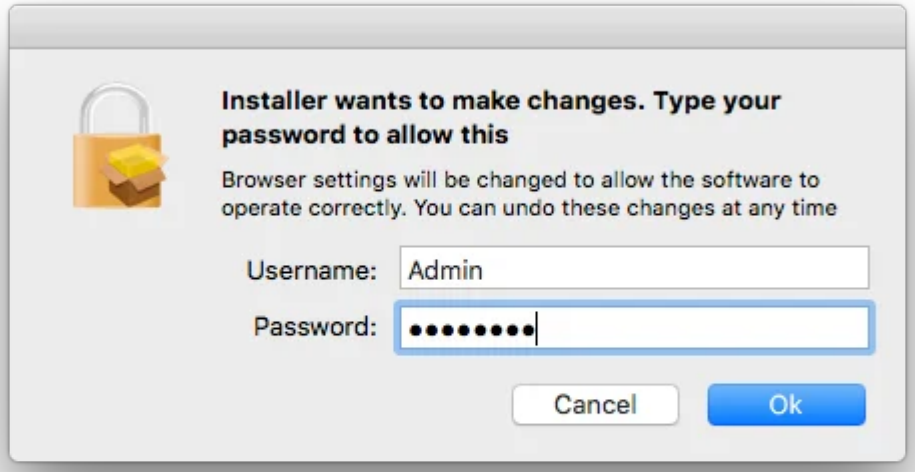
Once the installer is launched, an agreement will pop up that looks absolutely nothing like the one included in the real Adobe Flash Player installer, and two installation types are offered: Express (recommended) or Custom

Installation (expert). The wording is, of course, carefully chosen to deter users from selecting the Custom Installation option and seeing what is really being installed.

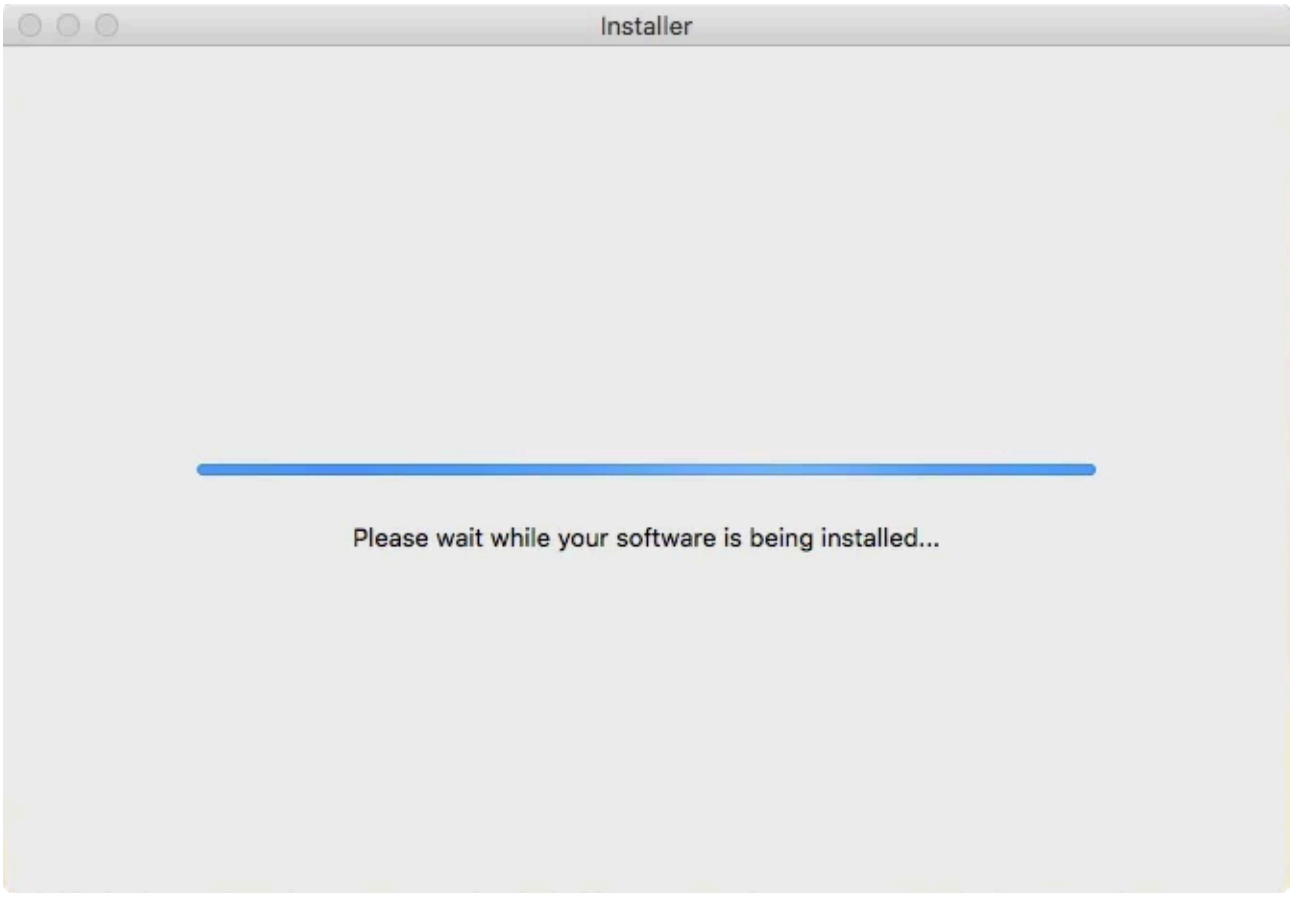
Even without scrolling through it, you can tell the presented agreement does not reference Adobe Flash Player, instead it references Advanced Mac Cleaner. This should be a big red flag, but most users may be so accustomed to quickly clicking “OK,” “Continue” and “Agree” to finally get their installation going. (These windows could mention irrefutable proof Bigfoot exists and in all likelihood no-one would notice.)



When the “Accept >>” button is clicked, the user will be presented with a password request.



And when the “Ok” button is clicked, the installer will take over. A window will cover most of the screen and display a progress bar asking the user to please wait. This window cannot be activated, moved or closed.



What does OSX/Shlayer install?

With the installer window open, several components are downloaded in the background. This includes all or some of the following:

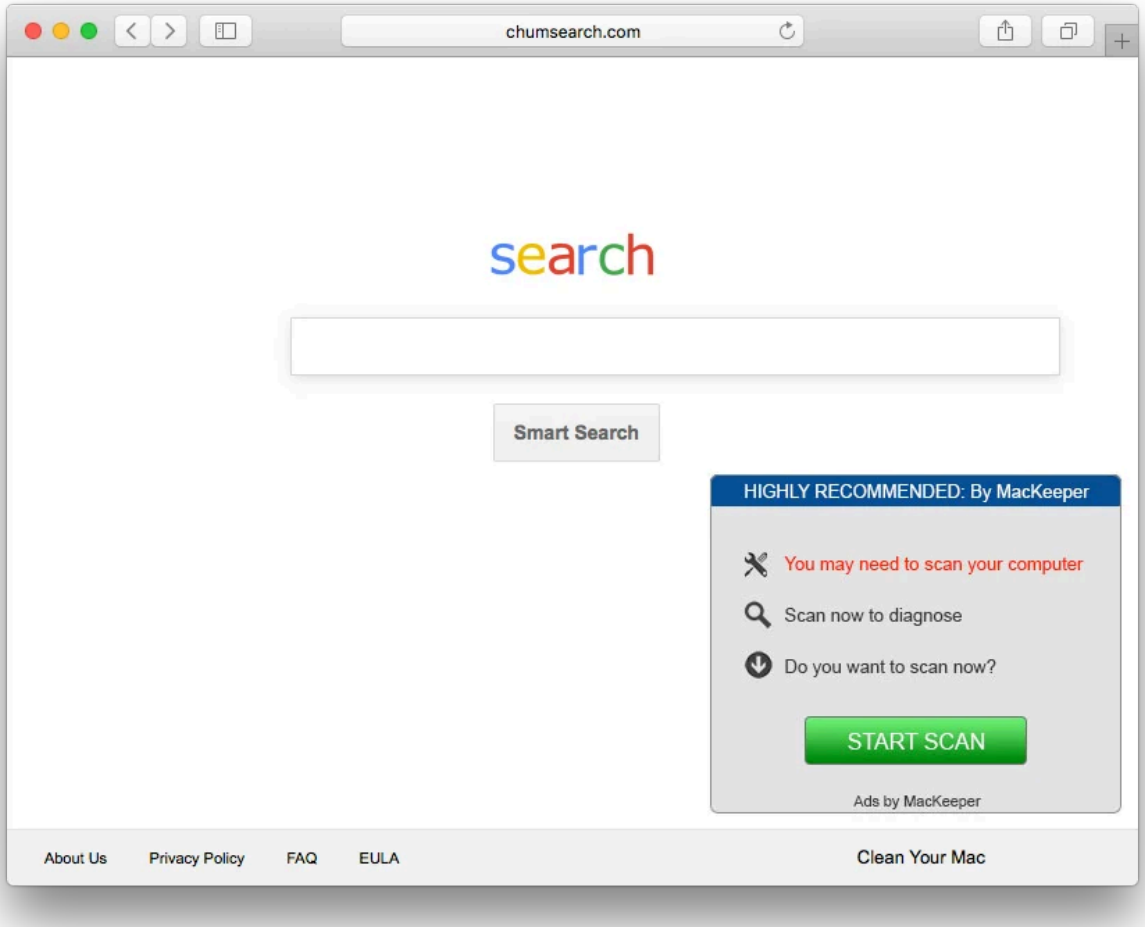
- Chumsearch Safari Extension (though proper installation only worked once)
- MyShopCoupon+ (this fails to install and ends up in the root of the startup drive)
- Advanced Mac Cleaner (ends up in the Applications folder)
- mediaDownloader (ends up in the Applications folder)
- MyMacUpdater (ends up in the Applications folder)
- An actual Adobe Flash Player installer (mounts on the desktop)

It also adjusts the Homepage in Safari, and probably Chrome and other browsers as well, to:

http: //www.chumsearch. com/search/?asset=hp&wtguid=61409200915943979&wtsrc=5409&wtdt=042318&wtbr=1&wtpl=10.12.6&v=5.0

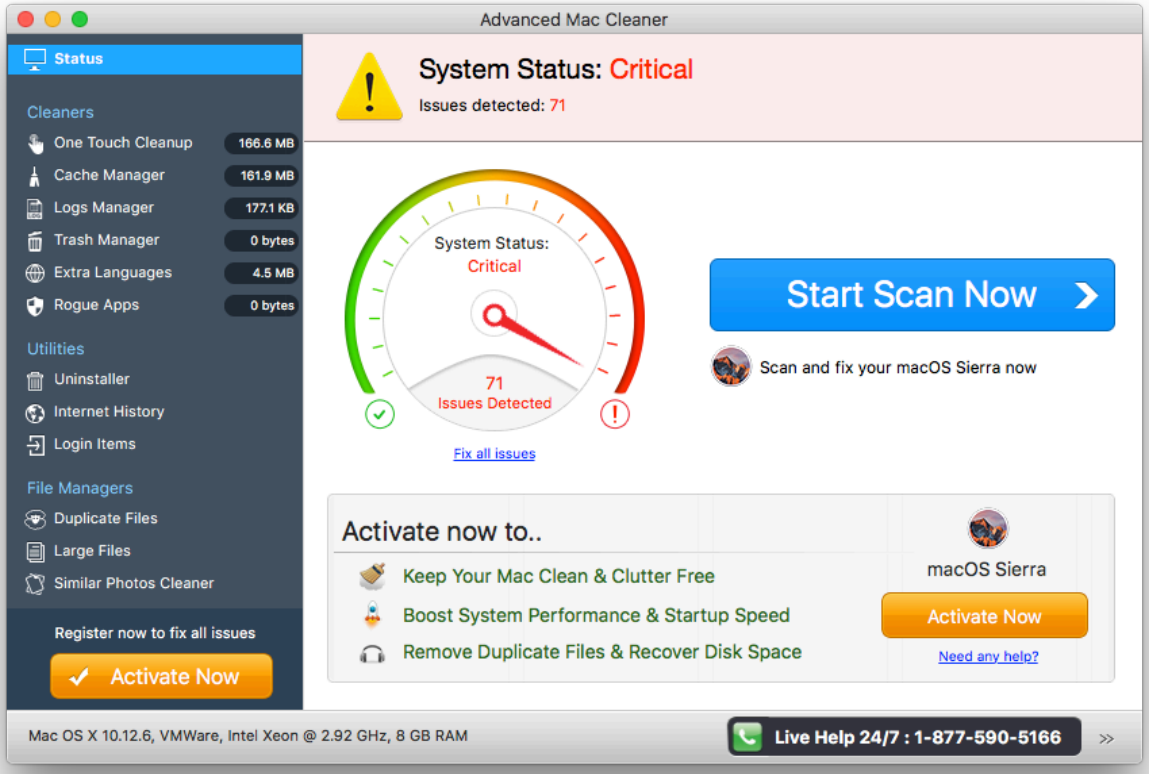
However, it fails to make further adjustments that would cause new windows or tabs to load this URL.

Chumsearch mimics a (very poor) Google search website, which will pop up any time the homepage is requested. This page also features an ad from another company, which should raise red flags right away.



Intego VirusBarrier detects Chumsearch and all of its components as **OSX/Chumsearch**.

Advanced Mac Cleaner is scareware. It shows a scanner that found a lot of issues on your Mac and, of course, claims that the way to fix all these issues is by paying up to $107. This application will pop up after every restart.



Intego VirusBarrier detects Advanced Mac Cleaner and all of its components as **OSX/AMC.fs**.

MyMacUpdater is another Potentially Unwanted Program (PUP), which did not install in this particular round of testing. However, we have encountered it before and Intego VirusBarrier detects it as **OSX/Bundlore**.

OSX/Shlayer is simply the dropper that acts as the gateway to your system and installs a host of other components, such as those mentioned above. This variant uses double base64 encoding to make it harder for malware researchers to, well, research. For example, the Shlayer installer is called on this path:

```
"YlcwdGFXNXpkR0ZzYkMxdFlXTnZjeTVoY0hBdlEyOXVkR1Z1ZEhNdlRXRmpUMU12YlcwdGFXNXpkR0ZzYkMxdFlXTn
```

Which is an encoded version of:

```
bW0taW5zdGFsbC1tYWNvcy5hcHAvQ29udGVudHMvTWFjT1MvbW0taW5zdGFsbC1tYWNvcwo=
```

Which is an encoded version of:

```
mm-install-macos.app/Contents/MacOS/mm-install-macos
```

By double encoding data, it doesn't fool automated processes, but it makes the discovery and analysis by humans a bit trickier.

According to Thomas Reed, this new Shlayer variant uses a new trick.

> In the case of this Crossrider variant, the configuration profile that is installed forces both Safari and Chrome to always open to a page on chumsearch[dot]com. This also prevents the user from changing that behavior in the browser's settings.

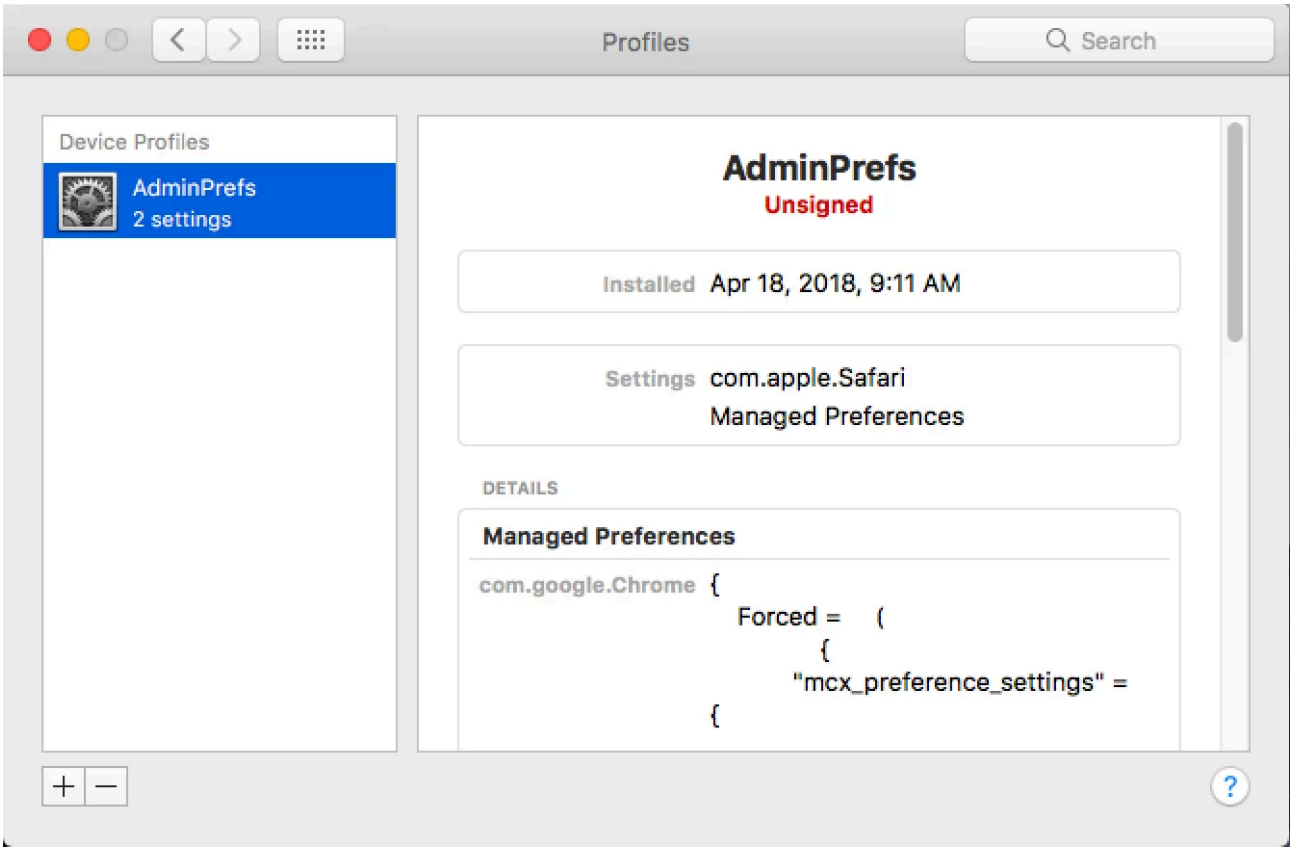


Image credit: Thomas Reed

This is not behavior we were able to reproduce, but we have seen at least one other report of this configuration profile being installed by a web developer in the MacAdmins Slack.

Should Mac users be concerned about OSX/Shlayer?

Currently, Shlayer has been found only on BitTorrent websites, disguised as fake Adobe Flash Player installers or embedded in downloaded torrent files posing as cracks. Therefore, if you do not frequent such websites—and you shouldn't because BitTorrent sites are a malware cesspool—chances of infection are at the moment very low.

If there is an increased risk of infection, users should be concerned. The injecting of ads and hijacking of the homepage are just one aspect of this malware. The Safari and Chrome extensions can do the following:

- Read content from webpages you visit
- Modify content on webpages you visit
- Transmit content from webpages you visit

This includes names, passwords, phone numbers, email addresses, credit card details and much more. Having your online bank statement or Amazon login details transmitted to an unknown party is certainly not ideal.

How to tell if your Mac is infected (and removal instructions)

A dropper like Shlayer can download and install anything it wants. The components that end up on your Mac are dictated by the servers it connects to and the instructions programmed into it. These kinds of installer are also constantly modified to include new techniques (such as the one found by Thomas Reed) and install new components. As such, it is not possible to give a definitive list of components to search for, but in the case of this particular OSX/Shlayer variant, we know of these components:

- /Applications/Advanced Mac Cleaner
- /Applications/MyMacUpdater
- /Applications/MyShopcoupon
- /Applications/mediaDownloader
- /Library/LaunchAgents/com.MyMacUpdater.agent.plist
- /Library/LaunchAgents/com.MyShopcoupon.agent.plist
- ~ Library/LaunchAgents/com.pcv.hlpramcn.plist
- ~ Library/Safari/Extensions/Chumsearch+.safariextz
- ~ Library/Application Support/amc
- ~ Library/Caches/com.apple.Safari/Extensions/Chumsearch+.safariextension
- /myshopcoupon.safariextz
- /mm-plugin.dylib

  In case you did stumble upon the particular installer Thomas Reed mentions, also have a look here:
- Open System Preferences and look for “Profiles”. If a profiles option is available, click on it and look for profiles that don’t belong (there might be legitimate profiles there if your Mac is managed by your work and/or an IT staff). In this case look for “AdminPrefs”, select it and click the “-” to remove it. If your Mac is managed by an IT staff, contact them to have them remove it or give you the OK to remove it yourself. IT admins can find removal instructions in Reed’s report.
- And finally don’t forget to delete the original file that got Shlayer on your Mac in the first place. This will most likely reside in your Downloads folder

If any of these components are found on your Mac, delete them, restart your Mac and empty the trash.

How to protect yourself from OSX/Shlayer

Intego VirusBarrier detects and eradicates this new malware variant (and several others) as **OSX/Shlayer.C.** Use of Intego’s anti-virus software will block and remove all known components of Shlayer malware. Also using a two-way firewall solution, such as Intego NetBarrier, can offer additional protection as it will alert you of any

connection attempts to/from applications on your Mac, which allows you to spot suspect behavior and block it before personal data escapes your computer.

We strongly encourage you to stay away from BitTorrent sites as this will reduce your exposure to malware significantly. You may also consider avoiding the use of Adobe Flash Player in general, so you won't be tempted to install a fake Flash Player update that's riddled with malware.

About Jay Vrijenhoek

Jay Vrijenhoek is an IT consultant with a passion for Mac security research. View all posts by Jay Vrijenhoek →
