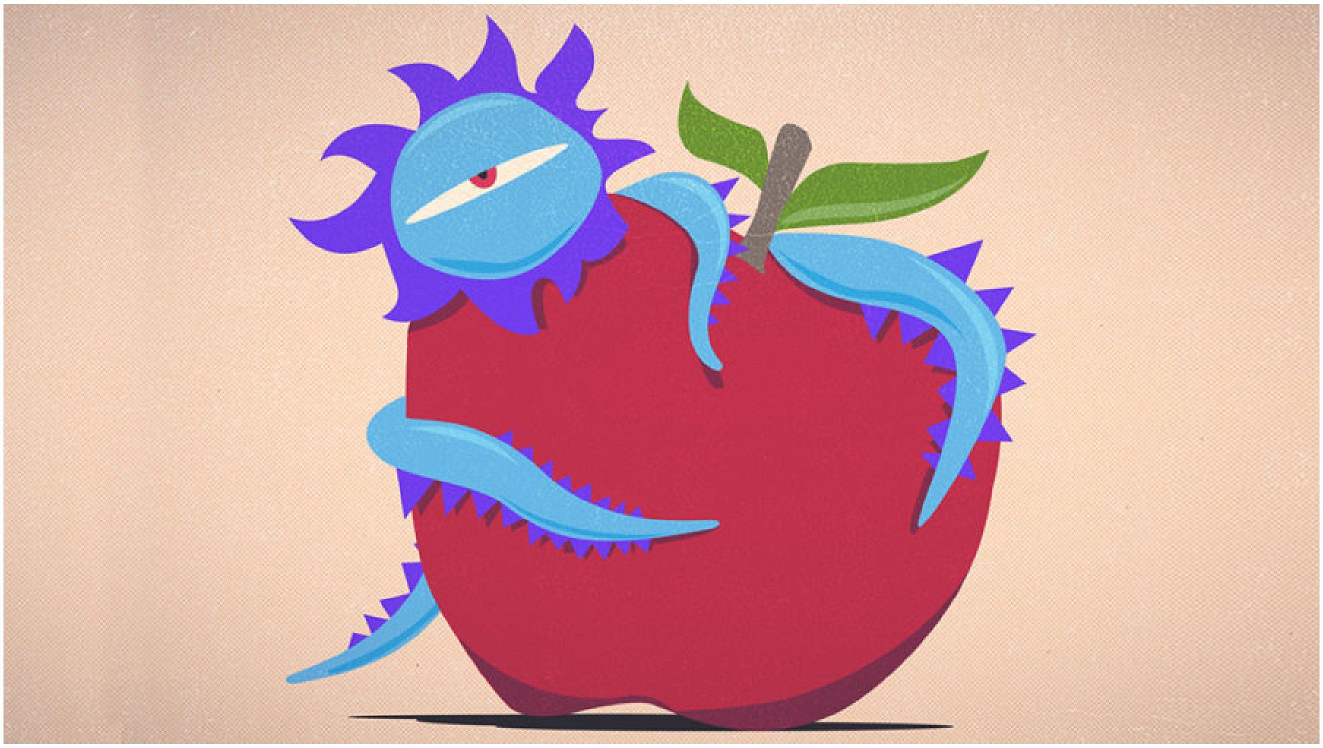
New Crossrider variant installs configuration profiles on Macs

blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/

Thomas Reed

April 24, 2018

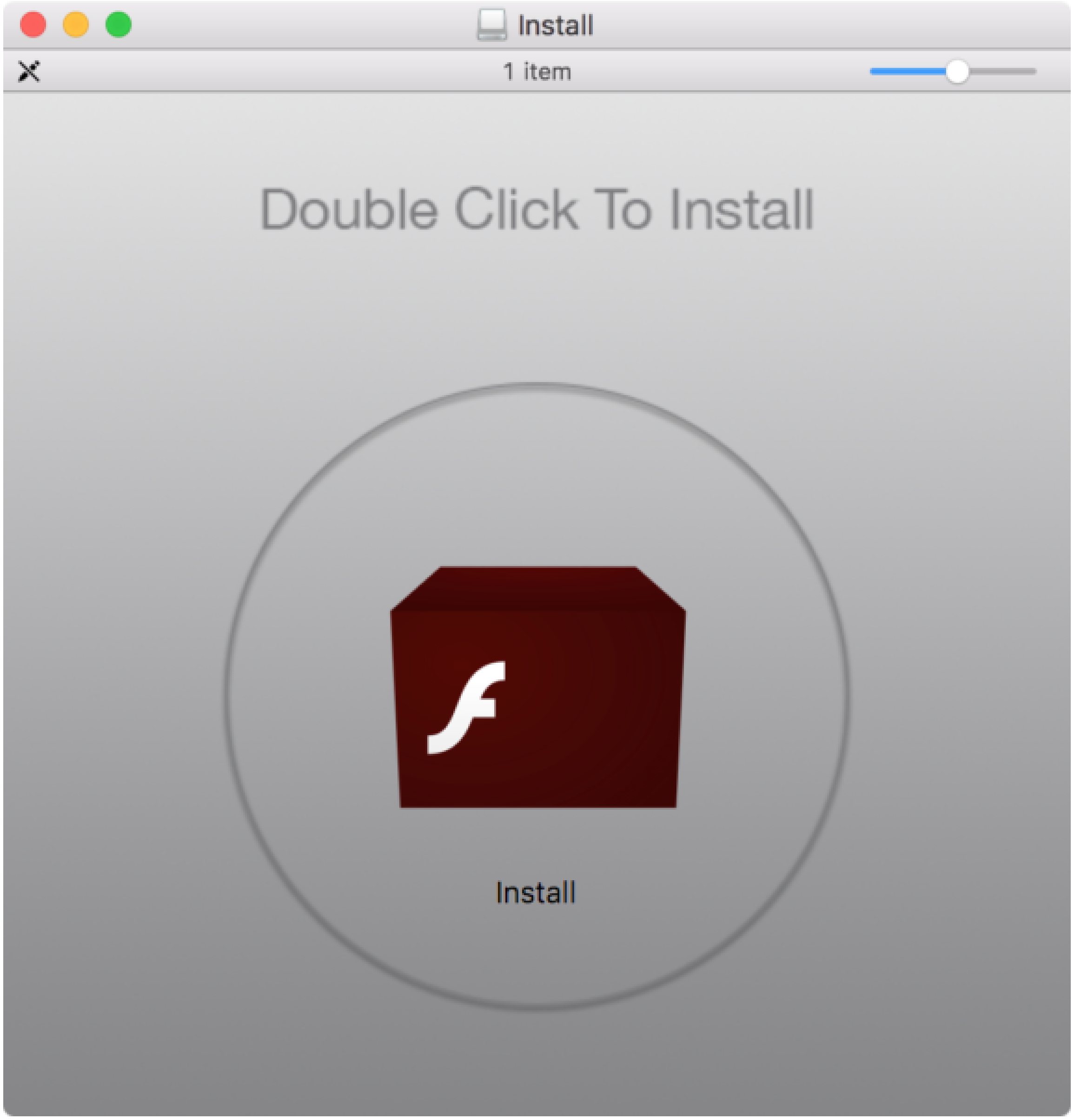


A new variant of the Crossrider adware has been spotted that is infecting Macs in a unique way. For the most part, this variant is still quite ordinary, doing some of the same old things that we've been seeing for years in Mac adware. However, the use of a configuration profile introduces a unique new method for maintaining persistence.

Persistence is the goal of most malware. After all, what good is it to infect a machine if the malware stops running as soon as the computer restarts? There are some cases where that can still be useful (ransomware, for example), but in most cases, that's not desired behavior. So malware creators are often stuck using the same old methods of persistence that are easy to spot. Sometimes, though, they get creative.

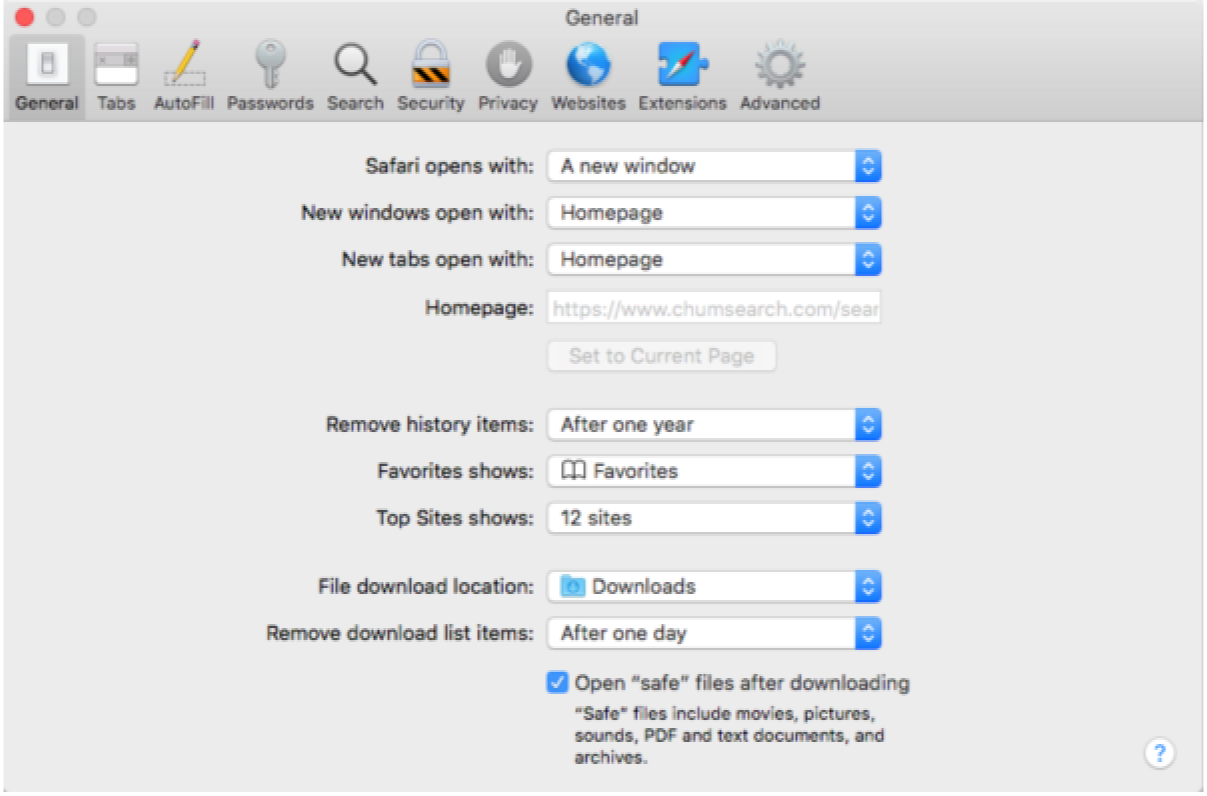
Infection method

This new Crossrider variant doesn't look like much on the surface. It's yet another fake Adobe Flash Player installer, looking like the thousands of others we've seen over the years.



Opening the installer results in a familiar install process, with nothing unique about it. In the course of installation, it dumps a copy of Advanced Mac Cleaner, which commences to announce that it has found problems with your system using Siri's voice. (No such problems actually exist, of course.) Safari also pops open and then closes again suspiciously. This is all very blasé, as far as malware goes.

But something interesting has happened behind the scenes. After removing Advanced Mac Cleaner, and removing all the various components of Crossrider that have been littered around the system, there's still a problem. Safari's homepage setting is still locked to a Crossrider-related domain, and cannot be changed.



Safari opens with: A new window

New windows open with: Homepage

New tabs open with: Homepage

Homepage: https://www.chumsearch.com/sear

Remove history items: After one year

Favorites shows: Favorites

Top Sites shows: 12 sites

File download location: Downloads

Remove download list items: After one day

☑ Open "safe" files after downloading

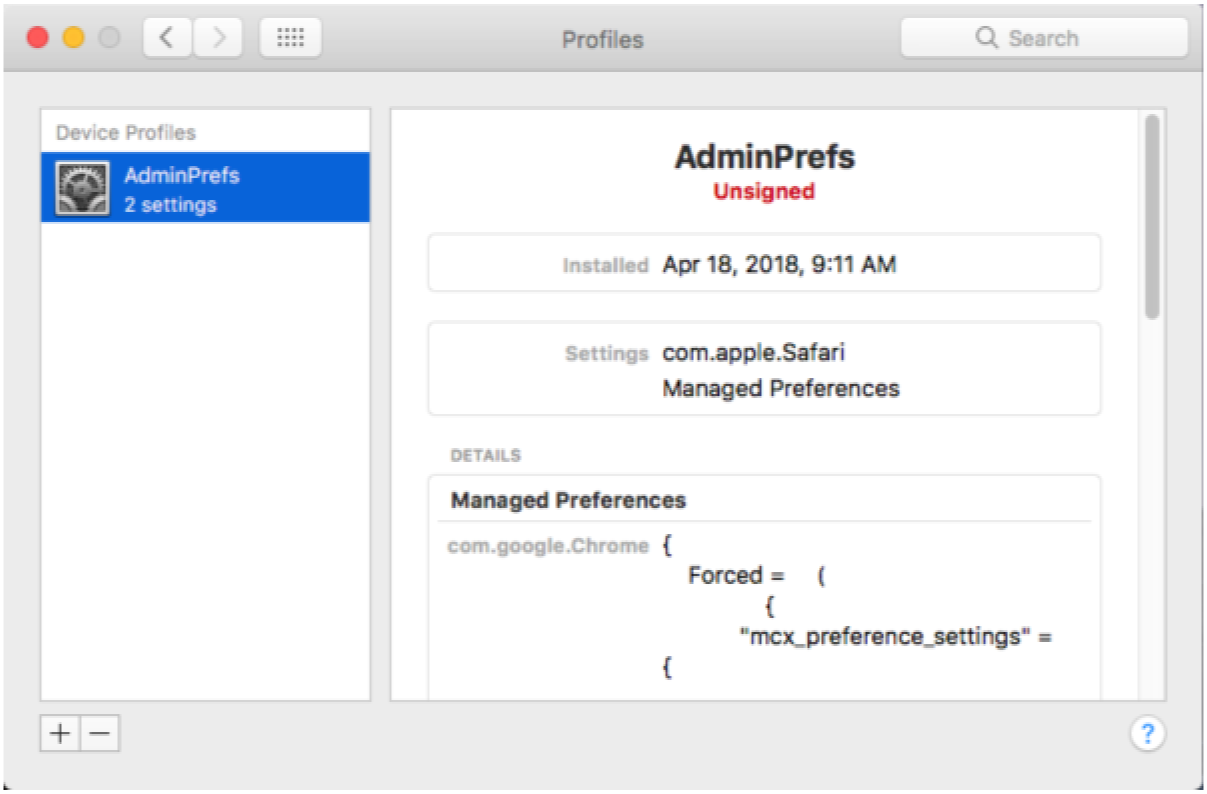
"Safe" files include movies, pictures, sounds, PDF and text documents, and archives.

Malicious configuration profile

It turns out that this is caused by a configuration profile installed on the system by the adware. Configuration profiles provide a means for IT admins in businesses to control the behavior of their Macs. These profiles can configure a Mac to do many different things, some of which are not otherwise possible.

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.

The profile can be found by opening System Preferences, then clicking the Profiles icon. (If there isn't a Profiles icon, you don't have any profiles installed, which is normal.)



AdminPrefs
Unsigned

Installed Apr 18, 2018, 9:11 AM

Settings com.apple.Safari
Managed Preferences

DETAILS

Managed Preferences

```
com.google.Chrome {
                      Forced =    (
                          {
                              "mcx_preference_settings" =
                      {
```

This profile installs with an identifier of com.myshopcoupon.www, which is not visible in System Preferences. However, the profile can definitely be identified by scrolling through the details and looking for references to chumsearch[dot]com. This malicious profile can be removed by selecting it and clicking the minus (-) button in the bottom left corner of the window.

Attribution

The chumsearch[dot]com domain is one that has been linked to a number of different adware programs, which can all be traced back to Crossrider. It is affiliated with one of the most widespread adware campaigns on the Mac, with only the infamous Genieo adware having a higher number of detections by Malwarebytes for Mac among all detected adware families.

The chumsearch[dot]com website contains an ad for MacKeeper (the most widely-distributed potentially unwanted program on macOS, made by Kromtech). Advertising money from Kromtech is undoubtedly one of the ways this site pays for itself. Ironically, this adware is also installed alongside another infamous Mac PUP called Advanced Mac Cleaner, by PCVARK, a program similar to and competing with MacKeeper.

Obviously, not all parts of this chain are affiliated with Crossrider, but the chumsearch domain imposed by the configuration profile definitely is.

If you’re an IT admin

For those readers who are managing fleets of Macs and need to check for and/or remove these profiles remotely, that's pretty easy using a few simple shell scripts.

On macOS 10.12 and earlier, you can use a command like this:

```
sudo profiles -L
```

This works on macOS 10.13 as well, but there is an updated syntax that would be best to use in the future:

```
sudo profiles list
```

Either way, if you see an unfamiliar profile, particularly one with a profileIdentifier of com.myshopcoupon.www, that profile should be removed. This can be done with the following command on macOS 10.12 and earlier:

```
sudo profiles -R -p com.myshopcoupon.www
```

Or, for macOS 10.13:

```
sudo profiles remove -identifier com.myshopcoupon.www
```

Gone in a Flash

The good news is that there was nothing particularly sneaky about the method of infection. Fake Adobe Flash Player installers are nothing new, and are easy to avoid. Still, people do continue to fall for such scams.

If you see a message in your web browser telling you that Adobe Flash Player needs to be updated, it's almost certainly a scam. Do not follow any of the directions provided by these messages, and especially don't download and install whatever they tell you to.

If you do have Flash installed on your Mac, and you believe that it needs an update, you can check for and install updates from the Update tab in the Flash Player pane in System Preferences.

If you want to install Flash for the first time on your Mac, the first thing you should do is think twice. Flash is a dying technology, and is a constant source of security vulnerabilities. Few sites these days truly require Flash. However, if you really do insist on installing it, you should download it only from Adobe's website.