OSX/Shlayer: New Mac malware comes out of its shell

By Joshua Long

Published: 2018-02-21 · Archived: 2026-04-05 12:58:57 UTC

Malware + Recommended

Posted on February 21st, 2018 by

Over the weekend, Intego researchers discovered multiple variants of new Mac malware, **OSX/Shlayer**, that leverages a unique technique.

Although malware that disguises itself as an update to Adobe Flash Player is nothing new, some of the latest incarnations of fake Flash Player installers have an unusual method of downloading additional content.

How are Macs getting infected?

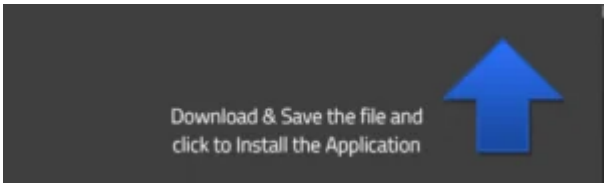
Intego researchers found OSX/Shlayer spreading via BitTorrent file sharing sites, appearing as a fake Flash Player update when a user attempts to select a link to copy a torrent magnet link.

Torrent sites are notorious for distributing malware and adware, sometimes through misleading advertisements, and sometimes through Trojan horse downloads that claim to be “cracks” or that may contain infected copies of legitimate software (watch our recent interview with Amit Serper or read our article Why BitTorrent Sites Are a Malware Cesspool to learn more about the dangers of torrent sites).

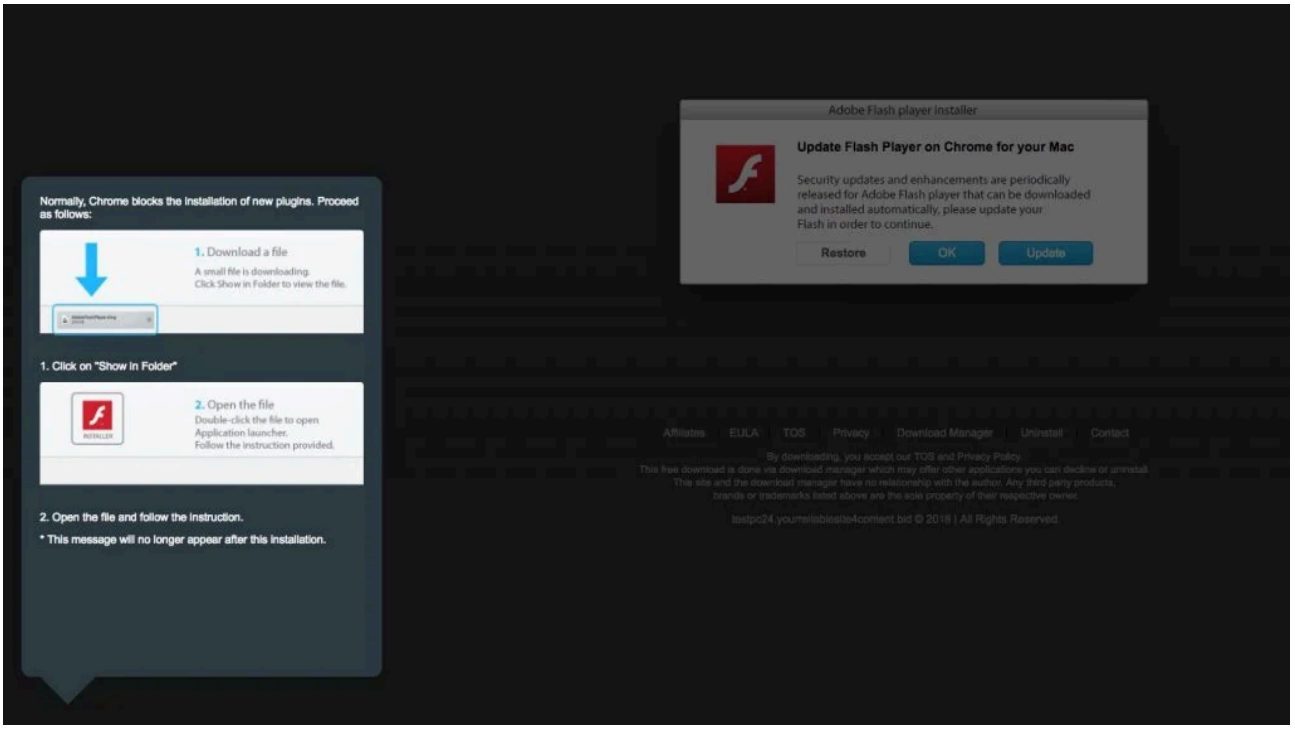
Even if you don’t use torrent sites, you may encounter other sites that claim you need to update Flash Player; in most cases, this is actually an attempt to install malware on your computer.

On some of the malware distribution pages, the fake Flash Player alerts are customized to your browser. If you’re using Mozilla Firefox, you may see an upward-facing arrow appear pointing to the browser toolbar that indicates

that there is a recent download available to open.



If you're using Google Chrome, you may see a pop-up message pointing to the bottom-left corner of the browser window where newly available downloads appear. Ironically, Google Chrome has its own built-in version of Flash Player that users don't need to update manually; it gets updated automatically whenever Google issues an update for Chrome itself.

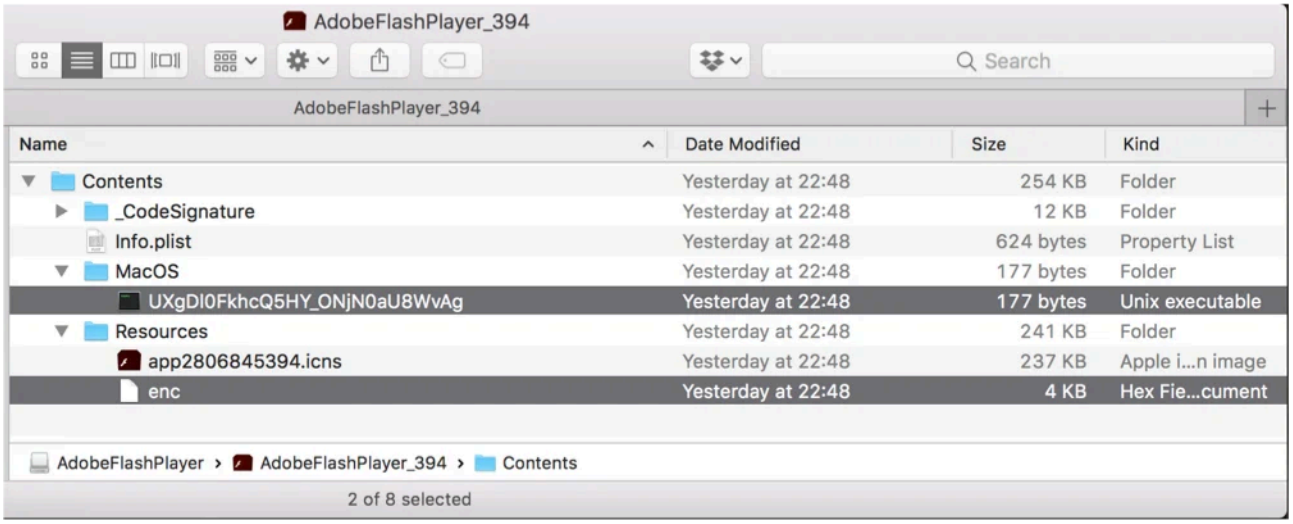


What's unique about OSX/Shlayer?

The initial Trojan horse infection (the fake Flash Player installer) component of OSX/Shlayer leverages shell scripts to download additional malware or adware onto the infected system.

You can think of **shell scripts** as a way to execute a series of commands in sequence, sometimes without requiring any user interaction. They're sort of like a command-line equivalent of an Automator or AppleScript app, or the Mac equivalent of a Windows .bat ("batch") file. Instead of malware having to open up the Terminal on your Mac and type commands right before your eyes (which would be a pretty obvious sign of

infection), malware can secretly execute those commands in the background without the user's knowledge by leveraging shell scripts.



Malware that downloads additional malicious or undesirable code is known as a **dropper**. Intego's research team observed OSX/Shlayer behaving as a dropper and installing **OSX/MacOffers** (also known as BundleMeUp, Mughthesec, and Adload) or **OSX/Bundlore** adware as a secondary payload.

There are three variants of the newly discovered malware, detected by Intego VirusBarrier as **OSX/Shlayer.A**, **OSX/Shlayer.B**, and **OSX/Shlayer.C**, that differ as follows:

- OSX/Shlayer.A uses two code-signed shell scripts
- OSX/Shlayer.B uses one code-signed shell script and one unsigned Mach-O app
- OSX/Shlayer.C uses one code-signed shell script

Code signing is a process used by both legitimate app developers and malware makers. By adding a cryptographic digital signature to Mac software, a developer can enable their apps to more easily bypass Apple's Gatekeeper protection (which is closely associated with Apple's XProtect bad download blocker functionality). Signing an app also provides a direct link between that app and a registered member of the Apple Developer Program.

What does the malware do if installed?

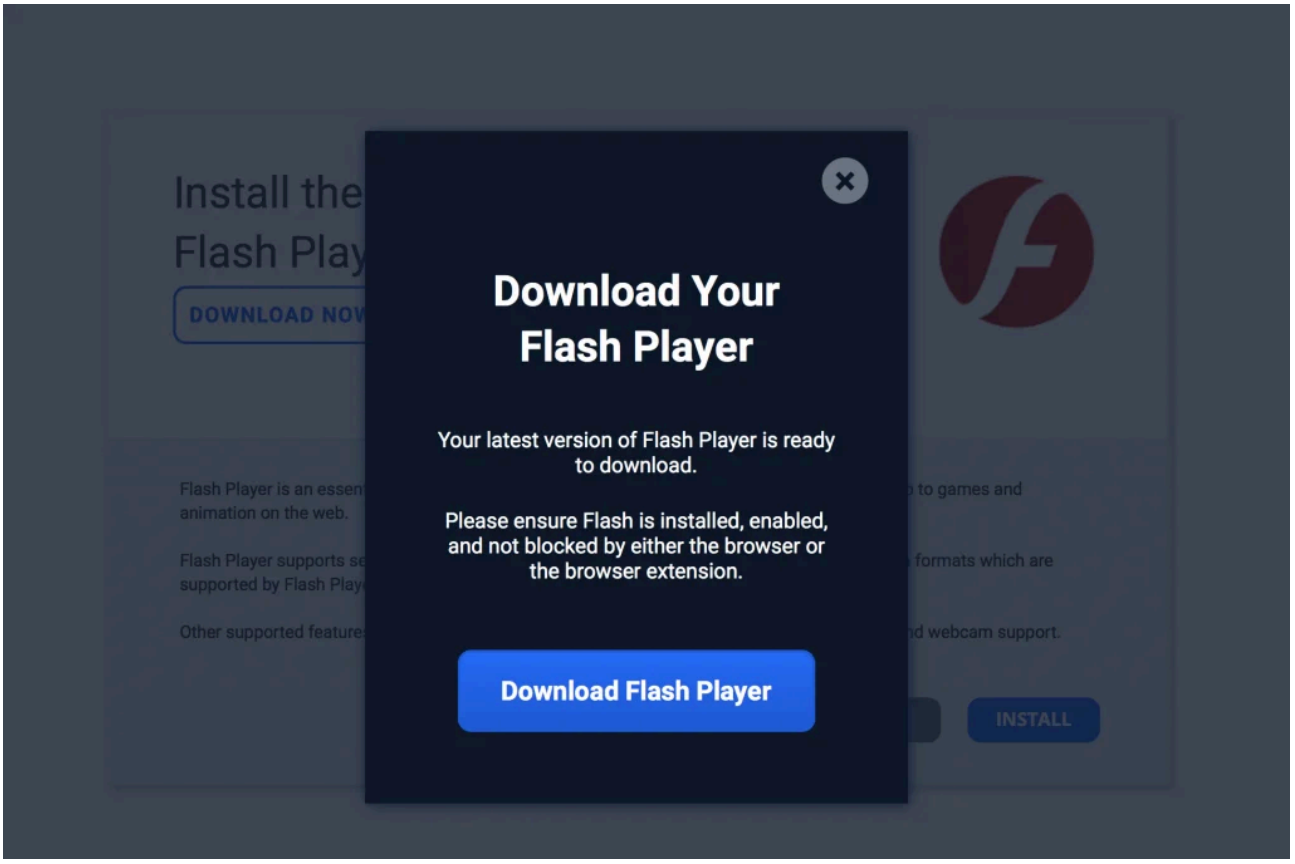
The primary goal of OSX/Shlayer is to download and install adware onto an infected Mac.

Although "adware" may not sound like a big deal, it can be a lot more harmful than the name implies; be sure to watch our aforementioned interview with Amit Serper to learn more about one particular example of malicious Mac adware.

At least one variant of the malware also appears to exhibit an interesting behavior: It checks whether one of several Mac anti-virus products is installed.

How can Mac users protect themselves from OSX/Shlayer?

To prevent infection, avoid any “Flash Player” update alerts you may encounter on the Web; in most cases, these are actually false warnings intended to trick you into downloading and installing malware.



A fake Flash Player alert on a site distributing OSX/Shlayer

If you use Google’s Chrome browser, it already has a built-in version of Flash Player, so you’ll never need to obtain a newer version of the plugin from a third party.

If you use Apple’s Safari browser, or Mozilla Firefox or other third-party Web browsers, you should bookmark https://get.adobe.com/flashplayer/ and only obtain Flash Player updates via that bookmark—that is, if you even need Flash Player in the first place.

In fact, when you get a new computer the best practice is to avoid installing Flash Player in the first place. Few legitimate sites require Flash these days, and for the rare site that does, you can

view the site in Google Chrome. Adobe is phasing out support for Flash and will cease updating Flash Player at the end of 2020.

If you accidentally download a fake Flash Player update and it comes as a .dmg (Mac disk image) file, don't double-click it! Simply drag it to the Trash, and then from the Finder menu (in the top-left corner of the screen, next to the Apple menu) select "Empty Trash…"

See also our article How to Tell if Adobe Flash Player Update is Valid for additional tips.

Users of Intego VirusBarrier X9 are already protected from all OSX/Shlayer variants that have been discovered in the wild.

What can I do if I think my computer is infected?

If you suspect that your computer might be infected, you can download VirusBarrier Scanner (free) from the Mac App Store to scan your computer for an existing infection.

We recommend installing antivirus software with real-time scanning protection, such as Intego VirusBarrier X9 (part of the Mac Premium Bundle X9 utility suite), to help block malware before an infection can occur.

Are there any other indicators of compromise (IOCs)?

WARNING: Do not attempt to connect to the domain names below; doing so may lead to infection!

Network administrators can check their organizations' Web traffic logs for attempts to connect to the following domains (or subdomains thereof) on port 80, which may indicate possible infection by either OSX/Shlayer or similar malware or adware campaigns that leverage the same domains:

- yourreliablesite4content(.)bid — registered on Feb 20, 2018
- macfantsy(.)com — registered in Dec 2017
- ponystudent(.)win — registered in Aug 2017
- childrenlawyer(.)win — registered in Jul 2017
- spoonstory(.)win — registered in Jul 2017
- macinstallerinfo(.)com — registered in 2015
- macresourcescdn(.)com — registered in 2015

Who's behind this malware?

The variants of OSX/Shlayer discovered to date have been associated with Apple Developer Program accounts registered to one of three names: "Harper Natalie," "Murphy Rachel," or "Gennadiy Karshin."

This does not necessarily mean that individuals by those names are the source of the malware; it's possible to register for an Apple Developer Program account using a false identity. (At least the first two names are likely fake, given that Natalie and Rachel are typically given names, not surnames.)

Moreover, if a legitimate Apple Developer Program account has been compromised, a third party may exploit that account's code signing capability for malicious purposes.

The domain names associated with this malware are registered using privacy screens, so little useful information about the domain registrants is obtainable via publicly searchable records.

Have something to say about this story? Share your comments below!

About Joshua Long

Joshua Long (@theJoshMeister), formerly Intego's Chief Security Analyst, is a renowned security researcher and writer, and an award-winning public speaker. Josh has a master's degree in IT concentrating in Internet Security and has taken doctorate-level coursework in Information Security. Apple has publicly acknowledged Josh for discovering an Apple ID authentication vulnerability. Josh has conducted cybersecurity research for well over 25 years, which is often featured by major news outlets worldwide. Keep up with Josh via X/Twitter, LinkedIn, Facebook, Instagram, YouTube, Patreon, Mastodon, the JoshMeister on Security, and more. — View all posts by Joshua Long →

Source: https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/