CSI MacMark: Janicab

macmark.de/blog/osx_blog_2013-08-a.php

Da ich den Janicab-"Trojaner" nicht "in the wild" auftreiben konnte, hatte ich Thomas von The Safe Mac um Rat gefragt. Er gab mir den Hinweis, bei VirusTotal anzufragen, ob sie mir Zugriff auf ihre Malware-Samples geben. Dank VirusTotal bin ich nun in der Lage, diesen Artikel als Fortsetzung von Trojanisches Pferd Janicab erledigt zu schreiben.

Die Berichte, die ich sonst so lesen konnte, sind mir zu wenig. Manche schreiben, es würde gar keine Warnmeldung angezeigt, was nicht stimmt. Und ich vermisse Hilfestellung für den normalen User, Infos darüber, wie er sich mit Bordmitteln schützen kann. Aus dem Grund mache ich hier eine kleine "Crime Scene Investigation" aus der Serie "CSI:MacMark".

CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS

Öffnen oder nicht?

Als Janicab frisch unterwegs war, bekam man, wenn man ihn doppelklickte, eine teils falschrum geschriebene Warnmeldung angezeigt, die verkündet, daß es sich um eine Anwendung handelt. Falschrum, weil der Dateiname ein Sonderzeichen für Leserichtungswechsel enhält. Die Meldung kommt, weil die üblichen Netzprogramme von OS X ein Quarantäne-Flag auf ihre Downloads setzen. Ist das Ding ausführbar, wird der Benutzer gewarnt.

Leider ist die Standardeinstellung in OS X, daß Datei-Endungen nicht angezeigt werden. Das ist keine gute Idee, weil man damit auf eine Kontrollstelle verzichtet.

Janicab ohne eingeschaltete Dateinamen-Erweiterungen im Finder.

Viel verdächtiger sieht das Trojanische Pferd aus, wenn man sich Datei-Endungen anzeigen läßt.

Janicab mit eingeschalteten Dateinamen-Erweiterungen im Finder.

In jedem Fall kann man aber die Info-Box aufrufen, bevor man etwas doppelklickt. In diesem Fall sagt sie eindeutig, daß es sich bei dem "PDF" um eine Application handelt, und, daß sie tatsächlich eine komische Doppelendung hat.

Die Infobox von Janicab zeigt, daß es ein Programm ist und den tatsächlichen Namen.

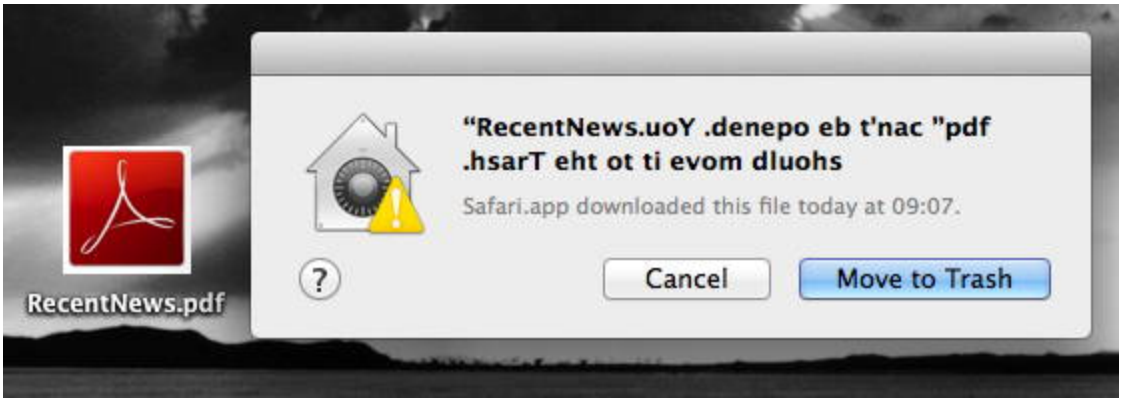
Signierte Malware

Janicab ist eine signierte Mac-Application, die ein Wrapper um Python-Skripte ist. Im Terminal kann man sich die Details der Signatur ansehen:

```
GoldCoast:Desktop joeuser$ codesign -vvvd RecentNews.fdp.app/
Executable=/Users/joeuser/Desktop/RecentNews.fdp.app/Contents/MacOS/installer
Identifier=org.pythonmac.unspecified.installer
Format=bundle with Mach-O universal (i386 x86_64)
CodeDirectory v=20100 size=344 flags=0x0(none) hashes=10+3 location=embedded
Hash type=sha1 size=20
CDHash=ee045a751fb61e33b353b0c91796cc3d4e8fc37b
Signature size=8510
Authority=Developer ID Application: Gladys Brady
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=23 Apr 2013 11:34:48
Info.plist entries=21
Sealed Resources version=1 rules=4 files=21
Internal requirements count=1 size=196
```

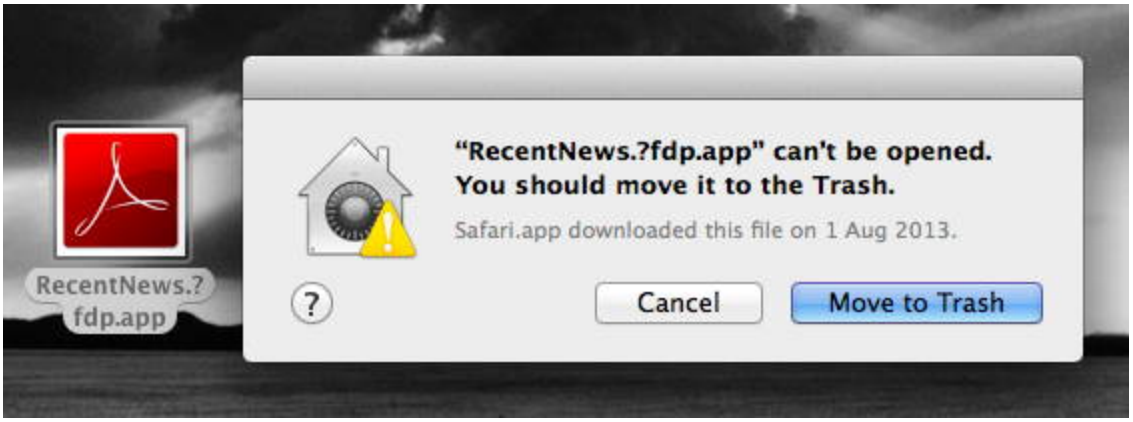
Diese Signatur macht es für Apple einfach, die Malware aus dem Verkehr zu ziehen. OS X bekommt von Apple Infos über ungültige Entwickler-Zertifikate. Nach kurzer Zeit hatte Apple offenbar das Zertifikat von Gladys Brady deaktiviert. Seitdem sieht man beim Öffnen des Schadprogrammes eine andere Meldung:

Janicab kann per Doppelklick im Finder nicht mehr geöffnet werden (deutsch).



Janicab kann per Doppelklick im Finder nicht mehr geöffnet werden (englisch).

Wie schon erwähnt, kommt die Meldung falschrum. Das allerdings nur, wenn man sich die Dateinamen-Erweiterungen im Finder nicht anzeigen läßt. Aktiviert man sie, dann ist die Meldung auch im Klartext richtigrum lesbar:



Janicab-Warnmeldung mit eingeschalteten Dateinamen-Erweiterungen im Finder.

Darum nochmals der Hinweis: Schaltet im Finder die Dateinamen-Erweiterungen ein!

Testlauf in der Sandbox

An der Signatur oben sieht man, daß die ausführbare Datei im Application-Bundle an der üblichen Stelle liegt und hier "installer" heißt. Damit deutet die Malware schon an, was sie tut. Man sieht, daß die App 32- und 64-Bit-Systeme nativ unterstützt.

```
GoldCoast:MacOS joeuser$ file installer
installer: Mach-O universal binary with 2 architectures
installer (for architecture i386):      Mach-O executable i386
installer (for architecture x86_64):    Mach-O 64-bit executable x86_64
```

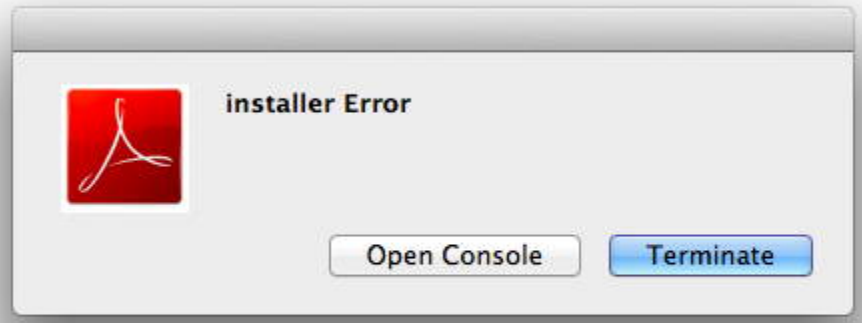
Manche Seiten schreiben, es handele sich um eine Multiplattform-Malware. Allerdings läuft dieses Exemplar nur auf OS X. Die Schwester-Malware für Windows ist eine andere Geschichte. Sie ist also nicht wirklich plattformübergreifend, sondern speziell für jedes Betriebssystem.

Um zu schauen, was Janicab wohl anstellen möchte, starte ich ihn in einer Sandbox, die sowohl das Schreiben von Dateien als auch Netzverkehr unterbindet. Außerdem schalte ich Debug-Ausgaben ein, um zu erfahren, was er tut:

```
GoldCoast:MacOS joeuser$ sandbox-exec -p "(version 1) (allow default) (deny network*)
(deny file-write*) (debug deny)" ./installer
mkdir: /Users/joeuser/.t: Operation not permitted
Traceback (most recent call last):
  File "/Users/joeuser/Desktop/RecentNews.fdp.app/Contents/Resources/__boot__.py",
line 65, in
    _run()
  File "/Users/joeuser/Desktop/RecentNews.fdp.app/Contents/Resources/__boot__.py",
line 60, in _run
    exec(compile(source, path, 'exec'), globals(), globals())
  File "/Users/joeuser/Desktop/RecentNews.fdp.app/Contents/Resources/installer.py",
line 49, in
    shutil.copy(fullName,workdir)
  File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/shutil.py",
line 119, in copy
  File
"/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/shutil.py",
line 83, in copyfile
IOError: [Errno 1] Operation not permitted: '/Users/joeuser/.t'
2013-08-01 09:48:34.833 installer[6961:d07] installer Error
2013-08-01 09:48:45.209 installer[6961:3007] Persistent UI failed to open file
file://localhost/Users/joeuser/Library/Saved%20Application%20State/org.pythonmac.unspe
 No such file or directory (2)
```

Er versucht ein Verzeichnis ".t" anzulegen in Home des Users. Der Punkt sorgt dafür, daß das Verzeichnis im Finder normalerweise nicht angezeigt wird. Wenn man Janicab ohne Sandbox laufen läßt, dann legt einen Cronjob für den User an, der die in .t gespeicherten Dateien verwendet:

```
crontab -l
* * * * * python ~/.t/runner.pyc
```



Augrund meiner Sandbox kann Janicab nicht tun, was er will, und endet mit einem Fehler.

Die in meiner Sandbox gestartete Malware wird in ihrer Aktion behindert und ist nicht weiter lauffähig. Ich muß sie erstmal zwingend beenden und sehe die App auch im Dock.

Janicab als laufendes Programm im Dock, also ganz offensichtlich kein Dokument.

Die Dateien, die Janicab in das Verzeichnis kopiert, wenn er normal ausgeführt wird, zeigen, daß er Kommandos von außen abholen möchte, Screenshots und Tonaufnahmen macht. Die Screenshots landen erstmal unter /tmp/cur.jpg. Für Sound-Aufgaben verwendet Janicab SoX, the Swiss Army knife of sound processing programs, ein Open Source Kommandozeilen-Tool für Sound-Verarbeitung. Wenn ich es direkt aufrufe, bestätigt es seine Identität:

```
sandbox-exec -p "(version 1) (allow default) (deny network*) (deny file-write*)
(debug deny)" ./sox
./sox:      SoX v14.4.0

./sox FAIL sox: Not enough input filenames specified

Usage summary: [gopts] [[fopts] infile]... [fopts] outfile [effect [effopt]]...
```

Als Sound-Format bevorzugt Janicab anscheinend OGG. Außerdem verwendet Janicab noch ein weiteres Drittprogramm, das er mitinstalliert: mt, die MouseTools:

```
sandbox-exec -p "(version 1) (allow default) (deny network*) (deny file-write*)
(debug deny)" ./mt

 MouseTools
 Created 31 July 2010 by Hank McShane
 version 0.5
 requires Mac OS X 10.4 or higher

 Updated 18 Nov 2012 by Hank McShane to v0.5
 - added leftClickNoRelease and releaseMouse at the request of a customer

 Updated 22 Feb 2011 by Hank McShane to v0.4
 - added a double click for the left mouse button

 Updated 31 August 2010 by Hank McShane to v0.3
 - fixed and issue where negative x or y values were not being read properly
 - fixed issue where the mouse cursor wasn't updating properly

 Updated 26 August 2010 by Hank McShane to v0.2
 - using simpler method to move the mouse: CGWarpMouseCursorPosition()
 - streamlined stepMouseToPoint()
 - added 64-bit builds for 10.5 and higher

 This foundation tool will help you perform things with your mouse.
 By default, Screen Coordinates are measured from the top-left
 corner of the screen but with the [-b] switch they can be measured
 from the bottom-left.
```

Janicab holt sich Einstellungen von einem Server, benutzt anscheinend FTP und einen Skype-Recorder. Zumindest deuten die Strings in StarterSettings.pyc darauf hin. In StarterCmdExec.pyc finden sich offenbar Funtionen für das Selbstupdate der Malware:

```
CE: handleUpdate: starting update procedure.s!
CE: Copied update file succefullys
/tmp/s
rm -f /tmp/R
CE: update: copy new files to work dirs+
/tmp/installer.app/Contents/Resources/Libscs

CE: copied: s
 to s
CE: detele the update files
rm -rf /tmp/installer.apps
```

StarterNetUtils.pyc richtete augenscheinlich die Crontab ein, prüft, auf welcher Maximum-System-Version Safari läuft mit "defaults read com.apple.Safari LastOSVersionSafariWasLaunchedOn". Neben anderen Dingen, ist dieser Teil wohl auch für die Verbindungsaufnahme mit den Spitzbuben zuständig:

```
Starting backConnect to R
Wrong parameters for backConnecti
/bin/shs
Connected to server at s
```

Eine Logdatei findet sich unter /tmp/starter.log. StarterRec.pyc kümmert sich um Tonaufnahmenim OGG-Format, deren Versandt und das Wegräumen selbiger. Unter anderem wird dazu benutzt:

```
osascript -e 'do shell script "~/.t/sox -q -V6 -d -t ogg s
 trim 0 01:00"'t
```

Der Teil StarterScreenShots.pyc verwendet die MouseTools und macht offenbar Screenshots, immer wenn die Maus bewegt wurde:

```
SS: Starting SS Threadt
SS: last mouse pos: s
SS: new mouse pos: s
SS: Creating new SS at: sN
osascript -e 'do shell script "/usr/sbin/screencapture -x -tjpg /tmp/cur.jpg"'t
shells
SS: delete the ss files%
SS: Same mouse position, Do Nothing..s
```

Insgesamt ist es also ein Spionage-Tool, das allgemeine Informationen über das System, sammelt und verschickt, anscheinend auch Kommandos von außen abfragt. Zusätzlich fertigt es Tonaufnahmen und Screenshots an. Es ist auch damit zu rechnen, daß Skype mitgeschnitten wird. Das Schadprogramm prüft, ob seine Tools brav laufen und aktualisiert sich bei Bedarf. Ehrlich gesagt ist mir ein bißchen übel nach dieser Kurz-Analyse.

Beseitigung

Sollte der genannte Cronjob (siehe oben) mit "crontab -l" auftauchen oder andere angesprochene Dateien aufzufinden sein, dann sollte man mit "crontab -r;rm -rf ~/.t" die Crontab leer machen, denn sie ist per Default auf OS X leer und die Dateien unter ~/.t löschen. Anschließend bitte Ausloggen, damit eventuelle Prozesse auch beendet werden. Dazu rät The Safe Mac und dem kann ich zustimmen.

1332498

Latest Update: 11. September 2015 at 19:49h (german time)
Link: www.macmark.de/blog/osx_blog_2013-08-a.php