# The Safe Mac » New signed malware called Janicab



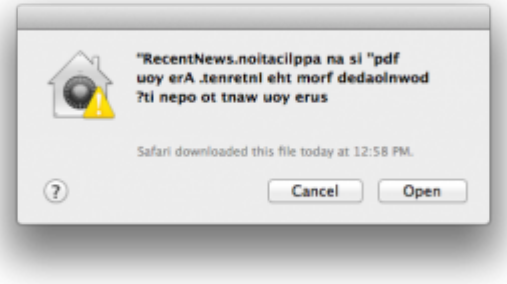
Published July 15th, 2013 at 2:27 PM EDT , modified July 16th, 2013 at 8:11 PM EDT

F-Secure announced the discovery today of a new trojan, which they have named Janicab. This malware makes use of a familiar old trick – disguising an application as a document to trick the user into opening it – but applies a couple newer twists. At this time, the built in defenses in Mac OS X will allow this trojan to run without much in the way of warnings, so users are advised to be on their guard.

The first new twist that makes this malware unique in the Mac world is the use of a right-to-left override (RLO) character in the name. What this character does is tell the system that the characters that follow should be displayed right-to-left, instead of left-to-right as is standard for the English language. Otherwise, the character is invisible.

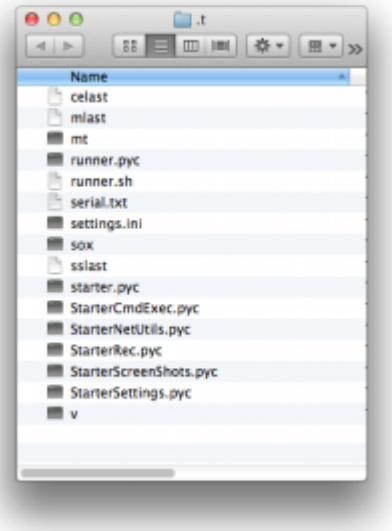
So why does this matter? Because it allows the hacker to hide the fact that the document is actually an application! The file is named “RecentNews.?fdp.app”, where the ‘?’ indicates the presence of the RLO character. This means that the Finder will want to display the name as “RecentNews.ppa.pdf”. In addition, the hackers used the old trick of marking the extension as being hidden, and the system knows the extension is “.app” regardless of how the Finder wants to display the name. Therefore, the name is actually displayed as “RecentNews.pdf”. This, plus the Adobe Acrobat icon given to the application, makes the app look like an innocent PDF file.

(As an interesting side note, I have observed that if I place the file on my desktop, the name gets wrapped in the middle of the “extension” based on my settings. When wrapped like this, the file’s name displays as “RecentNews.fdp”. Perhaps a text encoding expert could explain that one… it seems a bit like voodoo to me! 🙂 )




The second new twist, only exhibited previously by the recent KitM (aka Hackback) malware, is that the app is signed. Thus, the system will allow it to run unimpeded, as long as you approve it on the first run. Although that's a fairly serious issue in principle, if the victim is paying attention, he/she will notice something strange is going on, as most of the text in the warning will be backwards! Still, a lot of people are in the habit of just clicking whatever they need to click to make something work without reading the details of what they're agreeing to. So it's easily conceivable that someone would click the Open button without ever noticing the discrepancy.


When run, the trojan opens a document to avoid causing further suspicion. The astute observer will notice that the Acrobat icon will remain in the Dock and an additional PDF reader will be opened (Preview for most), which should tip off the user that something's not right. Again, though, many people aren't paying that close attention, or may not understand the implications of that. In the meantime, while the document is loading up, it does other nasty things before quitting.




According to F-Secure's post, the app installs a number of components in an invisible folder in the user's home folder (named ".t", where the initial period tells the system to hide the

folder) and creates a cron job to keep components running. Presumably it uses cron since that is older technology that has been abandoned in favor of launchd. Because other malware has used launchd recently, many users may already be aware of how to check for rogue launch agents and launch daemons, but because of its relative obscurity today, most will probably not know how to check for or disable a cron job.

Once installed, this malware locates its command & control server by searching a few specific places for specific text that contains an IP address. After contacting the C&C server, it begins taking screenshots and recording audio, uploading that to the server and polling the server for other commands to run.

At this time, Janicab is not detected by most anti-virus software, and it slips right past the built-in defenses of Mac OS X in the hands of an unobservant or unsavvy user. This makes it very dangerous. Further, seeing other malware using a signed app is troubling, as it may indicate that Gatekeeper will not offer as much security as had been hoped for.

Removal should be fairly easy. However, you need to take great care. Be sure you have up-to-date backups of all your data, then *read the instructions below carefully and follow them precisely*!

The following command should be copied and pasted into the Terminal (which is found in the Utilities folder in the Applications folder). **Do not try to re-type this command!** A simple typo as simple as a space added in the wrong place could have disastrous consequences. Also, note that this will remove all cron jobs. That is the default state in Mountain Lion (Mac OS X 10.8), but much earlier versions of Mac OS X may differ (though I don't know yet what versions of Mac OS X this malware is capable of infecting), and of course if you have created your own cron jobs, this will disrupt them.

```
crontab -r;rm -rf ~/.t
```

Once you have run this command, log out to ensure that all the malicious processes still loaded into memory are terminated. When you log back in, the malware should be gone.

## Updates

July 16, 2013: Looks like the developer certificate used to sign this trojan has already been revoked. I just tested it, and trying to open the app now results in only two choices: cancel or move it to the trash.

Tags: Gatekeeper, Janicab, Mac OS X, malware, trojan

---