Komplex Mac backdoor answers old questions

blog.malwarebytes.com/threat-analysis/2016/09/komplex-mac-backdoor-answers-old-questions/

Thomas Reed

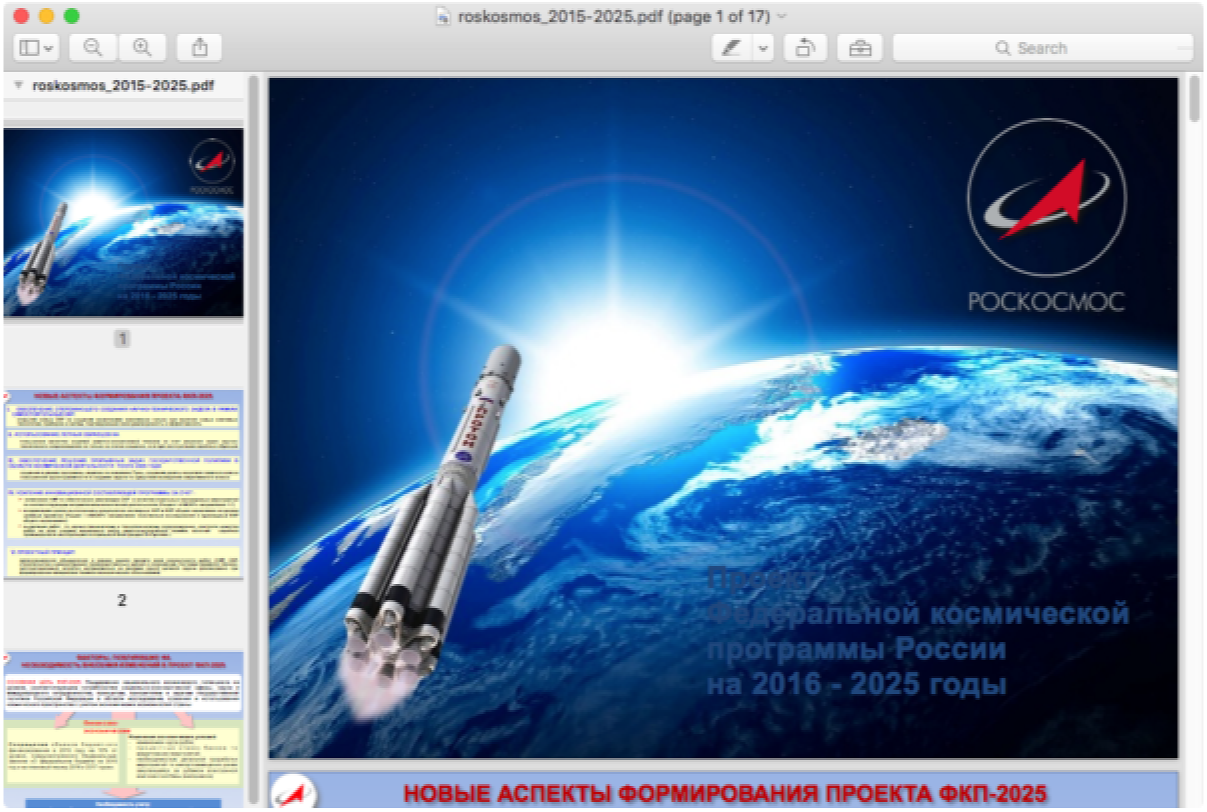
September 27, 2016

A new piece of Mac malware, dubbed Komplex, has been discovered by Palo Alto Networks. This malware provides a backdoor into the system, like most other recent Mac malware. Where it gets most interesting, though, isn't in its capabilities, but in the connections it allows us to make.

The implementation of Komplex is actually anything but complex. The end product of infection is nothing more than a launch agent masquerading as an Apple updater and a hidden executable that is kept running by that launch agent. Trivial in execution, trivial to detect, and trivial to remove.

The details of how the malware gets installed are still partly unknown. Palo Alto provided information about three different "binder" files, which are executable files that begin the process of installing the malware. What's not said, however, is how these files get executed on the user's system.

Those "binders" perform two tasks. The first is to install and run another executable at /tmp/content. The second is to create a PDF file – containing information about the Russian Federal Space Program – in the Downloads folder and open it. This is common behavior among Trojan apps that masquerade as some kind of document; they typically will create and open a decoy document, in an attempt to prevent the user from noticing that anything strange happened.



Проект
Федеральной космической
программы России
на 2016 - 2025 годы

НОВЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ПРОЕКТА ФКП-2025

(I've seen a few people under the impression that this is a PDF exploit, but there's no indication that this is the case at this time.)

The executable at /tmp/content is the "dropper" that actually installs the malicious payload. That payload consists of the following files:

```
/Users/Shared/.local/kextd
/Users/Shared/start.sh
~/Library/LaunchAgents/com.apple.updates.plist
```

The start.sh file is used to load the launch agent, which in turn ensures that the kextd process is kept running persistently.

After the installation is complete, the original "binder," the /tmp/content file and the start.sh file are all deleted.

In all, this is just more of the same old Mac malware. It doesn't even have quite the same level of backdoor capabilities as most of the new backdoors that have appeared this year. However, what makes this interesting is the connections it allows us to make with other malware.

Palo Alto makes a connection between this malware and other malware created by the Sofacy Group, an organization that is known to target governments. Sofacy appears to be a Russian group, possibly funded by the Russian government, and are considered to be involved in the recent Democratic National Committee hacking.

That's interesting, but perhaps more fascinating to Mac security folks is an additional connection made with an unnamed piece of malware discovered last year, which installed via a vulnerability in the MacKeeper app. Little was known about the malware beyond what BAE Systems published.

Now we seem to have the answer to the question of what that malware was. Palo Alto Networks identified a number of compelling code similarities between Komplex and that unnamed malware. Not only does this put a name to that old malware, but it also shows that Sofacy has had their eyes on the Mac for some time now.

Interestingly, although the method of infection has changed, not much seems to have changed about the payload, which was also a launch agent tasked with loading an executable file from the /Users/Shared folder.

Malwarebytes Anti-Malware for Mac detects the dropped components as OSX.Komplex.