Digitally signed data-stealing malware targets Mac users in “undelivered courier item” attack

nakedsecurity.sophos.com/2014/01/21/data-stealing-malware-targets-mac-users-in-undelivered-courier-item-attack/

By Paul Ducklin 21 Jan 2014

Our colleagues at SophosLabs pointed us at a interesting item of malware the other day, namely a data-stealing Trojan aimed at Mac users.

In fact, it was somewhat more than that: it was one of those “undelivered courier item” emails linking to a dodgy web server that guessed whether you were running Windows or OS X, and targeted you accordingly.

You’re probably familiar with “undelivered item” scams.

The idea is surprisingly simple: you receive an email that claims to be a courier company that is having trouble delivering your article.

In the email is a link to, or an attachment containing, what purports to be a tracking note for the item.

You are invited to review the relevant document and respond so that delivery can be completed.

We've seen a wide variety of courier brands "borrowed" for this purpose, including DHL, the UK's Royal Mail and even, in one bewildering case, a made-up courier company called TNS24, with its very own website, featuring its very own amusingly ill-Photoshopped planes, ships and automobiles.

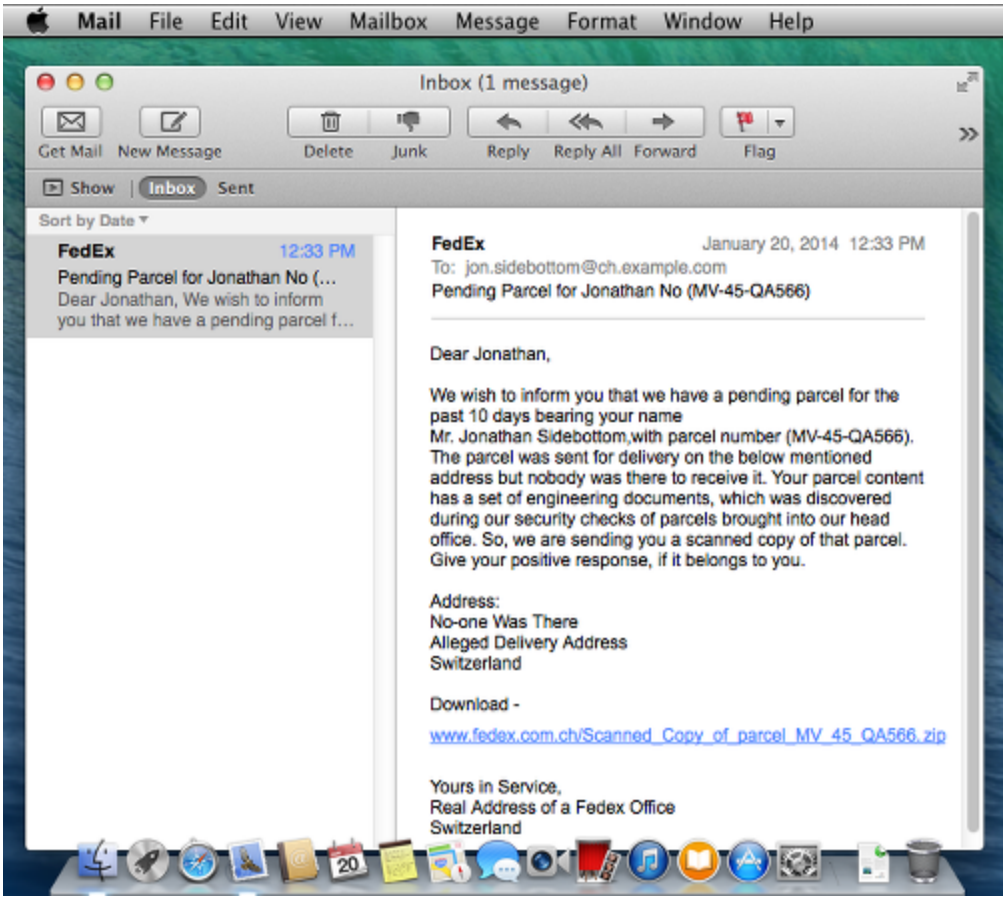
But a competently-executed courier scam can be fairly convincing, especially if the criminals behind it know enough about you to create what becomes a *targeted attack*.

Even a modest amount of detail (if that is not an oxymoron) can do the trick.

For example, the crooks will sound a lot more believable if they know your address and phone number; are aware of what you do in your job; and have a general idea about some of the projects you are working on right now.

Of course, if you open the attachment or click on the link in one of these scams, you are immediately put into harm's way: the attachment might try to trigger an exploit in your unpatched copy of Word, for instance, or the link might attack an unpatched Java plugin in your browser.

Here's what the emails looked like in this attack, with some details changed or redacted for safety:



> We wish to inform you that we have a pending parcel for the past 10 days bearing your name Mr. Jonathan Sidebottom,with parcel number (MV-45-QA566). The parcel was sent for delivery on the below mentioned address but nobody was there to receive it. Your parcel content has a set of engineering documents, which was discovered during our security checks of parcels brought into our head office. So, we are sending you a scanned copy of that parcel. Give your positive response, if it belongs to you.

If you are a native speaker of English, you will notice that the wording of the email is clumsy and unidiomatic, and if you were to receive a message like this you might well be suspicious on those grounds alone.

But if Mr Sidebottom really is in the engineering business, and regularly deals with inbound documents from courier companies around the world, an email of this sort could easily pass muster.

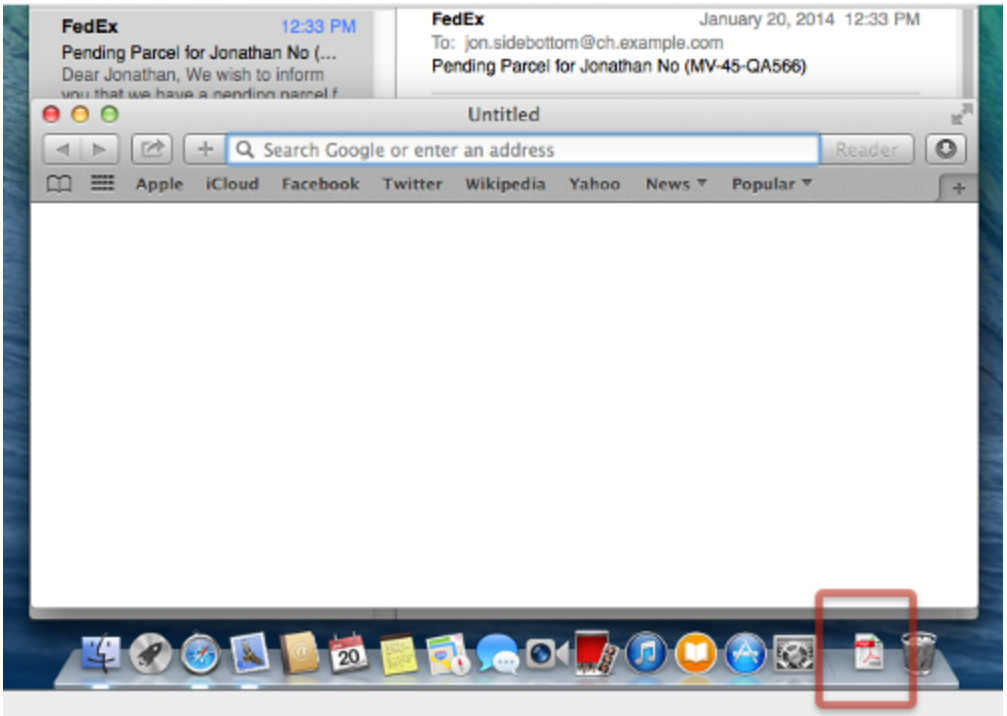
The link, of course, doesn't really lead to `fedex.com.ch`, but instead takes you to a domain name that is controlled by the attackers.

If you are on a mobile device, the server delivers an error message.

If you are using a desktop browser that isn't Safari, you receive a ZIP file containing a Windows program detected by Sophos Anti-Virus as **Mal/VBCheMan-C**, a vague relative of the Zbot or Zeus malware.

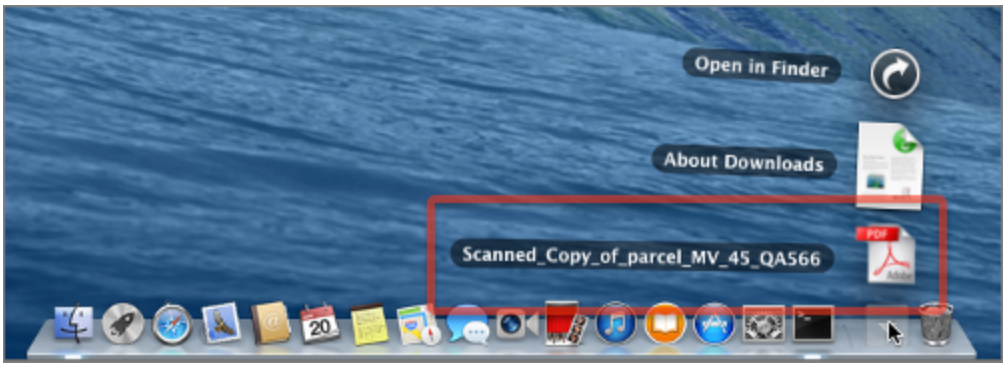
But if you are using Safari, you receive Mac malware, delivered as an Application bundle packaged inside a ZIP file.

By default, on OS X 10.9.1 (the latest update to Mavericks, Apple's most recent operating system version), Safari directly downloads the file, showing you an empty Safari window with the icon of the downloaded file in the Dock at the bottom of the screen:



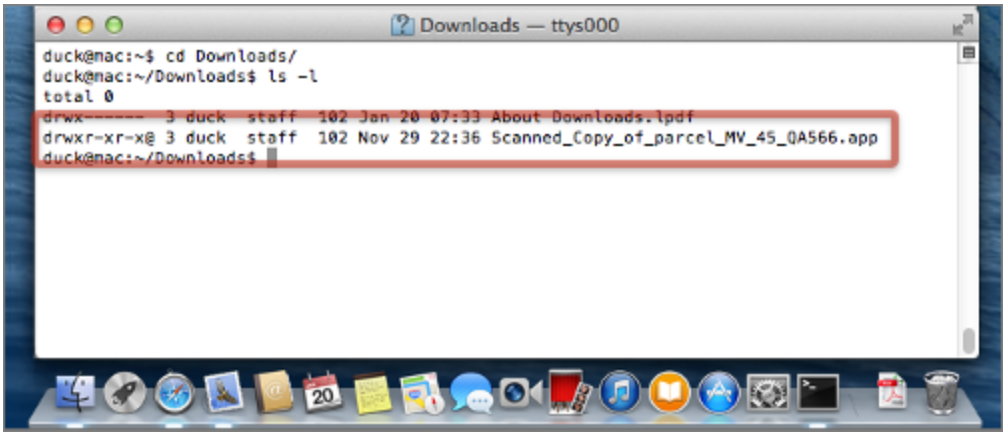
Clicking the email link automatically brings down a file that appears to be a PDF

Clicking on the download button shows you what looks like a PDF file:



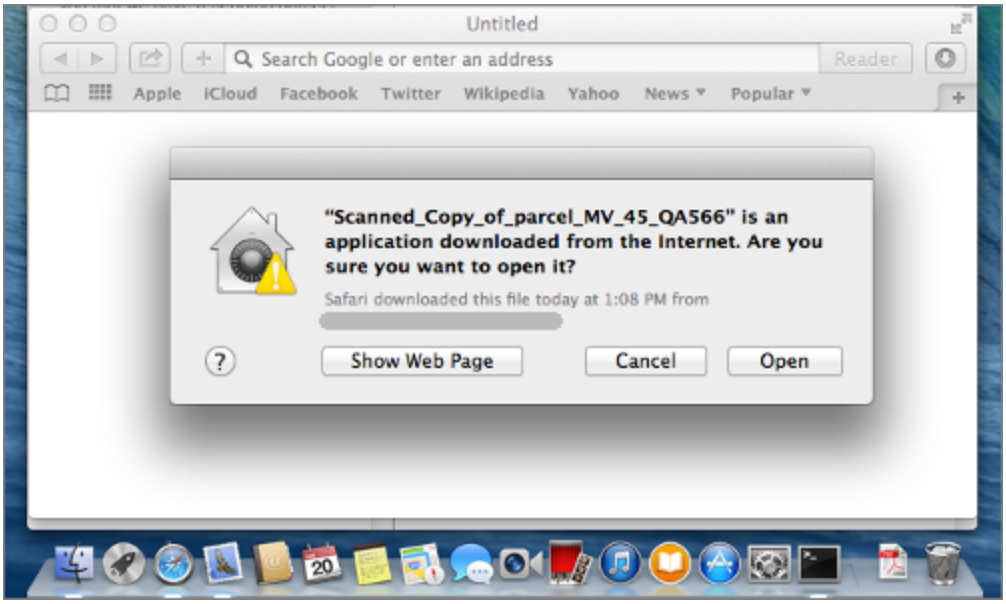
There is no PDF file, as a visit to the Terminal windows quickly reveals.

Safari has automatically unzipped the download, producing an Application bundle (actually just a subdirectory tree with a special structure) that has deliberately been given a PDF icon:



As you can imagine, the temptation is to click on what looks like a PDF file to see what it contains.

OS X does try to advise you that you aren't opening a document, although you can argue that the warning would be more compelling if it explicitly said that you were about to "run a software program", rather than merely to "open" the file:

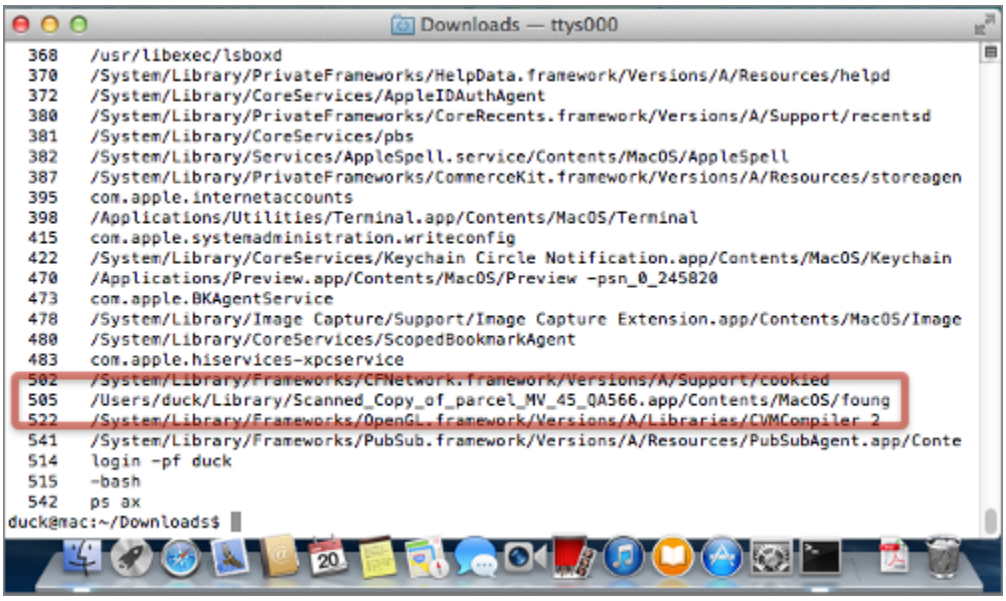


Note that you don't get a warning about the App being from an "unknown developer" because it is digitally signed, something that happens surprisingly often with modern malware.

→ The quantity of digitally-signed malware in circulation prompted Microsoft, which sees a lot more malware than Apple, to publish a recent blog post with the uncompromising title "Be a real security pro – Keep your private keys private." In that article, Microsoft documents a malware family it calls "Winwebsec" of which it has more than 15,000 digitally-signed samples, signed with 12 different stolen keys.

If you do click the `[Open]` button, nothing seems to happen: you end up back at the desktop with your email software open and an empty Safari window in front of it.

But a trip back to the Terminal shows that what looked like a PDF file is now running in the background as a process named `foung`:



As it happens, `foung`, like its counterpart delivered to Windows computers, is a bot, short for “robot malware”, detected by Sophos Anti-Virus as **OSX/LaoShu-A**.

LaoShu-A as good as hands control of your Mac over to the attackers, but its primary functions appear to be more closely associated with data stealing than with co-opting you into a traditional money-making botnet.

(You will often hear the term RAT, or Remote Access Trojan, rather than the more common term bot, used to describe this sort of malware.)

In other words, the attackers seem more concerned with digging around on your computer for what they can steal than with abusing your computer and your internet connection to aid and abet other cybercriminal activities.

Amongst other things, LaoShu-A contains code to:

- Search for files with extensions such as DOC, DOCX, XLS, XLSX, PPT and PPTX.
- ZIP those files.
- Upload (*exfiltrate*) them to a server operated by the attackers.

However, this RAT also knows how to:

- Download new files.
- Run arbitrary shell commands.

For example, during our tests, LaoShu-A downloaded a second application that took a screenshot with OS X’s built-in `screencapture` command, and tried to exfiltrate the image it had just grabbed.

But the behaviour of that second application can be varied by the attackers at any time, which is why, in our recent podcast, *Understanding botnets*, SophosLabs expert James Wyke warned as follows:

> Without analysing the full network capture of the entire interchange between a bot and the person controlling it, you can't say for sure exactly what that bot might have done... [it] might go and download some completely different piece of malware which carries out a completely different set of functionality.

James went on to recommend:

> Be more suspicious of things you get in e-mail. E-mail is still one of the most common ways people get infected, and it is predominantly through social engineering attacks... So when you receive an e-mail from someone you've never heard of before, or you've never communicated with before, and there's some interesting attachment to the e-mail or [a link to click], ...don't do that! That's one of the that most common ways people get infected.

LISTEN NOW

(Audio player not working? Listen on Soundcloud.)

Let's hope this malware reminds OS X users of a few simple truths that some Mac fans still seem willing to ignore:

- Mac malware is unusual, but not impossible.
- Data thieves are interested in what Mac users have on their computers.
- Malware writers can often get their hands on digital certificates to give software to give it a veneer of respectability and to bypass operating system warnings.
- Mac malware doesn't have to ask for a password before running.
- Mac malware can run directly from a download without an installation step.
- Bots and RATs are particularly pernicious because they can update and adapt their behaviour after you are infected.

As always, prevention is better than cure.

And that "undelivered courier item" almost certainly doesn't exist.

Free: Sophos Anti-Virus for Mac Home Edition

Sophos for Mac stops threats for Windows and Mac alike, protecting you and those you share files with.

Choose from blocking viruses in real time (on-access protection), scanning at scheduled times, or running a check whenever you want.

Free download, no registration required, no expiry date.

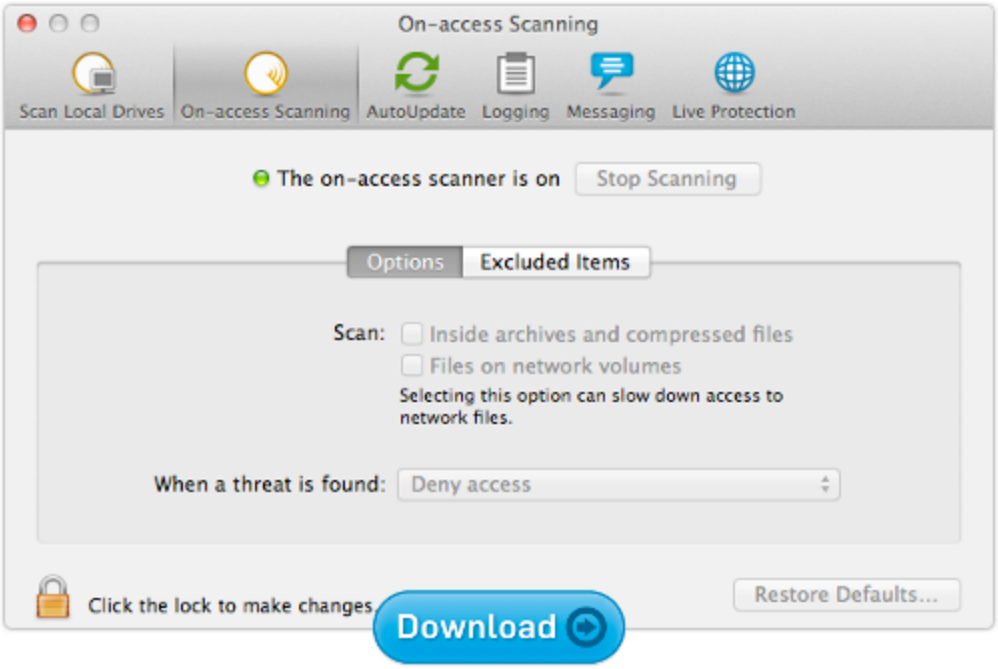


Image of forklift courtesy of Shutterstock.