January 2004 to September 2015

archive.f-secure.com/weblog/archives/00002576.html

F-SECURE LABS

<<< NEWS FROM THE LAB - Monday, July 15, 2013 >>>

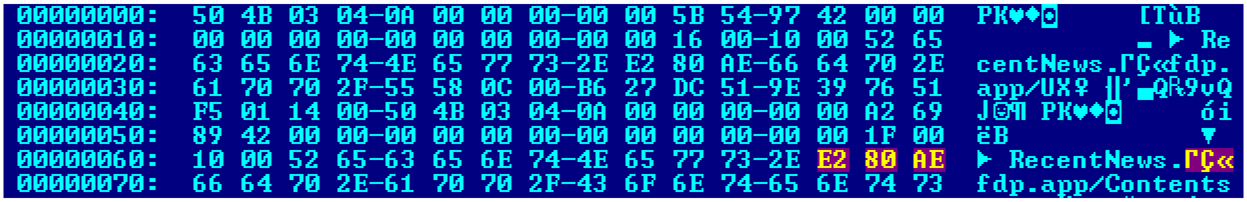
ARCHIVES | SEARCH

Signed Mac Malware Using Right-to-Left Override Trick

Posted by Brod @ 10:48 GMT

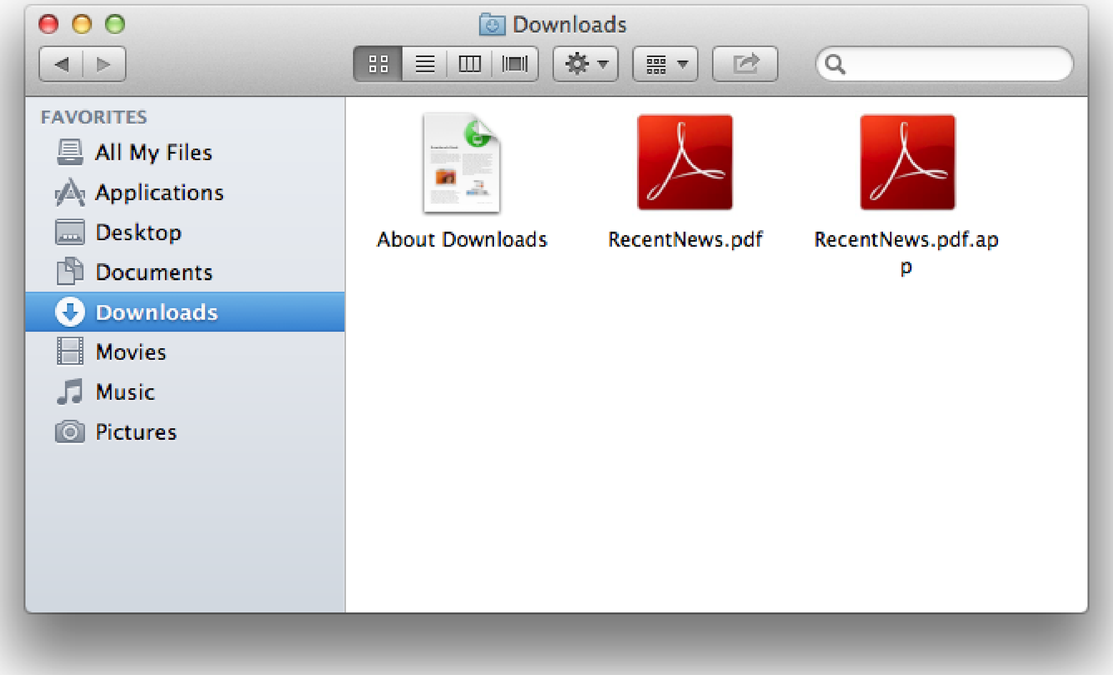
Right-to-left override (RLO) is a special character used in bi-directional text encoding system to mark the start of text that are to be displayed from right to left. It is commonly used by Windows malware such as Bredolab and the high-profile Mahdi trojan from last year to hide the real extension of executable files. Check out this Krebs on Security post for more details on the trick.

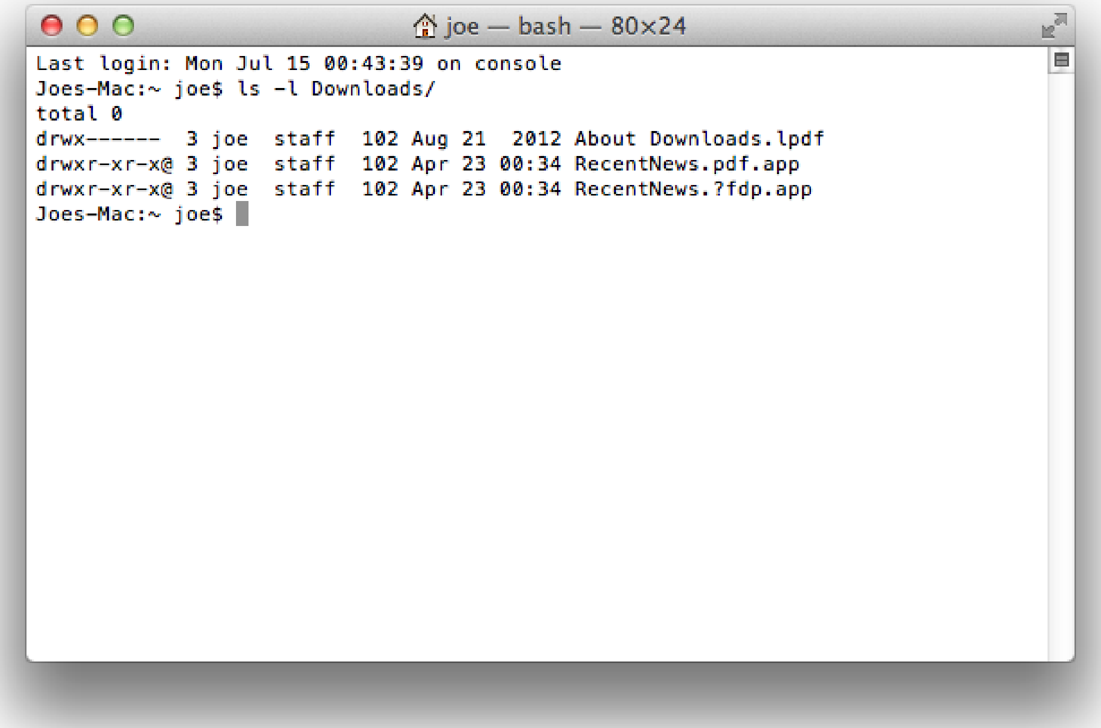
We've spotted a malware for Mac using the RLO trick. It was submitted to VirusTotal last Friday.



```
00000000:  50 4B 03 04-0A 00 00 00-00 00 5B 54-97 42 00 00  PK♥♦◙     [TùB
00000010:  00 00 00 00-00 00 00 00-00 00 16 00-10 00 52 65            ▬ ► Re
00000020:  63 65 6E 74-4E 65 77 73-2E E2 80 AE-66 64 70 2E  centNews.ΓÇ«fdp.
00000030:  61 70 70 2F-55 58 0C 00-B6 27 DC 51-9E 39 76 51  app/UX♀ ╢'▄Q₧9vQ
00000040:  F5 01 14 00-50 4B 03 04-0A 00 00 00-00 00 A2 69  J☺¶ PK♥♦◙     ói
00000050:  89 42 00 00-00 00 00 00-00 00 00 00-00 00 1F 00  ëB            ▼
00000060:  10 00 52 65-63 65 6E 74-4E 65 77 73-2E E2 80 AE  ► RecentNews.ΓÇ«
00000070:  66 64 70 2E-61 70 70 2F-43 6F 6E 74-65 6E 74 73  fdp.app/Contents
```

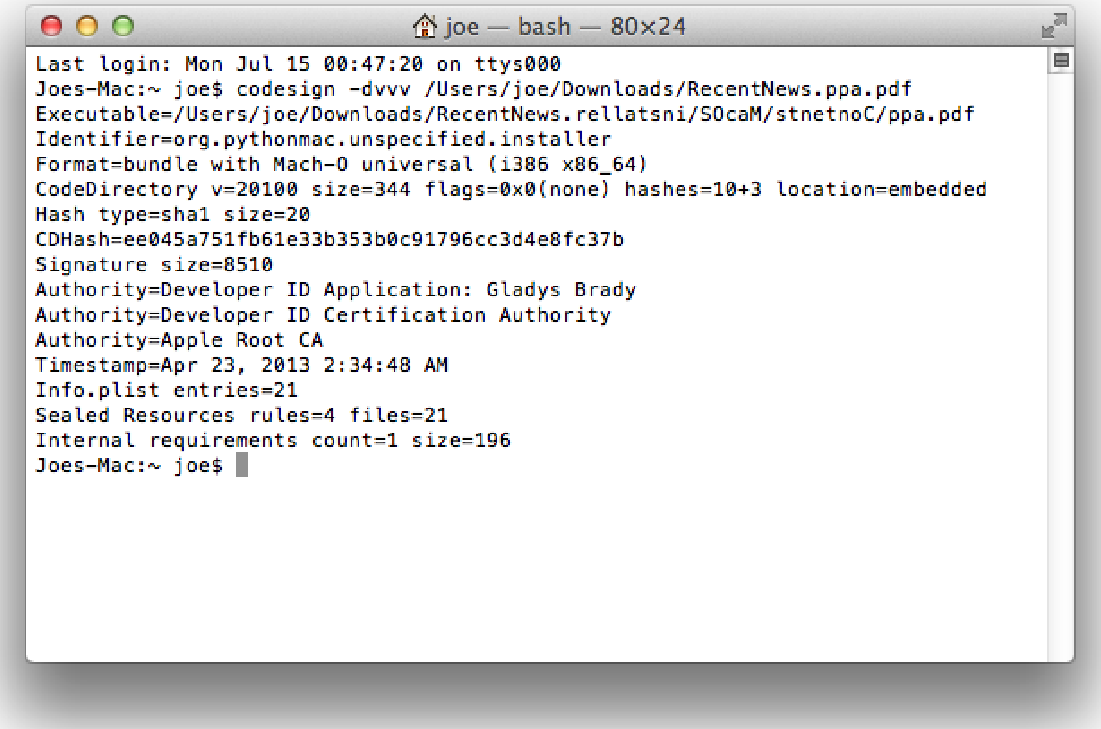
The objective here is not as convoluted as the one described in Kreb's post. Here it's simply to hide the real extension. The malware could have just used "Recent New.pdf.app". However OS X has already considered this and displays the real extension as a precaution.





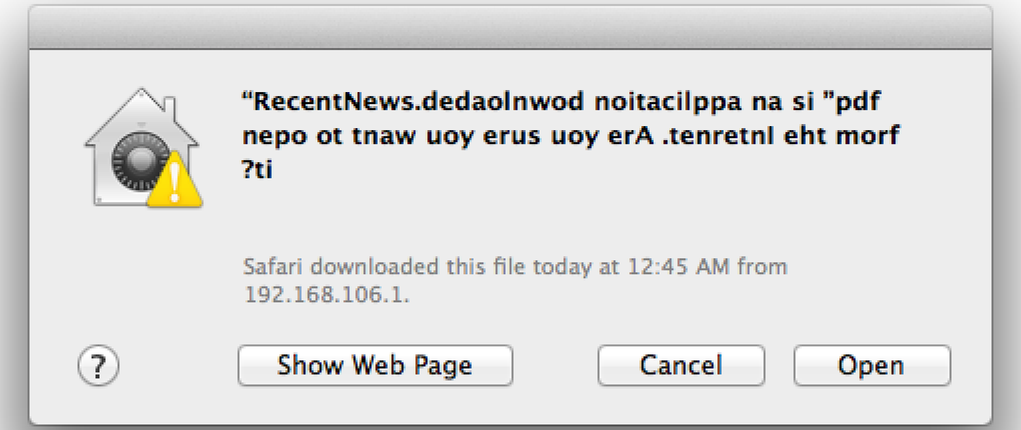
```
Last login: Mon Jul 15 00:43:39 on console
Joes-Mac:~ joe$ ls -l Downloads/
total 0
drwx------  3 joe  staff  102 Aug 21  2012 About Downloads.lpdf
drwxr-xr-x@ 3 joe  staff  102 Apr 23 00:34 RecentNews.pdf.app
drwxr-xr-x@ 3 joe  staff  102 Apr 23 00:34 RecentNews.?fdp.app
Joes-Mac:~ joe$
```

The malware is written in Python and it uses py2app for distribution. Just like Hackback, it's signed with an Apple Developer ID.



```
Last login: Mon Jul 15 00:47:20 on ttys000
Joes-Mac:~ joe$ codesign -dvvv /Users/joe/Downloads/RecentNews.ppa.pdf
Executable=/Users/joe/Downloads/RecentNews.rellatsni/SOcaM/stnetnoC/ppa.pdf
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=Apr 23, 2013 2:34:48 AM
Info.plist entries=21
Sealed Resources rules=4 files=21
Internal requirements count=1 size=196
Joes-Mac:~ joe$
```

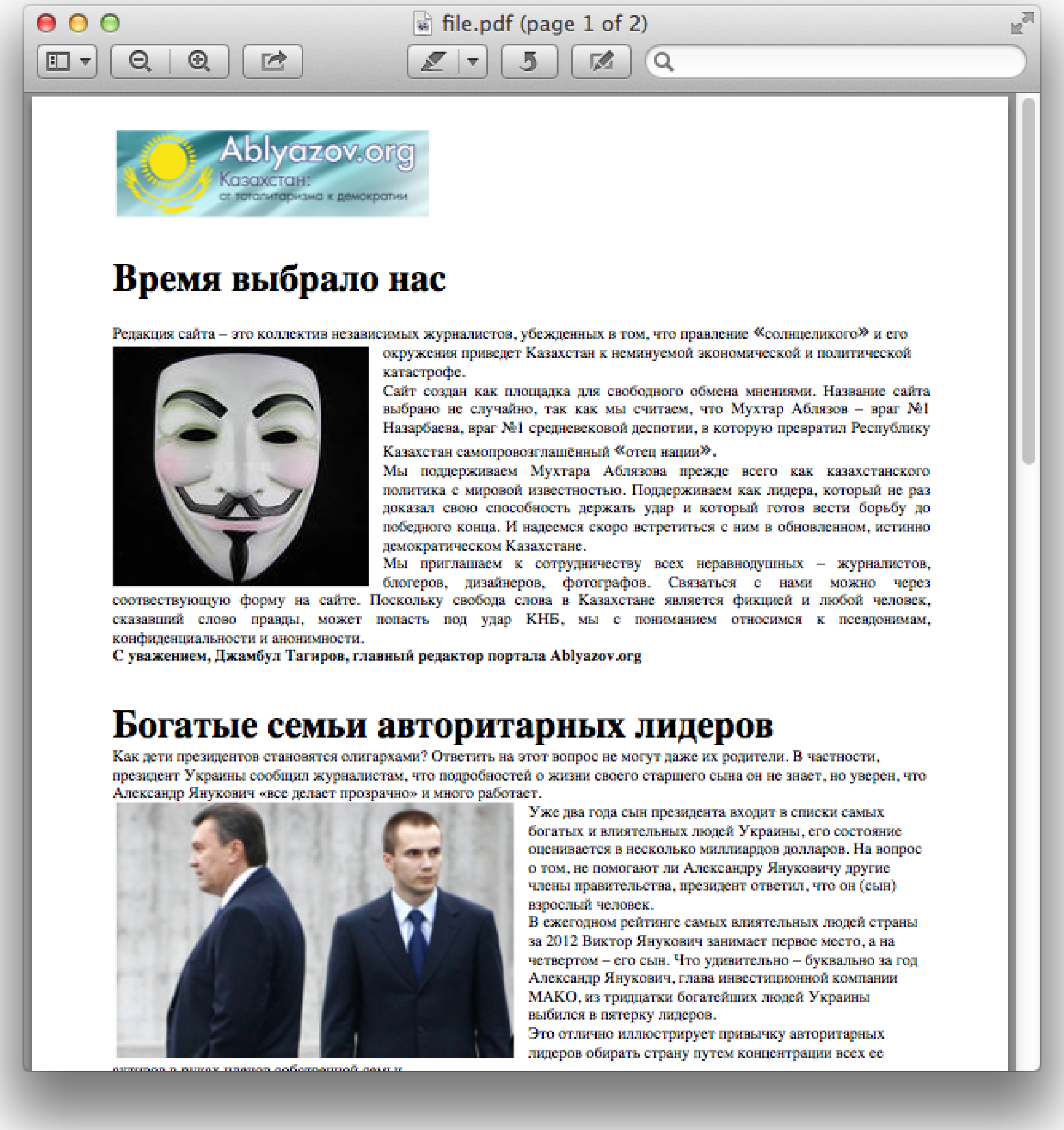
However, because of the RLO character, the usual file quarantine notification from OS X will be backwards just like the Krebs case.



“RecentNews.dedaolnwod noitacilppa na si ”pdf nepo ot tnaw uoy erus uoy erA .tenretnl eht morf ?ti

Safari downloaded this file today at 12:45 AM from 192.168.106.1.

The malware drops and open a decoy document on execution.



Время выбрало нас

Редакция сайта – это коллектив независимых журналистов, убежденных в том, что правление «солнцеликого» и его окружения приведет Казахстан к неминуемой экономической и политической катастрофе.

Сайт создан как площадка для свободного обмена мнениями. Название сайта выбрано не случайно, так как мы считаем, что Мухтар Аблязов – враг №1 Назарбаева, враг №1 средневековой деспотии, в которую превратил Республику Казахстан самопровозглашённый «отец нации».

Мы поддерживаем Мухтара Аблязова прежде всего как казахстанского политика с мировой известностью. Поддерживаем как лидера, который не раз доказал свою способность держать удар и который готов вести борьбу до победного конца. И надеемся скоро встретиться с ним в обновленном, истинно демократическом Казахстане.

Мы приглашаем к сотрудничеству всех неравнодушных – журналистов, блогеров, дизайнеров, фотографов. Связаться с нами можно через соотвествующую форму на сайте. Поскольку свобода слова в Казахстане является фикцией и любой человек, сказавший слово правды, может попасть под удар КНБ, мы с пониманием относимся к псевдонимам, конфиденциальности и анонимности.

С уважением, Джамбул Тагиров, главный редактор портала Ablyazov.org

Богатые семьи авторитарных лидеров

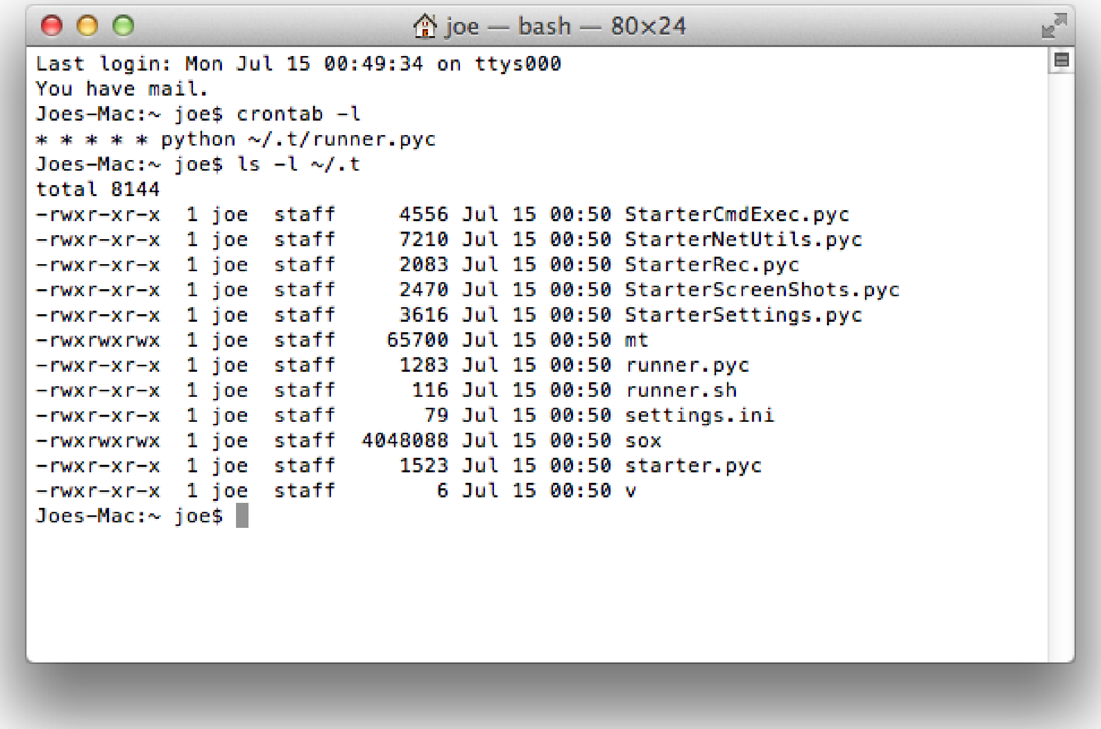
Как дети президентов становятся олигархами? Ответить на этот вопрос не могут даже их родители. В частности, президент Украины сообщил журналистам, что подробностей о жизни своего старшего сына он не знает, но уверен, что Александр Янукович «все делает прозрачно» и много работает.

Уже два года сын президента входит в списки самых богатых и влиятельных людей Украины, его состояние оценивается в несколько миллиардов долларов. На вопрос о том, не помогают ли Александру Януковичу другие члены правительства, президент ответил, что он (сын) взрослый человек.

В ежегодном рейтинге самых влиятельных людей страны за 2012 Виктор Янукович занимает первое место, а на четвертом – его сын. Что удивительно – буквально за год Александр Янукович, глава инвестиционной компании МАКО, из тридцатки богатейших людей Украины выбился в пятерку лидеров.

Это отлично иллюстрирует привычку авторитарных лидеров обирать страну путем концентрации всех ее активов в руках членов собственной семьи и

Then it creates a cron job for its launch point and a hidden folder in the home directory of the infected user to store its components.



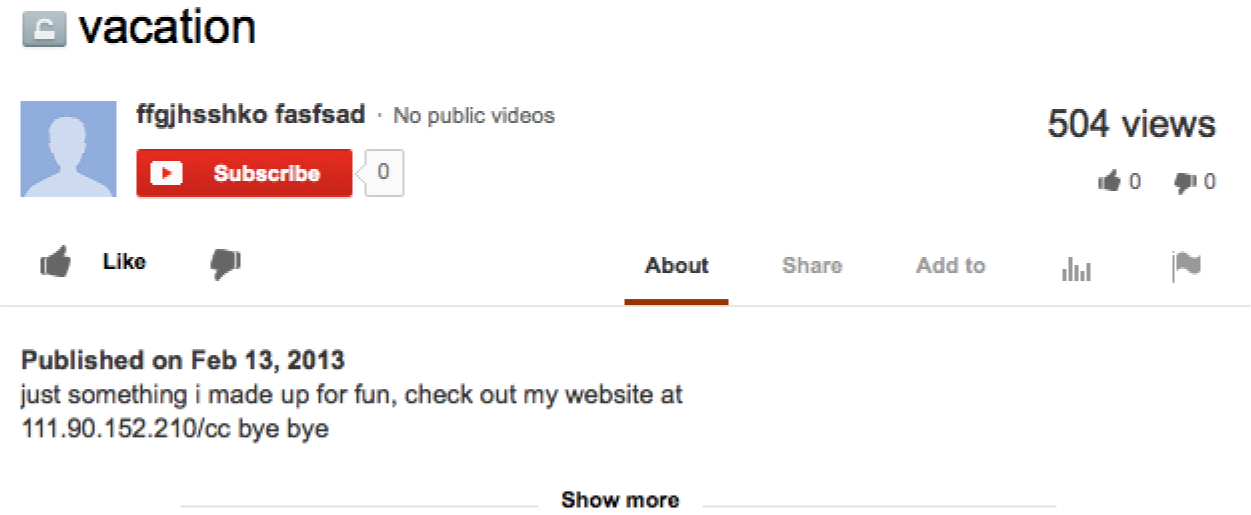
```
Last login: Mon Jul 15 00:49:34 on ttys000
You have mail.
Joes-Mac:~ joe$ crontab -l
* * * * * python ~/.t/runner.pyc
Joes-Mac:~ joe$ ls -l ~/.t
total 8144
-rwxr-xr-x  1 joe  staff     4556 Jul 15 00:50 StarterCmdExec.pyc
-rwxr-xr-x  1 joe  staff     7210 Jul 15 00:50 StarterNetUtils.pyc
-rwxr-xr-x  1 joe  staff     2083 Jul 15 00:50 StarterRec.pyc
-rwxr-xr-x  1 joe  staff     2470 Jul 15 00:50 StarterScreenShots.pyc
-rwxr-xr-x  1 joe  staff     3616 Jul 15 00:50 StarterSettings.pyc
-rwxrwxrwx  1 joe  staff    65700 Jul 15 00:50 mt
-rwxr-xr-x  1 joe  staff     1283 Jul 15 00:50 runner.pyc
-rwxr-xr-x  1 joe  staff      116 Jul 15 00:50 runner.sh
-rwxr-xr-x  1 joe  staff       79 Jul 15 00:50 settings.ini
-rwxrwxrwx  1 joe  staff  4048088 Jul 15 00:50 sox
-rwxr-xr-x  1 joe  staff     1523 Jul 15 00:50 starter.pyc
-rwxr-xr-x  1 joe  staff        6 Jul 15 00:50 v
Joes-Mac:~ joe$
```

The malware connects to the following pages to obtain the address of its command and control server:

- http://www.youtube.com/watch?v=DZZ3tTTBiTs
- http://www.youtube.com/watch?v=ky4M9kxUM7Y
- http://hjdullink.nl/images/re.php

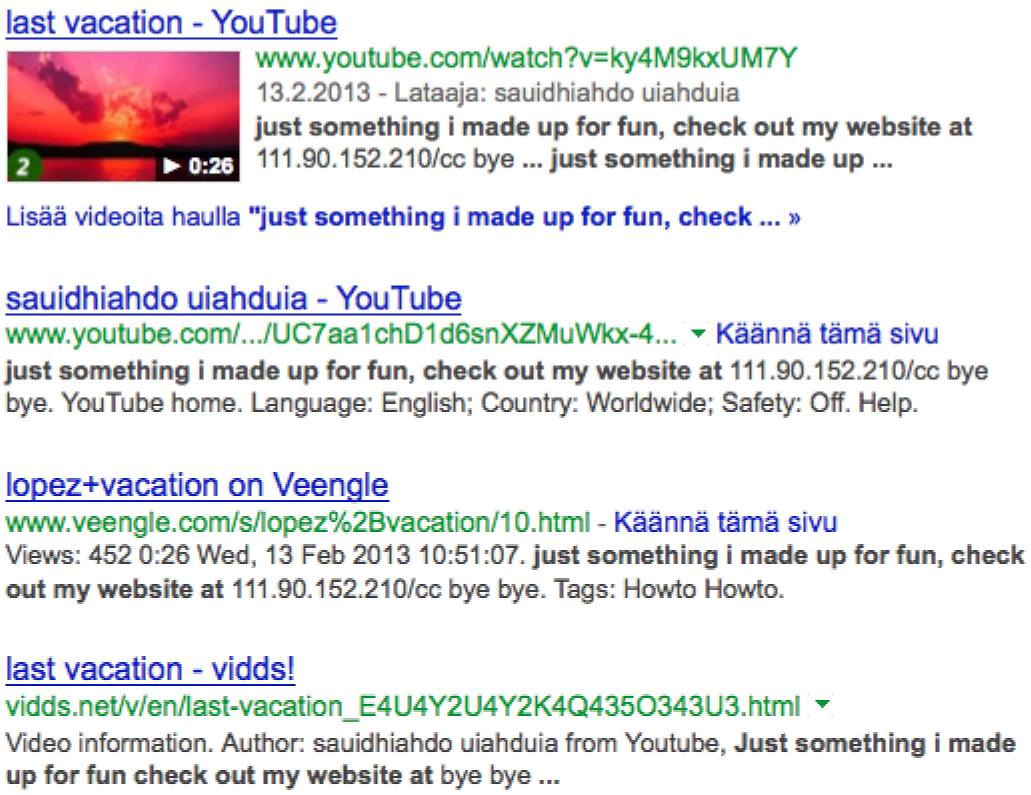
It parses for the address in the string "just something i made up for fun, check out my website at (address) bye bye".

The YouTube page look like this:



Published on Feb 13, 2013
just something i made up for fun, check out my website at
111.90.152.210/cc bye bye

Doing a Google search for the string reveals that there are other sites being abused besides those mentioned above.



last vacation - YouTube
www.youtube.com/watch?v=ky4M9kxUM7Y
13.2.2013 - Lataaja: sauidhiahdo uiahduia
just something i made up for fun, check out my website at 111.90.152.210/cc bye ... **just something i made up ...**

Lisää videoita haulla **"just something i made up for fun, check ... »**

sauidhiahdo uiahduia - YouTube
www.youtube.com/.../UC7aa1chD1d6snXZMuWkx-4... ▾ Käännä tämä sivu
just something i made up for fun, check out my website at 111.90.152.210/cc bye bye. YouTube home. Language: English; Country: Worldwide; Safety: Off. Help.

lopez+vacation on Veengle
www.veengle.com/s/lopez%2Bvacation/10.html - Käännä tämä sivu
Views: 452 0:26 Wed, 13 Feb 2013 10:51:07. **just something i made up for fun, check out my website at** 111.90.152.210/cc bye bye. Tags: Howto Howto.

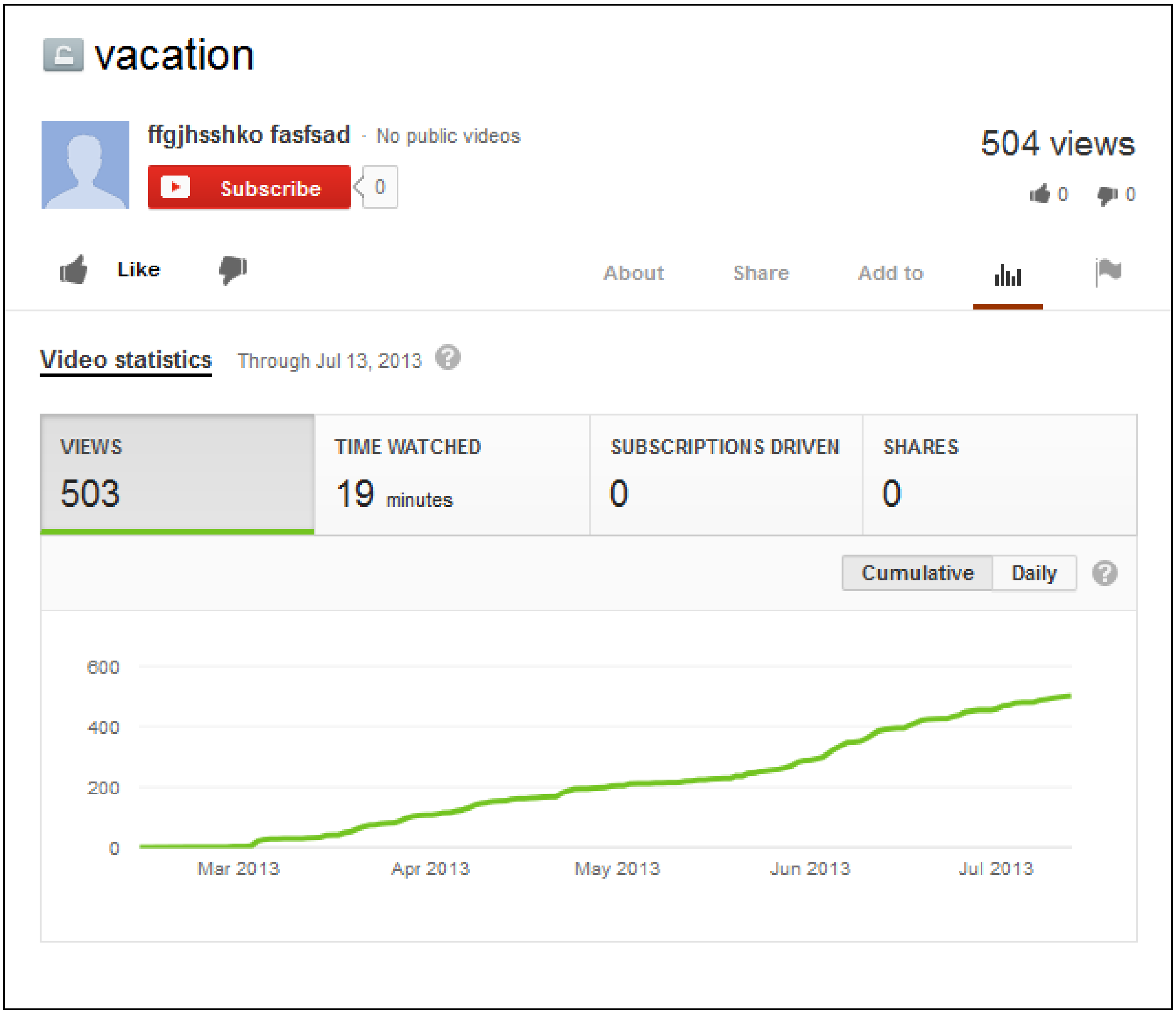
last vacation - vidds!
vidds.net/v/en/last-vacation_E4U4Y2U4Y2K4Q435O343U3.html ▾
Video information. Author: sauidhiahdo uiahduia from Youtube, **Just something i made up for fun check out my website at** bye bye ...

The malware then continuously takes screen shots and records audio (using a third party software called SoX) and uploads them to the command and control server. It also continuously polls the command and control server for commands to execute.

The malware is detected by F-Secure as Backdoor:Python/Janicab.A.

Updated to add:

Here are the stats from one of the YouTube videos being used as a C&C locater:



vacation

ffgjhsshko fasfsad · No public videos

Subscribe 0

504 views

0 0

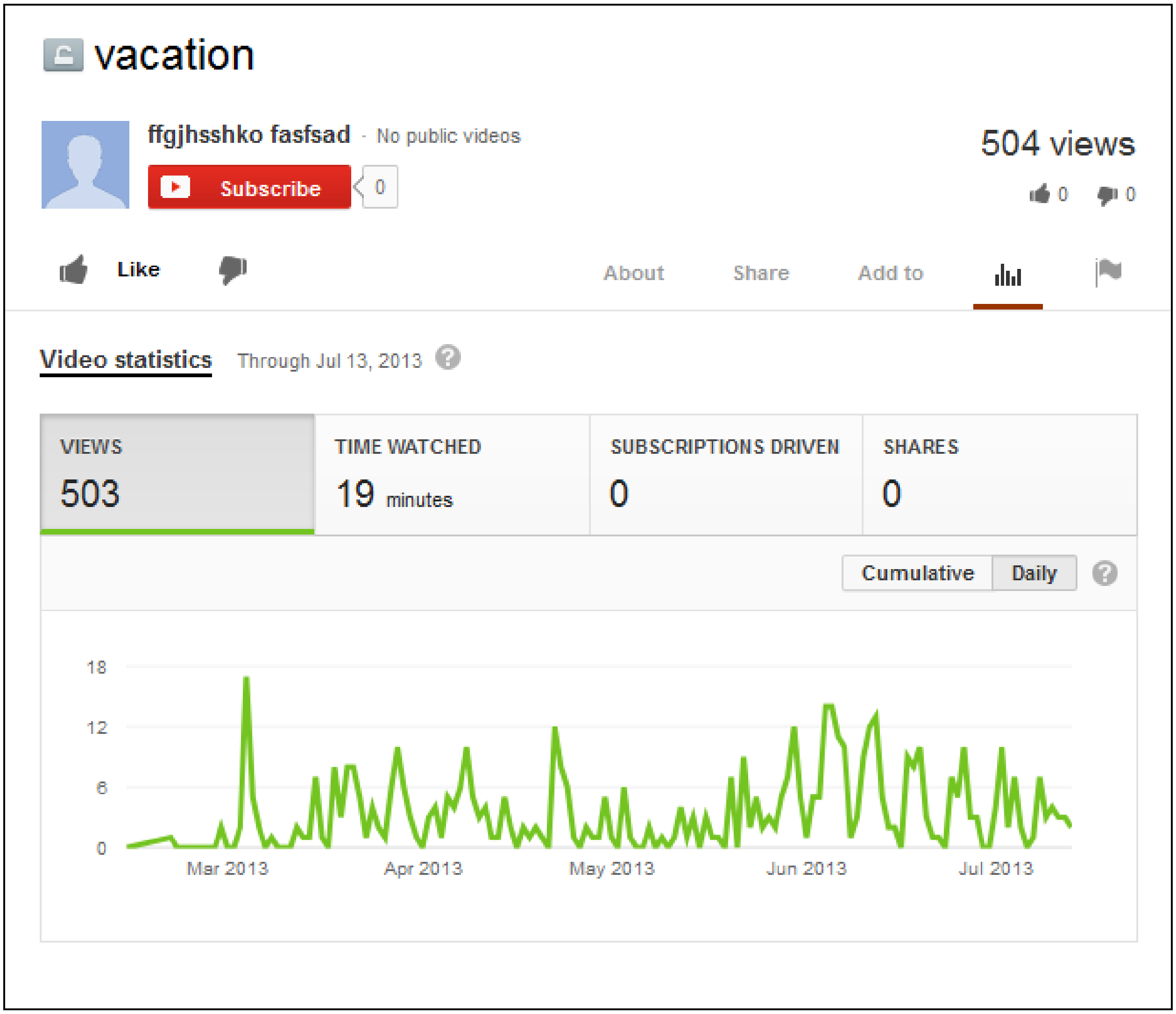
Like

About Share Add to

Video statistics Through Jul 13, 2013

VIEWS	TIME WATCHED	SUBSCRIPTIONS DRIVEN	SHARES
503	19 minutes	0	0

Cumulative Daily



vacation

ffgjhsshko fasfsad · No public videos

504 views

Video statistics Through Jul 13, 2013

VIEWS	TIME WATCHED	SUBSCRIPTIONS DRIVEN	SHARES
503	19 minutes	0	0

The videos predate the Janicab.A binary by at least a month. Based on the stats, it seems likely there are earlier variants in the wild.