1. Skip to navigation
2. Skip to content
3. Skip to secondary-content

F-Secure

Tools

Choose Location:

Labs

Search

Search Go

Navigation

- **Labs**
- **News**
- **Threats**
- **How To**
- **Submit Samples**
- **Beta Programs**
-

Subnavigation

- Virus and Threat descriptions
- Mobile Security
- Vulnerability Protection
- Classifications

Labs

- Latest Threats
- Submit Samples (SAS)
- Free Tools
- Terminology

Where You Are

1. Labs
2. Threats
3. Virus and threat descriptions
4. Trojan-Downloader:OSX/Flashback.I

Trojan-Downloader:OSX/Flashback.I

Detection Names:	Exploit:Java/Flashback.I, Trojan-Downloader:OSX/Flashback.I, Trojan:OSX/Flashback.I, Backdoor:OSX/Flashback.I
Category:	Malware
Type:	Trojan-Downloader
Platform:	OSX

Summary

Trojan-Downloader:OSX/Flashback.I connects to a remote site to download its payload; on successful infection, the malware modifies targeted webpages displayed in the web browser.

Disinfection

Manual Removal

Caution: Manual disinfection is a risky process; it is recommended only for advanced users. Otherwise, please seek professional technical assistance. F-Secure customers may also contact our Support.

Manual Removal Instructions

1. Run the following command in Terminal:

```
defaults read /Applications/Safari.app/Contents/Info LSEnvironment
```

2. Take note of the value, DYLD_INSERT_LIBRARIES
3. Proceed to step **8** if you got the following error message:

"The domain/default pair of (/Applications/Safari.app/Contents/Info, LSEnvironment) does not exist"

4. Otherwise, run the following command in Terminal:

```
grep -a -o '__ldpath__[ -~]*' %path_obtained_in_step2%
```

5. Take note of the value after "__ldpath__"
6. Run the following commands in Terminal (first make sure there is only one entry, from step 2):

```
sudo defaults delete /Applications/Safari.app/Contents/Info LSEnvironment
```

```
sudo chmod 644 /Applications/Safari.app/Contents/Info.plist
```

7. Delete the files obtained in steps 2 and 5
8. Run the following command in Terminal:

```
defaults read ~/.MacOSX/environment DYLD_INSERT_LIBRARIES
```

9. Take note of the result. Your system is already clean of this variant if you got an error message similar to the following:

```
"The domain/default pair of (/Users/joe/.MacOSX/environment, DYLD_INSERT_LIBRARIES) does not exist"
```

10. Otherwise, run the following command in Terminal:

```
grep -a -o '__ldpath__[ -~]*' %path_obtained_in_step9%
```

11. Take note of the value after "__ldpath__"
12. Run the following commands in Terminal:

```
defaults delete ~/.MacOSX/environment DYLD_INSERT_LIBRARIES
```

```
launchctl unsetenv DYLD_INSERT_LIBRARIES
```

13. Finally, delete the files obtained in steps 9 and 11.

Note:

Some Flashback variants include additional components, which require additional steps to remove. Please refer to our Trojan-Downloader:OSX/Flashback.K description for additional information and removal instructions.

Additional Details

Trojan-Downloader:OSX/Flashback.I is dropped by malicious Java applets that exploit the known CVE-2011-3544 vulnerability.

On execution, the malware will prompt the unsuspecting user for the administrator password. Whether or not the user inputs the administrator password, the malware will attempt to infect the system, though entering the password will affect how the infection is done.

If infection is successful, the malware will modify the contents of certain webpages displayed by web browsers; the specific webpages targeted and changes made are determined based on configuration information retrieved by the malware from a remote server.

Installation

On execution, the malware checks if the following path exists in the system:

- /Library/Little Snitch
- /Developer/Applications/Xcode.app/Contents/MacOS/Xcode
- /Applications/VirusBarrier X6.app
- /Applications/iAntiVirus/iAntiVirus.app
- /Applications/avast!.app
- /Applications/ClamXav.app
- /Applications/HTTPScoop.app
- /Applications/Packet Peeper.app

If any of these are found, the malware will skip the rest of its routine and proceed to delete itself.

Downloading the Payload

The malware connects to the following URL to download its payload:

- h t t p : / / 95.215.63.38/counter/%encoded_data%

  Where decoded data follows this format:

  - %hardware_UUID|%machine_architecture%|%kernel_version%|%encoded_data2%|%architecture_of_malware_process%|%current_hardware_type_of_system%|%is_user_daemon%

    - %encoded_data2% is the MD5 hash of the following:

      - %hardware_UUID%Jiangxi

    - %is_user_daemon% is "1" if the process is running as the first OS X user account or daemon "0" otherwise

The filename and actual content of the payload depends on reply of the remote host. The reply is compressed and encrypted but the actual content follows this format:

- %encoded_filename%|%encoded_binary1_content%|%encoded_payload_config%|

%encoded_binary2_content%|%encoded_png_content%

Where:

- ***Binary 1***

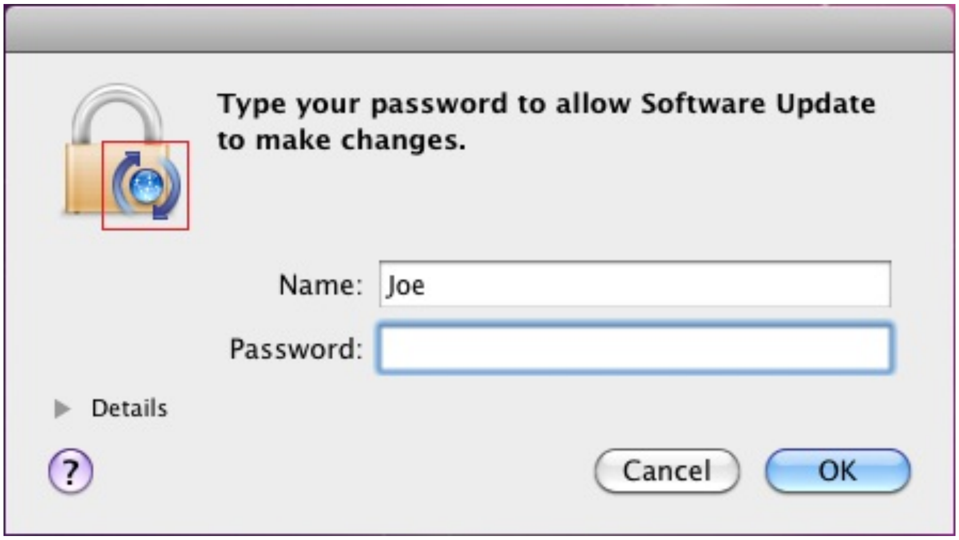
  Binary1 is more or less the malware's main component. In the sample that we analyzed, it hijacks CFReadStreamRead and CFWriteStreamWrite by creating an interposition to these functions. The malware modifies contents returned or send by these APIs. It targets the contents of specific webpages, as determined by config information returned by the remote host.

- ***Binary 2***

  Binary2 is basically a filter component that will load binary1 only into a targeted process. This is to avoid crashing incompatible applications and raising the user's suspicions. In the sample that we analyzed, it targets the Safari web browser.

Infection

Only after downloading the payload does Flashback.I proceed with infecting the machine. To do so, the malware prompts for the administrator password, as in the following screenshot:



Type your password to allow Software Update to make changes.

Name: Joe

Password:

The icon indicated by the red box in the screenshot is the PNG content returned by the remote host. This is dropped to the location '/tmp/.i.png' on the system. Since this image is controlled by the remote host, it can be changed any time the author deems necessary.

Whether or not the user inputs their administrator password at the prompt determines the type of infection the malware subsequently performs:

Infection Type 1

If the user inputs their administrator password, the malware will create the following files:

- **/Applications/Safari.app/Contents/Resources/.%decoded_filename%.png** - contains %decoded_binary1_contents% and %decoded_payload_config%
- **/Applications/Safari.app/Contents/Resources/.%decoded_filename%.xsl** - contains %decoded_binary2_contents%

The malware then creates a launch point, inserting the following line into "/Applications/Safari.app/Contents/Info.plist":

- <key>LSEnvironment</key><dict><key>DYLD_INSERT_LIBRARIES</key><string>/Applications/Safari.app/Contents/Resources/.%decoded_filename%.xsl</string></dict>

This in effect will inject binary2 into Safari when the browser is launched.

If the malware was able to infect the system this way, it reports success to the following URL:

- h t t p ://95.215.63.38/stat_d/

If it failed to infect the system, the malware reports to the following URL:

- h t t p ://95.215.63.38/stat_n/

Infection Type 2

In cases where the user did not input their administrator password, the malware checks if the following path exists in the system:

- /Applications/Microsoft Word.app
- /Applications/Microsoft Office 2008
- /Applications/Microsoft Office 2011
- /Applications/Skype.app

If any of these are found, the malware again skips the rest of its routine and proceeds to delete itself, presumably to avoid infecting a system that has an incompatible application installed.

If none of the incompatible applications are found, the malware will create the following files:

- **~/Library/Application Support/.%decoded_filename%.tmp** - contains %decoded_binary1_contents% and %decoded_payload_config%
- **/Users/Shared/.libgmalloc.dylib** - contains %decoded_binary2_contents%

The malware then creates a launch point by creating "~/.MacOSX/environment.plist", containing the following lines:

- <key>DYLD_INSERT_LIBRARIES</key>
  <string>/Users/Shared/.libgmalloc.dylib</string>

This in effect will inject binary2 into every application launched by the infected user.

For this infection type, the malware reports the successful infection to the following URL:

- h t t p : / / 95.215.63.38/stat_u/

- Antivirus
- RSS Feeds
- Products
- Sitemap