OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic (updated)

By bferrite

Published: 2017-04-27 · Archived: 2026-04-02 10:41:26 UTC

Research by: Ofer Caspi

People often assume that if you're running OSX, you're relatively safe from malware. But this is becoming less and less true, as evidenced by a new strain of malware encountered by the Check Point malware research team. This new malware – dubbed **OSX/Dok** — affects all versions of OSX, has 0 detections on VirusTotal (as of the writing of these words), is signed with a valid developer certificate (authenticated by Apple), and is the first major scale malware to target OSX users via a coordinated email phishing campaign.

Once OSX/Dok infection is complete, the attackers gain complete access to all victim communication, including communication encrypted by SSL. This is done by redirecting victim traffic through a malicious proxy server.

The malware mostly targets European users. For instance, one phishing message was observed to target a user in Germany by baiting the user with a message regarding supposed inconsistencies in their tax returns (see image, and translation, below).

——

Update – May-4-2017

Our ongoing investigation of the OSX/DOK campaign have led us to detect several new variants of this malware.

Following Apple's revocation of the previous developer ID, it seems the attackers have quickly adapted and are now using a new Apple developer ID.

These new variants also contain an extra obfuscated layer using UPX in an attempt to avoid security products detection.

Apple has been notified about these new developments, and the new developer ID has now been revoked.

Check Point customers remain protected against these threats with the following detections:

- Trojan.OSX.DOK
- Trojan.OSX.DOK-Domain
- Mac OSX/Dok Unauthorized Remote Access

IOCs:

- 3f0130cfd7bf61b8e8226dd4775319c7376a08ec019f9df12875e9ea55992e94
- cd93142f1e0bac1d73235515bc127f5f9634eafde0bea2d6c294bf3549d612b7

- 4252e482c9801463e6f684c71f70cb64a17ae74957ed8986f2401c653acae1d7

——

Technical details:

The malware bundle is contained in a .zip archive named Dokument.zip. It was signed on April 21th 2017 by a "Seven Muller" and the bundle name is **Truesteer.AppStore**.

Upon execution, the malware will copy itself to the /Users/Shared/ folder, and will then proceed to execute itself from the new location by running the shell commands below:

Then, the malware will pop-up a fabricated message claiming that "the package is damaged" and therefore cannot execute:

If a loginItem named "AppStore" exists, the malware will delete it, and instead add itself as a loginItem, which will persist in the system and execute automatically every time the system reboots, until it finishes to install its payload.

The malicious application will then create a window on top of all other windows. This new window contains a message, claiming a security issue has been identified in the operating system that an update is available, and that to proceed with the update, the user has to enter a password as shown in the picture below. The malware checks the system localization, and supports messages in both German and English.

The victim is barred from accessing any windows or using their machine in any way until they relent, enter the password and allow the malware to finish installing. Once they do, the malware gains administrator privileges on the victim's machine.

Using those privileges, the malware will then install **brew**, a package manager for OS X, which will be used to install additional tools – **TOR** and **SOCAT**

Tor, the latter is a low-level command-line utility that allows connection to the dark web.

The malware will then give the current user admin privileges immediately on demand without prompting for a password. This is done so that the malware won't provoke constant admin password prompts when abusing its admin privileges with the sudo command. This is done by adding the following line to /etc/sudoers:

The malware then changes the victim system's network settings such that all outgoing connections will pass through a proxy, which is dynamically obtained from a Proxy AutoConfiguration (PAC) file sitting in a malicious server. The script that makes this configuration changes can be seen below:

Then resulting change can be seen in the Network Settings:

The malware will then proceed to install a new root certificate in the victim system, which allows the attacker to intercept the victim's traffic using a Man in The Middle (MiTM) attack. By abusing the victim's new-found trust in this bogus certificate, the attacker can impersonate any website, and the victim will be none the wiser. The new certificate is installed using the following command:

The newly-installed certificate can be seen in the two images below.

The malware will also install 2 `LaunchAgents` that will start with system boot, and have the following names:

These `LaunchAgents` will redirect requests to 127.0.0.1 through the dark web address "**paoyu7gub72lykuk.onion**". This is necessary for the previous PAC configuration to work (note that the original configuration looks for the PAC file on the local host 127.0.0.1).

These `LaunchAgents` consist of the following BASH commands:

As a result of all of the above actions, when attempting to surf the web, the user's web browser will first ask the attacker web page on TOR for proxy settings. The user traffic is then redirected through a proxy controlled by the attacker, who carries out a Man-In-the-Middle attack and impersonates the various sites the user attempts to surf. The attacker is free to read the victim's traffic and tamper with it in any way they please.

When done, the malware will delete itself.

All is left to say: beware of Trojans bearing gifts, especially if they ask for your root password.

IOCs

Sample hash – 7819ae7d72fa045baa77e9c8e063a69df439146b27f9c3bb10aef52dcc77c145

4131d4737fe8dfe66d407bfd0a0df18a4a77b89347471cc012da8efc93c661a5

`LaunchAgent` :

Check Point Protections

Trojan.OSX.DOK

DOK

Source: https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/