

CYBERSECURITY CYBER-ATTACK SERIES

SIDE CHANNEL – SIDE LOADING ATTACKS

Prepared by David Mohajer

What is a Side Loading attack?

This type of attack can be classified as a Trojan attack.

A side loading attack is a type of side **channel** attack where one user-installed application is programmed to install an unauthorized application on-the-side in an automated quiet fashion. This is very similar to receiving malware by visiting a bad website; but it is even more insidious as side-loading attacks are the preferred method to attack smartphones and other mobile devices that have a culture of “I don’t need security” within the user community.

An example of a side loading app was revealed by Snoopwall in 2014, where they found that the top ten flashlight apps on the android play store were actually a kind of Trojan horse for side-loading various other malicious apps. These malicious apps quietly gathered and uploaded data from the user’s device without authorization to servers in China.

The Aim of a Side Loading attack

The purpose of side-loading other apps onto your device is to circumvent the initial security checks put in place by the ecosystem provider such as Google Play or Apple iTunes. Once the side loaded apps are in place then the attacks or data exfiltration will begin via the side-loaded apps.

Finally, side-loaded apps are masked by the initiator app. In our 2015 research, we found that Android games were fully functional games that also injected other apps into our test environment. Raising the bar on detection even more as to whether the app “works” or not cannot be used as a test of fitness for safety.

Types of Side Loading attacks

Identity Theft

Data ex-filtration is the number one activity that side-loaded apps will participate in and is also the easiest by far, for cyber criminals to develop and implement. Data ex-filtration is a simple client server solution and can be deployed easily through many applications without much work.

Remote Monitoring

Cyber criminals have created the opposite system to identity theft – whereby the mobile device itself has a server application installed and receives commands from a remote controller. This can presumably be used to force the mobile device to participate in zombie DDoS attacks, breach secure firewalls that have the device on a trusted list, track the user themselves



Your Cybersecurity Partner

including forcing the camera to take video, audio, and text information and send it back to the central controller setup by the hackers.

Complex Side Channel attacks

In some cases, hackers such as nation-state sponsored hackers have the resources to place and coordinate even more complex attacks using a mobile device as a vector for breaching a secure target. In this case the mobile device might perform data ex-filtration along with disruption and even complex synergetic behaviour to disrupt SCADA systems and other targets of high importance.

Determining if your system has suffered a Side Loading attack

This is almost impossible to find out without having a network engineer virtualize your connections and analyze the behaviour of your device with respect to what it should be doing.

If you have a good firewall that allows logging by an IP or MAC address, then you can filter what your mobile device is doing and determine if it is “calling home” when it should not be. This includes when it is “locked”, or when you are playing a game and there is no browser app loaded.

Preventing a Side Loading attack

Preventing side loading attacks is extremely difficult as they are making their way through legitimate channels. The Snoopwall example cited a flashlight app that had over 100 Million downloads. Who could blame the victims for trusting the download when that many people had already downloaded it?

Caveat Downloader

If the file-size is large and the app is requesting permissions that seem suspicious you should consider what the app is intended to do.

In 2015, XAHIVE found a 50-megabyte flashlight app during an analysis of suspected Chinese side-channel attacking apps. This app was full of side apps it was trying to load onto our virtual phone.

The legitimate version of the app was developed in the United States by a different developer. It was only 250KB and had all of the same reported features, without any of the side channel attacks. The malicious app was 1000x the size of the real app.

The malicious app had over 10 million downloads on the Google Play store! Many more apps were analyzed, the common feature being that the malicious ones were dubiously large in size, and tended to request more permissions than they needed to perform the advertised features.

Works Cited

Mikkelson, D. (2014, September 1). *Flash and Grab*. Retrieved from Snopes:
<http://www.snopes.com/computer/internet/flashlight.asp>

Snoopwall. (2014, October 1). *FLASHLIGHT APPS*. Retrieved from Snoopwall:
<https://www.snoopwall.com/wp-content/uploads/2014/10/Flashlight-Spyware-Appendix-2014.pdf>