Matthew Kachar

COSC4931

Homework 5 WireLurker

In July, 2014, the security consultancy FireEye had briefed Apple about a vulnerability within their *enterprise provisioning* development program. Even without Apple distribution the development profile could potentially allow untrusted software to be installed on iOS devices. Users downloading from these third-party profiles were exposing themselves to potential threats on their desktops and notebooks. Since mobile devices could not directly access these open profiles, a common path for the infected software was through physically connecting these devices to some other work station. A user would download some infected software on his or her Apple laptop, easily bypassing certain security checks. This specific malicious software would wait for devices to connect via USB, then upon connection, the malware would automatically install itself on the device replicating an existing application—often one previously considered safe and secure. This malware would resemble anything from email to banking apps, where the user may not even realize the device is infected.

Named for this USB listener mechanic, the malware *WireLurker* specifically targeted Apple users in China through the third-party app store *Maiyadi.*(web)While Apple repeatedly said the malicious apps could not infect user devices unintentionally since the user had to disable standard protections to install this software, more and more cases of infected mobile devices were cited. The Palo Alto Networks, another security company, wrote an extensive report about the characteristics of the new malware and explicitly outline its propagation through hundreds of thousands of devices, including those in which the Apple security protocol and default protections had not been compromised. The way the infection of the OS X applications was performed was by attaching additional files to the application package and modifying its executables. Essentially, WireLurker was injecting malicious code into different apps that were not previously thought to be hazardous, such as popular games and device management apps.(web) After install the malware would run as background processes, performing updates and repackaging other OS X applications with the malicious code. Spreading from one device to another was accomplished through a static listener which monitored for USB connection to mobile iOS devices— which typically check for profile updates when connected to a desktop or laptop. The malware would also perform automatic updates from the attacker’s servers resulting in three distinct version of the source code. For users who had not compromised the security of their device through “jailbreaking,” an innocuous prompt appeared when an attempt was made to download apps from the third-party enterprise provisioning profile. This prompt simply required confirmation, and had given no type of explicit warning as to the security risk. It took apple several months to recognize the threat as a legitimate problem and by that time the WireLurker malware had evolved into *Masque Attack*, making installation on mobile devices much easier.

The attack was originally identified by a developer, finding questionable files on his personal devices. According to the Palo Alto report, the developer started a forum for other Chinese developers.(web) Over a month had passed before it was reported to Apple by FireEye that several thousand Apple devices had been infected, including non-jailbroken iPhones. Apple did not respond to the claims that the software was able to be downloaded on non-jailbroken mobile devices until November, and by that time Apple developers were having difficulties finding a solution to the threat. Appthority, a mobile security company claimed to be the first group to develop and launch a risk assessment application for enterprise software. Their program identified and archived potentially hazardous apps and warned iOS users when the application they wish to install could be harmful. This solution was published in December. The Palo Alto Network put forth several other recommendations for not just the iOS users but also Apple to correct the threat posed by WireLurker, and now Masque Attack— including revisions to the enterprise provisioning program. The user recommendations included some good hygiene practices such as avoiding downloads from untrusted sources and connecting to unknown devices. One of the major differences though for Palo Alto was requiring enterprises to run their own protection protocol; of which would require all applications be checked through some protection software as well as checking for updated Apple signatures on all applications and not just those purchase through the Apple app store. This malware is quite a nuisance for the user not just because of the personal data leaks it can possibly create, but also all current security software designed to eliminate WireLurker and Masque Attack automatically deletes the source applications and all subsequently modified applications containing the flagged signatures. This can virtually wipe out small mobile devices since this malicious software can acquire root access and penetrate the operating system’s critical processes.

Resources

Dilger, Daniel Eran. *WireLurker, Masque Attack malware only a threat for users who disable Apple's iOS,*

*OS X security.* Apple Insider. Nov. 10, 2014. web. www.appleinsider.com

Xiao, Claud. *WireLurker: A New Era in iOS and OS X Malware.* Palo Alto.

Palo Alto Networks. Santa Clara, CA. web. 2014. www.paloaltonetworks.com

Xue, Hui. Tao Wei, Yulong Zhang. *Masque Attack: All Your iOS Apps Belong to Us.*

FireEye. Inc. Milpitas, CA. Nov. 10, 2014. web. www.fireeye.com