KeyRaider Malware

Discovered in July of 2015 [1], KeyRaider is malware that tags along in programs used to jailbreak iOS devices. Though it is hidden in several different programs [2], the malware’s main purpose is to steal your Apple account credentials. To date, over 225,000 accounts have been stolen, with over 20,000 users abusing the stolen data [1], making this Apple’s largest known account theft via malware [3]. The malware was advertised as a jailbreak tweak allowing users to access paid apps for free [2].

KeyRaider was found by WeipTech member i\_82 [1] after unauthorized purchases were showing up on some Apple user’s accounts. After the common thread of a particular jailbreak tweak was found, WiepTech dug into the code and found a SQL table named aid (apple id) with 225,941 entries in it [1]. 20,000 of those entries had usernames, passwords, and GUIDs stored as plaintext [1]. PaloAlto began researching KeyRaider and found that the remaining 205 thousand entries were encrypted using AES and could be decrypted with the key “mischa07” [1], which, in conjunction with KeyRaider being found in several other apps hosted by mischa07, led them to conclude that mischa07 was the author of the malware [1].

KeyRaider works by abusing the plugin API of iOS’s MobileSubstrate [1]. According to PaloAlto, this is a common target for iOS malware, and has been used in the SSLCreds and Unflod Baby Panda malware [1]. Using the aforementioned API, the itunesstored (iTunes store daemon) process that communicates with the AppStore has hooks inserted into the SSLRead and SSLWrite functions which permit the malware to steal apple accounts usernames, passwords, and the device GUID [1]. Once acquired, the stolen information is encrypted via AES and sent to a C2 server [1].

Using that C2 server and additional hooks in to itunesstored’s SSLRead and SSLWrite functions, a program was written that allows users to spoof one of the stolen accounts and purchase App Store apps as that user [1]. This program has been downloaded over 20,000 times [1]. The total number of fraudulent purchases made using this method is unknown.

Protecting yourself from this attack is as simple as not jailbreaking your iOS device [4]. If your device is already jail broken, you can see if you’re infected by grepping for wushidou, gotoip4, bamu, and getHanzi for all files in /Library/MobileSubstrate/DynamicLibraries/ [1].

KeyRaider is a great example of a trojan. It masquerades as a way to jailbreak your device, and instead breaks your wallet, and possibly your device. Variants of KeyRaider can lock your device and delete the original unlock code, prompting you to contact a QQ user in order to regain access to your device [1]. This malware affects less than 0.2% of iTunes accounts [4].

[1] C. Xiao, "KeyRaider: iOS Malware Steals Over 225,000 Apple Accounts to Create Free App Utopia - Palo Alto Networks Blog", Palo Alto Networks Blog, 2015. [Online]. Available: http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/. [Accessed: 24- Jan- 2016].

[2] D. Storm, "KeyRaider malware stole over 225,000 Apple credentials from jailbroken iOS devices", Computerworld, 2016. [Online]. Available: http://www.computerworld.com/article/2978152/cybercrime-hacking/keyraider-malware-stole-over-225-000-apple-credentials-from-jailbroken-ios-devices.html. [Accessed: 24- Jan- 2016].

[3] M. Addady, "This is the 'Largest Known' Apple Malware Infection Ever", Fortune, 2015. [Online]. Available: http://fortune.com/2015/09/01/apple-malware/. [Accessed: 24- Jan- 2016].

[4] S. Perez, "KeyRaider Malware Responsible For Possibly Largest Known Apple Account Theft To Date, Affecting 225,000 Users", TechCrunch, 2016. [Online]. Available: http://techcrunch.com/2015/08/31/keyraider-malware-responsible-for-possibly-largest-known-apple-account-theft-to-date-affecting-225000-users/ [Accessed: 24- Jan- 2016].