WireLurker: A New Era in OS X and iOS Malware

By Claud Xiao

Published: 2014-11-05 · Archived: 2026-04-06 00:22:36 UTC

Today we published a new research paper on WireLurker, a family of malware targeting both Mac OS and iOS systems for the past six months. We believe that this malware family heralds a new era in malware attacking Apple's desktop and mobile platforms based on the following characteristics:

- Of known malware families distributed through trojanized / repackaged OS X applications, it is the biggest in scale we have ever seen
- It is only the second known malware family that attacks iOS devices through OS X via USB
- It is the first malware to automate generation of malicious iOS applications, through binary file replacement
- It is the first known malware that can infect installed iOS applications similar to a traditional virus
- It is the first in-the-wild malware to install third-party applications on non-jailbroken iOS devices through enterprise provisioning

WireLurker was used to trojanize 467 OS X applications on the Maiyadi App Store, a third-party Mac application store in China. In the past six months, these 467 infected applications were downloaded over **356,104** times and may have impacted hundreds of thousands of users.

How It Works

WireLurker monitors any iOS device connected via USB with an infected OS X computer and installs downloaded third-party applications or automatically generated malicious applications onto the device, regardless of whether it is jailbroken. This is the reason we call it "wire lurker". Researchers have demonstrated similar methods to attack non-jailbroken devices before; however, this malware combines a number of techniques to successfully realize a new brand of threat to all iOS devices.

WireLurker exhibits complex code structure, multiple component versions, file hiding, code obfuscation and customized encryption to thwart anti-reversing. In this whitepaper, we explain how WireLurker is delivered, the details of its malware progression, and specifics on its operation.

We further describe WireLurker's potential impact, as well as methods to prevent, detect, contain and remediate the threat. We also detail Palo Alto Networks Enterprise Security Platform protections in place to counter associated risk.

WireLurker is capable of stealing a variety of information from the mobile devices it infects and regularly requests updates from the attackers command and control server. This malware is under active development and its creator's ultimate goal is not yet clear.

We recommend users take the following actions to mitigate the threat from WireLurker and similar threats:

- Enterprises should assure their mobile device traffic is routed through a threat prevention system using a mobile security application like GlobalProtect
- Employ an antivirus or security protection product for the Mac OS X system and keep its signatures up-to-date
- In the OS X System Preferences panel under “Security & Privacy,” ensure “Allow apps downloaded from Mac App Store (or Mac App Store and identified developers)” is set
- Do not download and run Mac applications or games from any third-party app store, download site or other untrusted source
- Keep the iOS version on your device up-to-date
- Do not accept any unknown enterprise provisioning profile unless an authorized, trusted party (e.g. your IT corporate help desk) explicitly instructs you to do so
- Do not pair your iOS device with untrusted or unknown computers or devices
- Avoid powering your iOS device through chargers from untrusted or unknown sources
- Similarly, avoid connecting iOS devices with untrusted or unknown accessories or computers (Mac or PC)
- Do not jailbreak your iOS device; If you do jailbreak it, only use credible Cydia community sources and avoid the use or storage of sensitive personal information on that device

Download “WireLurker: A New Era in OS X and iOS Malware” here.

Visit Unit 42 for new research and a full list of speaking appearances, as well to subscribe to updates.

Unit 42 On the Road

Unit 42 team leads regularly appear at industry conferences throughout the world. In November, Unit 42’s regular roadshow will make three stops in Canada. Click each link to register, and watch for more Unit 42 roadshows coming to cities near you.

- Tuesday, Nov. 18 in Toronto, Ont.
- Wednesday, Nov. 19 in Calgary, Alberta
- Thursday, Nov. 20 in Vancouver, B.C.
